Request for Proposals (RFP)
Integrated Information Management Solution
Children's Services Council of Leon County (CSC Leon)
Issue Date: September 16, 2022
Questions Deadline: September 23, 2022, 5:00 PM ET
Question Responses Posted: September 27, 2022
Response Deadline: October 14, 1:00 PM ET
Estimated Notice of Intent to Award: November 4, 2022
(see section 2.C for complete Timeline of Events)

Do not contact the CSC Leon Executive Director, any member staff, any member of the Council or their respective staffs regarding this request. Direct all correspondence or inquiries during the RFP process to the following **Purchasing Official:**

Holly McPhail, Special Projects Manager
Children's Services Council of Leon County
C/O Bryant Miller Olive P.A.
1545 Raymond Diehl Rd, Suite 300
Tallahassee, FL 32308
procurement@cscleon.org

Table of Contents

SECTION 1 – INTRODUCTION

A. Solicitation Objective, Overview and Goals

The Children’s Services Council of Leon County (“CSC Leon”) seeks to establish, through this Request for Proposal (“RFP”), a contract for the development of an integrated information management system to manage specific business functions efficiently and maximize data analysis capabilities (“Contract”). Specifically, CSC Leon seeks a comprehensive solution to:

1. Develop a grant making and contract management system with comprehensive performance measurement and reporting functions.
2. Integrate with the current CSC Leon accounting software with task flow management and automation.
3. Introduce an integrated customer relationship management (CRM) solution to enhance community engagement efforts.
4. Work with existing community partner database systems to develop data sharing agreements and processes to better serve clients.

CSC Leon intends to select a single vendor that will demonstrate its ability to integrate various data sets across software solutions without extensive supplemental systems, add-ons, or customization.

CSC Leon has developed a draft Statement of Work (“SOW”) for the Contract, which is attached as Schedule A to the draft Contract which is included as Exhibit I. The SOW describes the purpose and goals in more details and includes a description of CSC Leon’s current technological environment and existing software.

B. Background of Organization

CSC Leon is a catalyst for positive change to improve the lives and outcomes of children and families in the local community.

Approved by a majority of the Leon County (“County”) electorate in the November 2020 general election, CSC Leon has been established to provide children with early learning and reading skills, development, treatment, preventative and other children's services.

As an independent special district authorized by section 125.901, Florida Statutes, CSC Leon will provide funding for these children's services throughout the County by annually levying ad valorem taxes, not exceeding the maximum millage rate of one-half (1/2) mill. CSC Leon has independent oversight and accountability, and the following powers and functions:

1. To provide and maintain in the County such preventive, developmental, treatment and rehabilitative services for children as CSC Leon determines are needed for the general welfare of the County.
2. To provide such other services for all children as CSC Leon determines are needed for the general welfare of the County.

3. To allocate and provide funds for other agencies in the County which are operated for the benefit of children, provided they are not under the exclusive jurisdiction of the public school system.
4. To collect information and statistical data and to conduct research, which will be helpful to CSC Leon and the County in deciding the needs of children in the County.
5. To consult with other agencies dedicated to the welfare of children, to the end that the overlapping of services will be prevented.
6. To lease or buy such real estate, equipment, and personal property and to construct such buildings as are needed to execute the foregoing powers and functions, provided that no such purchases shall be made or building done unless paid for with cash on hand or secured by funds deposited in financial institutions. Nothing in this subsection shall be construed to authorize CSC Leon to issue bonds of any nature, nor shall CSC Leon have the power to require the imposition of any bond by the Board of County Commissioners.
7. To employ, pay, and provide benefits for any part-time or full-time personnel needed to execute the foregoing powers and duties.

One of CSC Leon's first tasks was to identify and assess the needs of the children in the County. In November 2021, CSC Leon contracted with a third-party research firm to conduct a comprehensive assets and needs assessment of the community resources available to meet the varying needs of children, youth and families. That work concluded in June 2022.

Currently, CSC Leon is developing its strategic plan based on the results of the assets and needs assessment. It will include a written description of:

1. The activities, services and opportunities that will be provided to children.
2. The anticipated schedule for providing those activities, services, and opportunities.
3. The manner in which children will be served, including a description of arrangements and agreements which will be made with community organizations, state and local educational agencies, federal agencies, public assistance agencies, the juvenile courts, foster care agencies, and other applicable public and private agencies and organizations.
4. The special outreach efforts that will be undertaken to provide services to at-risk, abused, or neglected children.
5. The manner in which CSC Leon will seek and provide funding for unmet needs.
6. The strategy which will be used for interagency coordination to maximize existing human and fiscal resources.

In the future, CSC Leon is required to report the following to the Leon County Board of County Commissioners:

1. Information on the effectiveness of activities, services, and programs offered by CSC Leon, including cost-effectiveness.
2. A detailed anticipated budget for continuation of activities, services, and programs offered by the Council, and a list of all sources of requested funding, both public and private.

3. Procedures used for early identification of at-risk children who need additional or continued services and methods for ensuring that the additional or continued services are received.
4. A description of the degree to which CSC Leon's objectives and activities are consistent with the goals of the County ordinance establishing CSC Leon (No. 2018-13).
5. Detailed information on the various programs, services, and activities available to participants and the degree to which the programs, services, and activities have been successfully used by children.
6. Information on programs, services, and activities that should be eliminated; programs, services and activities that should be continued; and programs, services and activities that should be added to the basic format of CSC Leon.

In its roadmap to complete these activities, CSC Leon recognized the need for a comprehensive data system necessary to track and report on several of its programmatic functions. CSC Leon issued a “Request for Information” entitled Enterprise Resource Planning Software Solutions (“RFI”) in December 2021 to determine the potential level of interest, competition adequacy, and technical capabilities of commercial vendors to provide the anticipated required products and services.

In March 2022, CSC Leon formed the Enterprise Software Solutions Workgroup to review responses to the RFI and help understand how future enterprise application solution(s) might be architected. Many ideas about an ideal enterprise application environment were discussed, including timeline for implementation and meeting immediate needs. The Workgroup instructed staff to engage in additional market research before developing what is now this RFP.

C. Minimum Qualifications of Respondents

To respond to this RFP, a Respondent must demonstrate at least five years of experience providing services materially similar to those specified in the SOW. A Respondent may satisfy this requirement via the experience of its proposed key project members, even if those members performed the service for another company. Responses not satisfying this minimum requirement will be deemed non-responsive and will not be evaluated.

D. Purchasing Official and “Quiet Period”

The Purchasing Official is identified on the RFP cover page. Any person requiring a special accommodation due to a disability should contact the Purchasing Official.

All Respondent communications regarding the RFP shall be limited to the Purchasing Official. There shall be a “quiet period” between the date the RFP is advertised and the date the recommended award (or cancellation) has been announced. During the quiet period, no one acting on Respondent’s behalf may engage in any written or verbal communication or other attempts to influence anyone else at CSC Leon regarding this RFP, the merits of the Respondent, or whether CSC Leon should award the Contract to the Respondent. This includes staff members, evaluation team members, and council members. Any unauthorized contact may disqualify the Respondent from further consideration.

SECTION 2 – SOLICITATION PROCESS

A. Overview

This RFP is a method of competitive solicitation under CSC Leon's Purchasing Policy. Those interested in submitting a Response are to comply with all terms and conditions described in this solicitation. CSC Leon will hold a public opening of the Responses at the date, time, and location provided in the Timeline of Events (section 2.C below).

During the evaluation phase, all Respondents, except those deemed non-responsive, will be invited to make a 45-minute, closed, virtual presentation to the CSC Leon solicitation committee. Following this event, the solicitation committee will independently evaluate Responses against the published evaluation criteria. The scores of each solicitation committee member will be aggregated and then reviewed by the solicitation committee at a public meeting to reach consensus on a final ranking and recommend Contract award. The CSC Leon Governing Council will take up the recommendation at a subsequent public meeting and make the final decision concerning Contract award. CSC Leon will determine final contract terms, including the SOW, upon selection.

B. Questions and Answers

CSC Leon will host a virtual informational session for any vendor interested in submitting a response. This session will be recorded and made available for public viewing. The purpose of the session is to communicate the intent, vision and ideal timeline for this RFP. Vendors will be permitted to ask questions during the informational session; however, all questions must be submitted in writing via the chat function. CSC Leon will provide verbal responses when appropriate *and* will publish the question and response in written format along with any other questions submitted to the Purchasing Official via email. The deadline for submission of questions is reflected in the Timeline of Events (section 2.C below).

CSC Leon reserves the right to accept or reject any or all requests for clarification, either in whole or in part, and may require requests to be clarified or supplemented through additional written submissions. Respondents will be notified of the rejection of their request for clarification. Oral requests for clarification will not be accepted at any time.

CSC Leon's responses to questions will be posted on the CSC Leon website at *www.cscleon.org/announcements*. Respondents unable to download responses should direct their requests for hard copies via e-mail to the Purchasing Official. Answers to questions will be published as an addendum to and, as such, an integral part of this RFP.

CSC Leon does not guarantee the validity or reliability of information obtained from other sources. If it becomes necessary to revise any part of this RFP, an addendum will be posted on the CSC Leon website at *www.cscleon.org/announcements*. The Respondent is responsible for checking the website for any addenda or clarifications.

C. Timeline of Events

The table below contains the anticipated timeline of events for this solicitation. The dates and times are subject to change. The Respondent is responsible for ensuring that CSC Leon receives all required documentation by the dates and times (Eastern time) specified below (or as revised by RFP addenda).

Sep 16	RFP Issued	By 5:00 PM ET
Sep 19	Informational Session (via Zoom)	At 2:00 PM ET
Sep 23	Deadline to submit questions to the Purchasing Official	By 5:00 PM ET
Sep 27	Publication of CSC Leon's answers to Respondents' questions	By 5:00 PM ET
Oct 14	Deadline to submit Response to the Purchasing Official	By 1:00 PM ET
Oct 14	Public Opening [BMO Law Firm; Live Stream}	At 3:00 PM ET
Oct 14-25	Evaluation Phase	By 5:00 PM ET
Oct 18-20	Vendor Presentations [Closed Meeting]	Varies
Nov 3	Evaluation Team Public Meeting: Score Responses and Recommend Award	At 2:00 PM ET
Nov 4	Purchasing Official Communicate Recommendation of Award	By 9:00 AM ET
Nov 17	CSC Leon Governing Council Meeting to Consider Recommendation of Award	At 2:00 PM ET
Dec 1	Anticipated Contract Start Date	

D. Response Submittal and Deadline

Submit one bound copy and one electronic copy on a flash drive via postal or commercial courier services of the complete Response by the deadline indicated in the Timeline of Events. The electronic copy must include the required forms and documents completed in the format they were originally published (e.g., Word, Excel).

Submit Responses to CSC Leon care of the Purchasing Official at the delivery address reflected on the RFP cover page. Facsimile transmissions will not be accepted. All bound responses must be submitted in a sealed envelope or box and must be marked "RFP for CSC Leon Enterprise Software Solutions." CSC Leon accepts no responsibility whatsoever for failure to deliver or late delivery by postal or commercial courier services. Failure by postal or commercial courier services to meet the response deadline may result in disqualification.

E. Multiple Responses

Respondents may submit alternative proposals for various levels of service(s) or products meeting specifications. Alternative proposals must specifically identify the RFP specifications and advantage(s) addressed by the alternative proposal. Any alternative proposal must be clearly marked with the legend prescribed below. If a Respondent chooses to respond with various service or product offerings, each must be an offer with a different price and a separate proposal. Respondents may also provide multiple offers for software or systems coupled with support and maintenance options, provided, however, all proposals must satisfy the specifications.

Alternative proposals must be submitted as a separate document(s) and clearly marked "[Respondent Name] Alternative Proposal [#] for CSC Leon RFP Integrated Information Management Solution" and numbered sequentially if multiple proposals are submitted.

F. CSC Leon Not Liable for Respondent's Cost

CSC Leon shall not be liable or responsible for any costs incurred by any Respondent for preparing and submitting any response to this RFP, attending any presentation, or for any other activities or occurrences related in any way to this RFP on or prior to the execution of a contract.

G. Disclosure of Contents

All material submitted by Respondents shall become the property of CSC Leon and will not be returned. Responses submitted may be reviewed and evaluated by persons designated by CSC Leon, in its sole discretion. Records made and received by CSC Leon in connection with this RFP are public records and must be furnished and disclosed to any person under a request to inspect or copy such documents or records, pursuant to Chapter 119, Florida Statutes.

If information is provided that could reasonably be ruled a "trade secret" as defined in Section 812.081, Florida Statutes, include such information in a separate attachment clearly marked – "Trade Secret Information." Include a table of contents within this attachment with a detailed listing of and explanation for EACH item marked as a "trade secret."

Designation of items as "trade secret" by Respondents is not dispositive and does not guarantee that the items will not ultimately be disclosed pursuant to Chapter 119, Florida Statutes. The State of Florida places a high priority on the public's right of access to governmental meetings and records. By submitting a response, each Respondent further understands and agrees that CSC Leon shall have the right to use any and all information, records, documentation, or items, including any derivation or adaptation thereof or knowledge gained thereby, presented by any Respondent in connection with this RFP in negotiating and entering into any contract or for any purpose. CSC Leon shall have such rights regardless of whether CSC Leon enters into any contract with such Respondent or any Respondent under this RFP, successfully negotiates any contract with any Respondent, rejects any or all responses to this RFP, amends or withdraws this RFP at any time, or otherwise satisfies its needs through alternative means.

H. Right to Cancel

CSC Leon, in its sole discretion, may cancel this RFP at any time and for any reason. Issuance of this RFP in no way constitutes a commitment by or obligation of CSC Leon to enter into any contract, and CSC Leon may, in its sole discretion, reject all Responses to this RFP for any reason whatsoever.

I. Responsiveness and Responsibility

CSC Leon will be the sole judge of a Response's responsiveness. CSC Leon will reject any Response that it deems non-responsive; provided, however, that CSC Leon may also waive any minor defect in a Response or deviation from the RFP requirements. CSC Leon will reject the Response of any Respondent it deems non-responsible.

J. RFP Specifications Protest Process

Any protest of the terms of this solicitation or the award of any contract shall be filed via email to the Purchasing Official within five calendar days after the advertisement of the solicitation. A protest must state with particularity the facts and law upon which it based. Failure to file a timely protest shall constitute a waiver of any pre-award challenges.

K. Contract Terms and Formation

RFP Exhibit I is the form of contract that will govern the project. By submitting a Response, Respondent acknowledges its understanding and acceptance of all terms and conditions of the contract, subject only to this Section 2.K. Respondent must price and propose its scope of work with this understanding.

This understanding does not apply to Response content that the Respondent is instructed to propose, e.g., the Statement of Work content. Such content, however, must be presented in final and binding form, suitable for acceptance by CSC Leon to result in a binding agreement. This requirement does not prejudice or limit CSC Leon's ability later to request changes in the process of finalizing the contract documentation.

DO NOT include in a Response statements like the following: "This Response does not constitute a binding offer"; "This Response will be valid only if Respondent is selected as a finalist"; "Respondent does not commit or bind itself to any terms and conditions by this submission"; "This Response and all associated documents are non-binding and shall be used for discussion purposes only"; "This Response will not be binding on either party until incorporated in a definitive agreement signed by authorized representatives of both parties"; or a statement of similar intent. Such statements will render a Response non-responsive and subject to rejection by CSC Leon without further consideration or evaluation.

While failure to accept the contract terms will render a Proposal non-responsive, CSC Leon will entertain proposed changes presented in accordance with this Section 2.K. Again, the Response must not be conditioned upon CSC Leon's acceptance of any such proposed changes. Do not construe this section as inviting deviation or implying that any deviation will be acceptable. Extensive and/or material proposed changes will diminish the perceived value of the Response.

All proposed changes must be presented solely through use of Form B. Failure to propose changes in accordance with this section 2.K and Form B will preclude later attempts by Respondent to request changes. Such attempts later may be cause for disqualification, even after CSC Leon has designated Respondent as the contract awardee.

SECTION 3 – RESPONSE FORMAT AND CONTENTS

Prepare the Response in a clear, comprehensive, and concise manner with six separately tabbed sections, A through F. Do not include any appendix or attachment beyond these sections. Attachments within sections are permissible, e.g., resumes within Tab B. Respond using no smaller than 12-point font. Tables and graphs are exempt from the font requirement but must be readable.

A. Cover Letter

Address the cover letter to the Purchasing Official. Identify the Respondent's name and principal address. Provide the name, telephone number and email address of the person authorized to represent the Respondent regarding all matters related to the RFP. Explain very briefly how the Respondent satisfies the minimum qualifications to respond (see Section 1.C). Affirm that the Respondent has thoroughly reviewed the RFP and agrees to provide the services set forth in the SOW if awarded a Contract. If the Response includes any alleged trade secrets, confirm compliance with Section 2.G.

Behind the cover letter, include the executed original of the completed RFP Form A, *Service Requirement: Disclosures and Affirmation Statement*. **Failure to include the executed form will result in the Response being deemed non-responsive**.

B. Respondent Experience, Qualifications and References

1. Describe briefly Respondent's background/history, ownership structure, primary location(s) and size (number of offices and employees).
2. Describe any anticipated changes to Respondent's basic ownership structure or any other significant changes in its organization, its management, or key personnel.
3. Describe Respondent's financial capability to provide the Contract services. Be specific. Attach brief evidence of objective details, such as portions of financial statements (if statements are available on-line, refer to URL).
4. CSC Leon strongly supports and encourages diversity and participation of historically disadvantaged business enterprises in contracting, as evidenced in the CSC Leon Purchasing Policy. Attach any evidence of firm certification by the *Minority, Women, and Small Business Enterprise Division of the Office of Economic Vitality* or comparable public body and identify the qualifying individuals. Non-certified firms may highlight individual

investments, e.g., the number and percentage of professionals who are minorities or women.

5. Describe generally Respondent's firm's qualifications for providing the Contract services and previous work experience in this area. Include history of on-time and on-budget implementations, and responsiveness to client requirements.
6. Has the Respondent or key personnel previously had a contract with any Children's Services Council in Florida or any entity seeking to create one? If yes, please disclose the entity with whom you worked and their primary contact (name, phone number, and email address), and the scope of services and level of engagement you provided.
7. Provide three client reference letters from entities that have used the Respondent for similar services within the last 12-18 months. Services should be similar in terms of proposed hardware, operating system, database platform, user count, services, and project size. CSC Leon may contact references and other users for additional verbal communication or written information, and possibly for on-site visits.
8. Provide resumes of Key Personnel identified in the response to the SOW (Schedule A – Section 10).

C. Technical Capabilities

1. Summarize in narrative form of how the proposed comprehensive solution specifically meets or does not meet the outlined criteria for the SOW as contained in the Technical Capabilities Form (Form C).
2. Complete and respond fully to the items in Form C. The electronic copy of the full response should include this form in its original format (Excel). Vendors can download Form C separately from the RFP at *www.cscleon.org/announcements*.

D. Proposed Statement of Work

1. Complete and respond fully to the "Response" items in the template SOW included with the RFP (Schedule A to RFP Exhibit 1). When completed, the proposed SOW should describe in detail the industry standards and resources needed to build, implement and fully support the required business functions. The electronic copy of the full Response should include the proposed SOW in its original format (Word). Vendors can download the SOW separately from the RFP at *www.cscleon.org/announcements*.

E. Proposed Pricing

CSC Leon's budget for the initial system and software development, implementation and training outlined in the SOW, Exhibit I, is up to $150,000. Additional funds will be available for annual maintenance and technical assistance.

1. Provide a detailed budget for performing the services described in the SOW by completing the Pricing Form (Schedule B to RFP Exhibit I). The electronic copy of the full response should include this form in its original format (Excel). Vendors can

download Schedule B separately from the RFP at *www.cscleon.org/announcements*.

F. Proposed Changes

If proposing changes as provided above in Section 2.K, complete and include Form B.

SECTION 4 – EVALUATION OF RESPONSES

A. Overview

The CSC Leon solicitation team members will independently evaluate written Responses and Vendor Presentations, except those deemed non-responsive, using the criteria below. The individual and aggregate scores will be published and then reviewed by the solicitation committee at a public meeting to reach consensus on a final ranking and used to recommend an award.

Evaluation Category	*Criteria Description*	*% of Total Score*
Experience, Qualifications and References	Detailed organizational structure that reflects business philosophy, financial capabilities, project experience, expertise, stability, history of on-time and on-budget implementations, and positive, recent references	15%
Technical Capabilities	Ability to meet technical requirements, build required environment, and demonstrate how the solution is comprehensive based primarily on the completed Form C, subject to validation during presentation	30%
Statement of Work	Demonstrated use of industry standards, project management protocols, milestone schedule, integrative capacity	55%
	Total	100%

CSC Leon will not “score” proposed pricing (Schedule B) but will consider it in the best value analysis. The non-price factors above, when combined, are significantly more important than price.

B. Vendor Presentations

CSC Leon requires each Respondent to participate in a 45-minute virtual demonstration of the proposed comprehensive solution. The purpose of this demonstration is to allow the CSC Leon solicitation committee members to “experience” a sample of the proposed solution to help inform its scoring using the criteria above. CSC Leon will distribute a presentation planning guide to each Respondent to guide its presentation development. All presentations will be timed. Representatives for each Respondent should plan to be available, without interruptions, for the entirety of the Respondent’s scheduled presentation. Additional time will be granted for brief introductions immediately preceding the presentation and a time-limited question and answer period immediately following the presentation.

In accordance with section 286.0113, Florida Statutes, vendor presentations between CSC Leon and Respondents are exempt from Chapter 286, Florida Statutes, and s. 24(b), Art. I of the State Constitution.

CSC Leon will record all meetings of the solicitation committee and all meetings between the solicitation committee and Respondents, as required by law, and such recordings will eventually become public record pursuant to Chapter 286, Florida Statutes. During presentations, Respondents must state whether any portion of the meetings should be considered confidential, proprietary, trade secret, or otherwise not subject to disclosure pursuant to Chapter 119, Florida Statutes, the Florida Constitution, or other authority, so that the solicitation committee can make appropriate arrangements for the segregation of the recording. If the Respondent fails to assert this protection, CSC Leon is authorized to produce the audio recording in answer to a public records request for these records.

C. Award Recommendation

The solicitation committee will formulate by consensus a recommendation of Contract award that will provide the best value to CSC Leon. “Best value” means the expected outcome that, in CSC Leon’s estimation, provides the greatest overall benefit in response to CSC Leon’s requirements. The solicitation committee may recommend award to other than the lowest priced Respondent or other than the highest technically rated Respondent. The solicitation committee will reduce its recommendation to writing, including a description of the basis of its recommendation, and convey that written recommendation to the Purchasing Official. The written recommendation will be a public record available for inspection (particular details may be redacted as authorized by Florida law).

SECTION 5 – AWARD PROCESS

The following outlines the award and contracting process governing this RFP.

1. The Purchasing Official will convey the solicitation committee’s written recommendation to the Executive Director, for purposes of planning the meeting at which the CSC Leon Governing Council will consider the recommendation.

2. The Purchasing Official will advise in writing (including email) every Respondent of the solicitation committee’s recommendation of award. This notice will include the date, time, and place of the meeting at which the CSC Leon Governing Council will consider the recommendation, which will be at least seven days after the date of the notice. The notice will also describe briefly CSC Leon’s protest process.

3. Any protest of a recommended award must be made within seven days after the Purchasing Official communicates notice of the recommended award, and before the CSC Leon Governing Council votes on the recommendation. Failure to provide written

notice of protest by certified letter received by CSC Leon within seven days after the Purchasing Official communicates notice of the recommended award will result in respondent waiving its right to protest.

4. No recommendation of award is binding on CSC Leon. Only the CSC Leon Governing Council may approve award of the Contract.

5. If the CSC Leon Governing Council votes to award the contract to a vendor other than the one recommended by the Evaluation Team, within three business days after the Council meeting, the Purchasing Official will advise in writing (including email) every Respondent of the Governing Council's decision. No notice will be given if the Governing Council adopts the Evaluation Team's recommendation of award. If notice is given, it will describe briefly the CSC Leon protest process.

6. Any protest of a final award decision must be made within seven days after the Purchasing Official communicates notice of the award decision. There is no right of protest if the Governing Council adopts the recommendation of award.

7. After Governing Council approval of Contract award and the expiration of any protest period, CSC Leon will execute the written Contract through its Council chairperson or authorized designee.

FORM A – DISCLOSURES AND AFFIRMATION STATEMENT

The undersigned certifies the following with respect to the Respondent and its response; if an unqualified certification is not accurate, attach explanation to this form:

- ❑ The selection of the Respondent will not result in any current or potential conflict of interest with CSC Leon. Alternately, should any potential or existing conflict be known by the Respondent, specify the party with which the conflict exists or might arise, the nature of the conflict, and whether the Respondent would step aside or resign from that engagement creating the conflict, including each of the items below.

  - ❑ Whether any officer, director, employee, or agent is also a current or former employee of CSC Leon, or any of the members of the Council, and if there are any factors, financial or otherwise, known to them which may give rise to a conflict of interest between you and CSC Leon and its employees, or have the effect of impacting your ability to meet your responsibilities, duties, and obligations to CSC Leon, as set forth in this ITN, and whether the Respondent would step aside or resign from that engagement creating the conflict. Disclose the name of any CSC Leon member or staff who owns, directly or indirectly, an interest of five percent (5%) or more of your company or any of its branches or affiliates.

  - ❑ Any arrangement with any individual or entity with respect to the sharing of any compensation, fees, or profit received from or in relation to acting as financial advisor for CSC Leon. If applicable, provide a copy of any contract relating to the arrangement and describe in detail the nature of the arrangement and the method of computing compensation.

  - ❑ Any person or firm retained for the purpose of seeking to be selected pursuant to this ITN. Will the Respondent pay or be obligated to pay any firm or an individual who is not a full-time employee of the Respondent if the Respondent is awarded a Contract under this ITN? If so, identify the individual or firm, provide specific information relating to compensation paid or to be paid, and provide a copy of any written contract relating to such arrangement.

- ❑ The Response is made without prior understanding, agreement, or connection with any other person or entity submitting a response for the same services, and the response is in all respects fair and without collusion or fraud. The Response is not made in connection with any competing Respondent submitting a separate response to the ITN and is in all respects fair and without collusion or fraud. The Respondent did not directly or indirectly induce any party to submit a false or sham Response or to refrain from responding. The Respondent did not participate in the ITN development process, had no knowledge of the specific contents of the ITN prior to its issuance, and did not involve any employee of CSC Leon directly or indirectly in the Response preparation.
- ❑ The Response is that of the Respondent and has not been copied or obtained from any other person or entity responding to any other competitive solicitation whether in Florida or elsewhere either in the past or present.

- □ The Respondent has not been convicted of or entered a plea of nolo contendere to fraud within a period of two years of such conviction.

- □ The Respondent and the agents, officers, principals, and professional employees thereof have not and will not participate in any communication prohibited in this ITN.

I hereby certify that all information provided in this Response is true and correct, that I am authorized to sign this Response for the Respondent, and that the Respondent is in compliance with all requirements of the ITN.

____
Authorized Signature (Manual)

____
Name and Title (Typed)

____
Date (Typed)

____
Respondent (Typed)

FORM B – PROPOSED CHANGES

In accordance with RFP Section 2.K, Respondents must use this Form B to propose any changes to the form of contract (RFP Exhibit I). In the table below, include references to the corresponding contract section or Schedule (other than A or B). Any proposed deviations shall be explained in detail. The proposed modifications do not alter the specifications, terms and conditions of the RFP and have no force or effect on the RFP or any contract unless accepted by CSC Leon and incorporated into final contract documentation. CSC Leon, at its sole discretion, may consider any of the proposed modifications submitted via this Form B, but it is not obligated to do so, and the Response may not be conditioned upon CSC Leon doing so.

Identify all persons who reviewed or proposed changes to the contract terms, and their title or role in Respondent's organization:

Name	Title/Role
(repeat as necessary)	

Include this completed Form B behind Tab F of the Response. If no changes are proposed, it is not necessary to submit the form.

PROPOSED CHANGES		
Contract Citation	**Redline of Proposed Modification**	**Detailed Explanation for the Request for Modification**
(section & page number)	(i.e., include text as published in RFP and use redlined strikethrough for words, phrases or sentences proposed to be deleted. Words, phrases or sentences proposed should be indicated by bold text and underlined.)	

FORM C – TECHNICAL REQUIREMENTS

This exhibit provides vendors the functional requirements that should be addressed in the proposal to meet the outlined needs of CSC Leon. Include this completed Form C behind Tab C of the Response.

It is the vendor's responsibility to understand the business issues presented, respond to the specific points, and clearly indicate whether their solution satisfies each requirement listed. When appropriate, the vendor should provide a more detailed explanation on how the solution specifically meets or does not meet the desired need in the narrative section immediately preceding the inclusion of Form C.

The vendor should respond to each of the requirements by indicating its ability to meet the requirement via (a) out of the box solution, (b) configuration or (c) customization. If a vendor cannot meet the requirement, it should indicate (d) not available. Vendors should be candid about their solution strengths and limitations and realistic in their responses and only choose one response per line. A description of each of the responses is provided below.

(a) **Out of the Box Solution** (OTB SOLUTION): The proposed solution/system platforms function currently exists as part of the Vendor's standard application and is in operation at a minimum of one client site.

(b) **Configuration** (CONFIG.): In order for the Vendor to meet this requirement, basic configuration is needed and will be provided at no additional cost. The Vendor is willing and able to provide this level of functionality and that the programming can be completed with minimal effort.

(c) **Customization** (CUSTOM.): In order for the Vendor to meet this requirement, custom programming would be needed, and it may incur additional costs. The time and costs associated with meeting this requirement is outlined in the corresponding narrative and budget worksheet.

(d) **Not Available** (NOT AVAIL.): This requirement cannot be met with the proposed solution and the Vendor does not currently have plans to provide this capability.

RFP for Integrated Information Management Solution
FORM C: TECHNICAL REQUIREMENTS

FEATURES LIST	OTS SOLUTION	CONFIG.	CUSTOM.	NOT AVAIL.
TECHNICAL				
Allow reports to be produced in multiple formats (e.g., Excel and PDF).				
Provide integration and import/export to Microsoft Office products.				
Provide integration with document management systems. Scan and attach documents, scanned images and MS Office files to records throughout all modules.				
Provide robust user interface for managing transaction and master file imports and exports in multiple file formats.				
Support report distribution (ideally web-based) without incurring additional license fees, including access security.				
Able to schedule reports to run at pre-defined time of the day.				
Support e-mailing scheduled reports or links to the previously run reports.				
Provide secure remote accessibility via the Internet, VPN, etc.				
Require strong passwords to be set at a minimum length and complexity.				
Provide a full transactional audit trail.				
Provide an interface for loading and extracting data to and from other systems (e.g., API calls, web services, etc.).				
Able to be hosted by a third party.				
Leverage Active Directory for user authentication.				
Support automatic forced password expiration and changes to user passwords at specific time intervals (e.g., 90-day expirations).				
Support multiple system instances/environments (e.g., test, QA, and production).				
Provide automated system archiving, purging, and backups.				
GENERAL FUNCTIONALITY				
Provide robust online documentation and user manuals.				
Provide complete drill-down and drill-across capabilities between the modules and transactions in the system.				
Provide role-based security by major function (role).				
Visibility to workflow status and approval queue.				
Support user-defined fields throughout the system and aid in customized functionality and reporting.				
Retain file attachments and source documents in electronic format (e.g., attach photos of damaged goods attributed to a sales order).				
Provide robust and configurable dashboards that display interactive content.				
Provide basic Business Intelligence (BI) and analytics capabilities.				
Facilitate data entry (e.g., field auto-completion, drop-down lists, etc.).				
Intuitive navigation for end users (e.g., desktop shortcuts).				
Provide a customer portal.				
Non-proprietary open reporting tools. List tools offered that are integrated with the system.				

FEATURES LIST	OTS SOLUTION	CONFIG.	CUSTOM.	NOT AVAIL.
User-level query and reporting tools that allow for formatting of data, headers, graphs, charts, etc.				
User-level security flows through to queries and reports.				
Drill down to source transactions within queries or reports following user-security rules.				
Schedule generation of reports and distribute via e-mail, to a shared folder or dashboard.				
Generate reports in multiple formats, e.g. HTML, PDF, Excel, Word, etc.				
Provide a robust report writer.				
GRANT MAKING & CONTRACT MANAGEMENT				
Agency Portal				
Ability to customize look and feel (branding) of Agency Portal				
Agency representatives can self-register for username/password				
Character limits within forms of applications				
Agency representatives can reset forgotten password				
CSC Leon can reset agency representative password				
Agency can edit contacts/users/deactivate old users				
System automatically checks EIN of agency when agency first registers. (Tax Status Verification against IRS Publication 78 and IRS Business Master File)				
Ability to enforce business rules (periodic agency profile updates)				
CSC Leon has ability to assign individualized permissions and associations for CSC team members				
Agency and CSC Leon has access to document repository, where documents can be uploaded and "turned on" agency by agency				
Visible to agency is a "countdown clock" that shows remaining time available for an agency to submit a proposal (response to a CSC Leon RFP). "Countdown clock" should be able to be applied to any process that requires an agency response (RFP response, quarterly reports, audits, etc.)				
Ability to store agency profile information, including: agency name, agency address, agency phone, agency staff names and contact info, agency staff contact codes/titles Import and export capabilities for all agency profile information				
CSC Leon assigned "administrator" able to set permissions for both CSC Leon staff and agency representatives				
System should support multiple programs per agency				
System should support multiple contacts/users per agency				
System prevents duplication of registered agencies. Each agency can only register once. System informs agency if they are already registered Distinctive names between agencies and programs.				
Distinctive names between agencies and programs.				
Programs created as separate entities, but information should be able to aggregate up to the agency entity level				
Customer Service				
Agency access to FAQs section via portal				
CSC Leon able to add/edit to FAQs section of portal				

RFP for Integrated Information Management Solution
FORM C: TECHNICAL REQUIREMENTS

FEATURES LIST	OTS SOLUTION	CONFIG.	CUSTOM.	NOT AVAIL.
CSC Leon staff able to broadcast/send announcements to agencies				
Announcement to appear on agency home page (visible when they first log in to the agency portal) (ie Communication Board)				
Ability to send bulk emails through portal				
Agency access to customizable resources on portal				
Agency access to Support (help desk) through established link on Agency home page				
User feedback sent to Administrators (QI)				
Procurement Development & Deployment				
CSC Leon able to build an RFP via a tool (online form, form builder)				
CSC Leon able to build content of RFP from content that was built for previous RFPs (copy and edit prior process)				
Include CSC Leon Publish RFP to select agencies via portal				
CSC Leon sets deadline for an agency to respond to RFP via portal				
Agency able to view RFP via portal				
Agency able to respond to RFP via portal by upload of required document(s) at both Agency and Program levels; one slot per required document, not a combined pdf or zipped file.				
RFPs should be able to be produced in form builder or from existing or already-created RFPs				
Automatic save feature for Agency responding to RFP when transitioning from one section to another when field entries have been made; Each page/screen should also have a manual Save button. Auto save feature in real time.				
Ability to convert sections or complete online RFP to preview and printer friendly PDF				
Agency access to FAQs				
Auto-save feature in real time, including calculations				
Portal Administrator has ability enable revisions after submission of form				
Proposal Review				
CSC Leon Staff ability to review and score proposals				
Council members able to review all proposals submitted				
CSC Leon staff should be able to create evaluation form with scoring for review of proposals; reviewer able to add notes attached to the agency submitted proposal				
Assigned outside-of-agency/External reviewers have ability to review and score proposals via portal				
Process of scoring proposals to include budget section to have column reflecting amounts requested in proposal by line item, column for recommended amount/amount to be awarded.				
Able to convert Budget section to Excel format/carry over budget to create allocation amounts by line item for contracting and allocations.				
Ability to create/build unique scoring tool for each RFP including ability to assign point values to each evaluation question with total review score.				

RFP for Integrated Information Management Solution
FORM C: TECHNICAL REQUIREMENTS

FEATURES LIST	OTS SOLUTION	CONFIG.	CUSTOM.	NOT AVAIL.
Ability to convert online evaluation form with responses to printer friendly pdf form.				
Security scan for malicious uploads				
Auto-save feature				
Contract Management				
CSC Leon able to publish contract via portal from MS Word/pdf format				
Agency able to access their particular contract(s)				
Agency able to view and download then upload signed contract				
Agency able to execute/sign contract electronically (i.e. Docusign integration)				
Integrate agency attestation with tick boxes for contract with attached budget and outcomes incorporated as part of contract				
Ability to connect approved RFP budget and outcomes to the contract				
Budgeting				
Ability to integrate line items budgets from proposal to establish line item budget allocations to include upload of supporting line item documentation with individual labels for multiple attachments				
Ability to use established line item budget allocations for roll over into annual contract				
Ability to report program budgets by priority areas for FY across proposal processes or funding streams				
Ability to export/exchange line item budget data from the CSC Leon evaluation process to the ERP system.				
Deliverables/Invoices				
Agency able to upload requests for payment along with multiple attachments				
Automatic Email notification of payment request to designated CSC Leon Team member(s)				
Ability for CSC Leon staff to view ongoing monthly payments, ytd totals, and remaining balances of line items.				
Ability to share/exchange budget data and expense data after contracting phase for use on agency/program dashboards to display up-to-date information regarding spendouts and remaining budget balances.				
PERFORMANCE MEASUREMENT **Data Collection & Reporting**				
Customizable reporting features (Report Builder) for System Querying and Reporting				
CSC Leon publishes participation (i.e. demographic) template				
Participation template able to collect multiple pieces of data to include				
• Population of Individual children, Group children, Individual adults, Group adults, families served each Quarter & YTD compared to targeted population goals.				
• Up to four outcomes per program w/ tracking of # served and # achieving the outcome per quarter & YTD				

FEATURES LIST	OTS SOLUTION	CONFIG.	CUSTOM.	NOT AVAIL.
• Progress field for narrative description of progress/steps toward achievement of each outcome				
Ability to track demographics (# served with subtotals by race/ethnicity, gender, age groupings, zip codes)				
Ability to track/display programs achieving 2 or more outcomes by quarter & YTD				
Ability to set “required”, “writable” or “read only” fields				
Ability to roll over data from one process to another (as in quarterly reports)				
Ability to schedule and record Site Visits including reports				
Import/Export/Integration capabilities with CRM and ERP				
Grantee outcomes evaluation – to capture progress on grant-specific milestones and intended outcomes.				
Programs Reporting				
Ability to roll over historical data to pre-populate forms				
Agency only able to report 1 quarter of information at a time				
All required items must be completed before submission is allowed.				
CSC Leon ability to open up and close reporting windows				
CSC Leon ability to lock previous quarter reported numbers to prevent agencies from modifying reported numbers (read only vs required field settings)				
CSC Leon ability to modify previous quarter reported numbers, based on CSC Leon staff member permissions (some staff prevented from changing agency-reported numbers)				
Quarterly reports saved historically for each quarter by Fiscal Year (FY); accessible by program or by quarter				
Able to attach files to slots for uploading information from program as part of reports (i.e. demographic tables, background screens, scans)				
Auto-save feature				
Ability to Archive data				
Customizable reporting features (Report Builder) for System Querying and Reporting				
Outcomes				
Grantee/Agency has ability to submit quarterly reporting				
Proposed Outcomes developed using documentation from outcome- services matrix in RFP				
CSC Leon staff sets final outcomes based upon proposal with ability to edit during the FY				
Ability to roll over proposed outcome data from grant proposal to annual contract with capacity to edit				
Ability to roll over proposed outcome data from grant proposal to quarterly report to establish baseline (Q1)				
Monitoring				
CSC Leon staff able to enter & track Contact-Progress-Review (C-P-R) notes by program using dates during the program year				
Metric for tracking C-P-R notes by days since last note (green for less than 30 days, yellow for 31 to 59 days, red more than 60 days since last entry)				

FEATURES LIST	OTS SOLUTION	CONFIG.	CUSTOM.	NOT AVAIL.
Program summary page for CSC Leon staff to see metrics for individual program				
Ability to sort/filter program information by priority funding areas				
Ability to give Programs access to Site Summary Report for their program.				
Ability to deactivate Agency and store data on portal and/or externally in Archive by fiscal year				
Dashboards				
Agency can monitor grant allocation balance via portal				
Agency can view outcomes via dashboard in portal				
Agency can view population served (number or % of contracted goal) via dashboard in portal				
Data represented in dashboard should be visible via pie charts, for awards (both present and historical). This should be available for viewing to both CSC Leon staff and agency representatives.				
Dashboards for Individual Outcomes should compare population achieving the outcome with population served for that outcome with % achieving quarterly and YTD.				
Dashboard visualizes historical and current agency data by program with ability to configure				
Other				
Product roadmap of system to view future planned development and updates to system (if yes, include URL where the product roadmap can be viewed)				
Form design and flexibility to allow application, reporting, and intake process forms to be fully managed and configured by CSC Team/designated Administrators				
CRM				
Classify CRM stakeholder records into different categories, such as "elected officials", "agency representative", "state government", etc.				
Automate task assignment and schedule follow-ups for CSC Leon staff members				
Track "touch points" as transactional for the sake of reporting and analysis.				
Integrate with other CSC Leon enterprise applications used specifically for grants management and accounting.				
Ability to "departmentalize" contacts within a single organization.				
Allow for a single contact to be associated with multiple organizations				
Allow for agency contacts to be associated to one or more "programs" of an organization.				
Allow for the recording of a single contact's roles with multiple organizations. For example, John Smith works at ABC Bank but also supports The School for Arts.				

FEATURES LIST		OTS SOLUTION	CONFIG.	CUSTOM.	NOT AVAIL.
	Ability to "Tag" conversation notes based on the conversation itself. Example, speaking with John Smith at ABC Bank about The School of Arts, tag conversation as relevant to both orgs Touch point classification that details method of contact, like phone, in person, text, etc.				
	Integrated text messaging (SMS send and receive)				
	Integrated task scheduling with MS Outlook, so that tasks and calendar entries can be managed on a single MS Outlook calendar.				
	MS Hosted Exchange email integration for the purpose of auto-generation of "touch points" and integration of data, like emails and email attachments.				
	Integration to email marketing for both distribution lists and touch points				
	Ability to search touch point by person but also by project or event				
	Mass distribution of event invitations and the recording of event attendance via RSVP functionality				
	Integration of site visit notes in both CRM and grants management solution.				
	Possible integration/dashboard of outcomes data directly in both the grants management, CRM and ERP				
	Possible integration of site review summaries for the sake of review by the board members. Board member instant access to site reviews.				
	Able to organize and manage multiple addresses per contact along with multiple contacts for each organization				
	Able to attach documents and emails to a customer master record.				
	Reporting/online inquiry for grants history and payment history.				
	Able to create ad-hoc stakeholder analysis report.				

CONTRACT FOR INTEGRATED INFORMATION MANAGEMENT SOLUTION

THIS CONTRACT (the “Contract”) is between the Children’s Services Council of Leon County (“CSC Leon”), an independent special district, and __________ (“Contractor”), a ____ (each individually a “Party” and collectively the “Parties”).

WHEREAS, Contractor responded to CSC Leon’s competitive solicitation entitled *Request for Proposals (RFP) Integrated Information Management Solution*; and,

WHEREAS, CSC Leon has relied on Contractor's proposal, and explanations and demonstrations thereof, to determine that the Contractor’s offer provides the best value to CSC Leon; and,

WHEREAS, the Parties desire to enter into the Contract pursuant to which Contractor will provide the services hereafter described.

NOW THEREFORE, in consideration of the premises set forth herein, the Parties agree as follows:

1. Definitions.

For the purposes of this Contract, the following terms have the following meanings:

“**Acceptance**” has the meaning set forth in Section 2.

“**Acceptance Tests**” means such tests as may be conducted in accordance with Section 2 and a Statement of Work to determine whether the Software meets the requirements of this Contract and the Documentation.

“**Affiliate**” of a Person means any other Person that directly or indirectly, through one or more intermediaries, controls, is controlled by, or is under common control with, such Person. For purposes of this definition, the term “control” (including the terms “controlled by” and “under common control with”) means the direct or indirect ownership of more than fifty percent (50%) of the voting securities of a Person.

“**Allegedly Infringing Materials**” has the meaning set forth in Section 18.

“**Approved Third Party Components**” means all third-party components, including OpenSource Components, that are included in or used in connection with the Software and are specifically identified by Contractor in the Proposal.

“**Authorized Users**” means all Persons authorized by CSC Leon to access and use the Software under this Contract, subject to the maximum number of users specified in the applicable Statement of Work.

“**Business Day**” means a day other than a Saturday, Sunday or other day on which CSC Leon is authorized or required by law to be closed for business.

“**Business Requirements Specification**” means the initial specification setting forth CSC Leon’s business requirements regarding the features and functionality of the Software, as set forth in a Statement of Work.

“Change” has the meaning set forth in Section 2.

“Change Notice” has the meaning set forth in Section 2.

“Change Proposal” has the meaning set forth in Section 2.

“Change Request” has the meaning set forth in Section 2.

“Confidential Information” has the meaning set forth in Section 22.1.

“**Configuration**” means CSC Leon-specific changes made to the Software without Source Code or structural data model changes occurring.

“**Contract**” has the meaning set forth in the preamble.

“**Contract Administrator**” is the individual appointed by each Party to (a) administer the terms of this Contract, and (b) approve any Change Notices under this Contract. Each Party’s Contract Administrator will be identified in Schedule A or subsequent Change Notices.

“**Contractor**” has the meaning set forth in the preamble.

“**Contractor Hosted**” means the Hosted Services are provided by Contractor or one or more of its Permitted Subcontractors.

“**Contractor Personnel**” means all employees of Contractor or any subcontractors or Permitted Subcontractors involved in the performance of Services hereunder.

“**Contractor Project Manager**” means the individual appointed by Contractor and identified in Schedule A or subsequent Change Notices to serve as the primary contact with regard to services, to monitor and coordinate the day-to-day activities of this Contract, and to perform other duties as may be further defined in this Contract, including an applicable Statement of Work.

“**CSC Leon Data**” has the meaning set forth in Section 21.1.

“**CSC Leon Materials**” means all materials and information, including but not limited to documents, data, know-how, ideas, methodologies, specifications, software, content and technology, in any form or media, directly or indirectly provided or made available to Contractor by or on behalf of CSC Leon in connection with this Contract.

“CSC Leon Project Managers” are the individuals appointed by CSC Leon, or their designees, to (a) monitor and coordinate the day-to-day activities of this Contract; (b) co-sign off on Acceptance of the Software and other Deliverables; and (c) perform other duties as may be specified in a Statement of Work. Project Managers will be identified in Schedule A or subsequent Change Notices.

“CSC Leon Systems” means the information technology infrastructure, including the computers, software, databases, electronic systems (including database management systems) and networks, of CSC Leon or any of its designees.

“**Customization**” means CSC Leon-specific changes to the Software's underlying Source Code or structural data model changes.

“**Deliverables**” means the Software, and all other documents and other materials that Contractor is required to or otherwise does provide to CSC Leon under this Contract and otherwise in connection with any Services, including all items specifically identified as Deliverables in a Statement of Work and all Work Product.

“**Deposit Material**” refers to material required to be deposited pursuant to Section 28.

“Disaster Recovery Plan” refers to the set(s) of documents, instructions, and procedures which enable the Contractor to respond to accidents, disasters, emergencies, or threats without any stoppage or hindrance in its key operations and to the actions the Contractor takes to meet the Recovery Point and Recovery Time Objectives.

“**Documentation**” means all user manuals, operating manuals, technical manuals and any other instructions, specifications, documents or materials, in any form or media, that describe the functionality, installation, testing, operation, use, maintenance, support, technical or other components, features or requirements of the Software.

“**Effective Date**” has the meaning set forth in Section 43.

“**Fees**” means the fees set forth in the Pricing Schedule attached as Schedule B.

“**Financial Audit Period**” has the meaning set forth in Section 23.

“**Harmful Code**” means any software, hardware or other technologies, devices or means, the purpose or effect of which is to: (a) permit unauthorized access to, or to destroy, disrupt, disable, encrypt, modify, copy, or otherwise harm or impede in any manner, any (i) computer, software, firmware, data, hardware, system or network, or (ii) any application or function of any of the foregoing or the integrity, use or operation of any data Processed thereby; or (b) prevent CSC Leon or any Authorized User from accessing or using the Services as intended by this Contract, and includes any virus, bug, trojan horse, worm, backdoor or other malicious computer code and any time bomb or drop dead device.

“**HIPAA**” has the meaning set forth in Section 2.

“**Hosted Services**” means the hosting, management and operation of the Operating Environment, Software, other services (including support and subcontracted services), and related resources for remote electronic access and use by CSC Leon and its Authorized Users, including any services and facilities related to disaster recovery obligations.

“**Implementation Plan**” means the schedule included in a Statement of Work setting forth the sequence of events for the performance of Services under a Statement of Work, including the Milestones and Milestone Dates.

“Integration Testing” has the meaning set forth in Section 9.

“**Intellectual Property Rights**” means all or any of the following: (a) patents, patent disclosures, and inventions (whether patentable or not); (b) trademarks, service marks, trade dress, trade names, logos, corporate names, and domain names, together with all of the associated goodwill; (c) copyrights and copyrightable works (including computer programs), mask works and rights in data and databases; (d) trade secrets, know-how and other confidential information; and (e) all other intellectual property rights, in each case whether registered or unregistered and including all applications for, and renewals or extensions of, such rights, and all similar or equivalent rights or forms of protection provided by applicable law in any jurisdiction throughout the world.

“**Key Personnel**” means any Contractor Personnel identified as key personnel in the Contract.

“**Loss or Losses**” means all losses, including but not limited to, damages, liabilities, deficiencies, claims, actions, judgments, settlements, interest, awards, penalties, fines, costs or expenses of whatever kind, including reasonable attorneys' fees and the costs of enforcing any right to indemnification hereunder and the cost of pursuing any insurance providers.

“**Maintenance Release**” means any update, upgrade, release or other adaptation or modification of the Software, including any updated Documentation, that Contractor may generally provide to its licensees from time to time during the Term, which may contain, among other things, error corrections, enhancements, improvements or other changes to the user interface, functionality, compatibility, capabilities, performance, efficiency or quality of the Software.

“**Milestone**” means an event or task described in the Implementation Plan under a Statement of Work that must be completed by the corresponding Milestone Date.

“**Milestone Date**” means the date by which a particular Milestone must be completed as set forth in the Implementation Plan under a Statement of Work.

“**New Version**” means any new version of the Software, including any updated

Documentation, that the Contractor may from time to time introduce and market generally as a distinct licensed product, as may be indicated by Contractor's designation of a new version number.

“**Nonconformity**” or **“Nonconformities”** means any failure or failures of the Software to conform to the requirements of this Contract, including any applicable Documentation.

“**Open-Source Components**” means any software component that is subject to any opensource copyright license agreement, including any GNU General Public License or GNU Library or Lesser Public License, or other obligation, restriction or license agreement that substantially conforms to the Open Source Definition as prescribed by the Open Source Initiative or otherwise may require disclosure or licensing to any third party of any source code with which such software component is used or compiled.

“**Operating Environment**” means, collectively, the platform, environment and conditions on, in or under which the Software is intended to be installed and operate, as set forth in a Statement of Work, including such structural, functional and other features, conditions and components as hardware, operating software, system architecture, configuration, computing hardware, ancillary equipment, networking, software, firmware, databases, data, and electronic systems (including database management systems).

“PAT” means a document or product accessibility template, including any Information Technology Industry Council Voluntary Product Accessibility Template or VPAT®, that specifies how information and software products, such as websites, applications, software and associated content, conform to WCAG 2.0 Level AA.

“**Permitted Subcontractor**” means any third party hired by Contractor to perform Services for CSC Leon under this Contract or have access to CSC Leon Data.

Exhibit 1
Page 5

“**Person**” means an individual, corporation, partnership, joint venture, limited liability company, governmental authority, unincorporated organization, trust, association or other entity.

“**Pricing Schedule**” means the schedule attached as Schedule B.

“Process” means to perform any operation or set of operations on any data, information, material, work, expression or other content, including to (a) collect, receive, input, upload, download, record, reproduce, store, organize, combine, log, catalog, cross-reference, manage, maintain, copy, adapt, alter, translate or make other improvements or derivative works, (b) process, retrieve, output, consult, use, disseminate, transmit, submit, post, transfer, disclose or otherwise provide or make available, or (c) block, erase or destroy. **“Processing”** and **“Processed”** have correlative meanings.

“**Proposal**” means the Contractor’s proposal submitted in response to the RFP.

“**Representatives**” means a Party's employees, officers, directors, partners, shareholders, agents, attorneys, successors and permitted assigns.

“**RFP**” means CSC Leon’s request for proposal designed to solicit responses for Services under this Contract.

“**Services**” means any of the services, including but not limited to, Hosted Services, Contractor is required to or otherwise does provide under this Contract.

“**Service Level Agreement**” means the schedule attached as Schedule D, setting forth the Support Services Contractor will provide to CSC Leon, and the Parties' additional rights and obligations with respect thereto.

“**Site**” means the physical location designated by CSC Leon in, or in accordance with, this Contract or a Statement of Work for delivery and installation of the Software.

“**Software**” means Contractor’s software as set forth in a Statement of Work, and any Maintenance Releases or New Versions provided to CSC Leon and any Customizations or Configurations made by or for CSC Leon pursuant to this Contract, and all copies of the foregoing permitted under this Contract.

“**Source Code**” means the human readable source code of the Software to which it relates, in the programming language in which the Software was written, together with all related flow charts and technical documentation, including a description of the procedure for generating object code, all of a level sufficient to enable a programmer reasonably fluent in such programming language to understand, build, operate, support, maintain and develop modifications, upgrades, updates, adaptations, enhancements, new versions and other derivative works and improvements of, and to develop computer programs compatible with, the Software.

"**Specifications**" means, for the Software, the specifications collectively set forth in the Business Requirements Specification, Technical Specification, Documentation, RFP or Proposal, if any, for such Software, or elsewhere in a Statement of Work.

"**State**" means the State of Florida.

"**Statement of Work**" means any statement of work entered into by the Parties and incorporated into this Contract. The initial Statement of Work is attached as Schedule A.

"**Stop Work Order**" has the meaning set forth in Section 15.

"**Support Services**" means the software maintenance and support services Contractor is required to or otherwise does provide to CSC Leon under the Service Level Agreement.

"**Technical Specification**" means, with respect to any Software, the document setting forth the technical specifications for such Software and included in a Statement of Work.

"**Term**" has the meaning set forth in Section 43.

"**Testing Period**" has the meaning set forth in Section 9.

"**Transition Period**" has the meaning set forth in Section 16.

"**Transition Responsibilities**" has the meaning set forth in Section 16.

"**Unauthorized Removal**" has the meaning set forth in Section 2.

"**Unauthorized Removal Credit**" has the meaning set forth in Section 2.

"**User Data**" means all data, information and other content of any type and in any format, medium or form, whether audio, visual, digital, screen, GUI or other, that is input, uploaded to, placed into or collected, stored, Processed, generated or output by any device, system or network by or on behalf of CSC Leon, including any and all works, inventions, data, analyses and other information and materials resulting from any use of the Software by or on behalf of CSC Leon under this Contract, except that User Data does not include the Software or data, information or content, including any GUI, audio, visual or digital or other display or output, that is generated automatically upon executing the Software without additional user input without the inclusion of user derived Information or additional user input.

"**Warranty Period**" means the ninety (90) calendar-day period commencing on the date of CSC Leon's Acceptance of the Software and for which Support Services are provided free of charge.

"WCAG 2.0 Level AA" means level AA of the World Wide Web Consortium Web Content Accessibility Guidelines version 2.0.

"**Work Product**" means all CSC Leon-specific deliverables that Contractor is required to, or otherwise does, provide to CSC Leon under this Contract including but not limited to customizations, application programming interfaces, computer scripts, macros, user interfaces, reports, project management documents, forms, templates, and other CSC Leon-specific documents and related materials together with all ideas, concepts, processes, and methodologies developed in connection with this Contract whether or not embodied in this Contract.

2. Duties of Contractor.

Contractor will provide Services and Deliverables pursuant to Statement(s) of Work entered into under this Contract. Contractor will provide all Services and Deliverables in a timely, professional manner and in accordance with the terms, conditions, and Specifications set forth in this Contract and Statement(s) of Work.

2.1 Statement of Work Requirements. No Statement of Work will be effective unless signed by each Party's Contract Administrator. The term of each Statement of Work will commence on the Parties' full execution of a Statement of Work and terminate when the Parties have fully performed their obligations. The terms and conditions of this Contract will apply at all times to any Statements of Work entered into by the Parties and incorporated into this Contract. CSC Leon will have the right to terminate such Statement of Work as set forth in **Section 16**. Contractor acknowledges that time is of the essence with respect to Contractor's obligations under each Statement of Work and agrees that prompt and timely performance of all such obligations in accordance with this Contract and Statements of Work (including the Implementation Plan and all Milestone Dates) is strictly required.

2.2 Change Control Process. CSC Leon may at any time request in writing (each, a "**Change Request**") changes to a Statement of Work, including changes to the Services and Implementation Plan (each, a "**Change**"). Upon CSC Leon's submission of a Change Request, the Parties will evaluate and implement all Changes in accordance with this section.

(a) As soon as reasonably practicable, and in any case within 20 Business Days following receipt of a Change Request, Contractor will provide CSC Leon with a written proposal for implementing the requested Change ("**Change Proposal**"), setting forth:

(i) a written description of the proposed Changes to any Services or Deliverables;
(ii) an amended Implementation Plan reflecting: (A) the schedule for commencing and completing any additional or modified Services or Deliverables; and (B) the effect of such Changes, if any, on completing any other Services under a Statement of Work;
(iii) any additional CSC Leon Resources Contractor deems necessary to carry out such Changes; and
(iv) any increase or decrease in Fees resulting from the proposed Changes, which increase or decrease will reflect only the increase or decrease in time and expenses Contractor requires to carry out the Change.

(b) Within 30 Business Days following CSC Leon's receipt of a Change Proposal, CSC Leon will by written notice to Contractor, approve, reject, or propose modifications to such Change Proposal. If CSC Leon proposes modifications, Contractor must modify and re-deliver the Change Proposal reflecting such modifications, or notify CSC Leon of any disagreement, in which event the Parties will negotiate in good faith to resolve their disagreement. Upon CSC Leon's approval of the Change Proposal or the Parties' agreement on all proposed modifications, as the case may be, the Parties will execute a written agreement to the Change Proposal ("**Change Notice**"), which Change Notice will be signed by CSC Leon's Contract Administrator and will constitute an amendment to a Statement of Work to which it relates; and

(c) If the Parties fail to enter into a Change Notice within 15 Business Days following CSC Leon's response to a Change Proposal, CSC Leon may, in its discretion:

(i) require Contractor to perform the Services under a Statement of Work without the Change;
(ii) require Contractor to continue to negotiate a Change Notice;
(iii) initiate a Dispute Resolution Procedure; or
(iv) notwithstanding any provision to the contrary in a Statement of Work, terminate this Contract under **Section 16.1**.

(d) No Change will be effective until the Parties have executed a Change Notice. Except as CSC Leon may request in its Change Request or otherwise in writing, Contractor must continue to perform its obligations in accordance with a Statement of Work pending negotiation and execution of a Change Notice. Contractor will use its best efforts to limit any delays or Fee increases from any Change to those necessary to perform the Change in accordance with the

Exhibit 1
Page 9

applicable Change Notice. Each Party is responsible for its own costs and expenses of preparing, evaluating, negotiating, and otherwise processing any Change Request, Change Proposal, and Change Notice.

(e) The performance of any functions, activities, tasks, obligations, roles and responsibilities comprising the Services as described in this Contract are considered part of the Services and, thus, will not be considered a Change. This includes the delivery of all Deliverables in accordance with their respective Specifications, and the diagnosis and correction of NonConformities discovered in Deliverables prior to their Acceptance by CSC Leon or, subsequent to their Acceptance by CSC Leon, as necessary for Contractor to fulfill its associated warranty requirements and its Support Services under this Contract.

(f) Contractor may, on its own initiative and at its own expense, prepare and submit its own Change Request to CSC Leon. However, CSC Leon will be under no obligation to approve or otherwise respond to a Change Request initiated by Contractor.

2.3 Contractor Personnel.

(a) Contractor is solely responsible for all Contractor Personnel and for the payment of their compensation, including, if applicable, withholding of income taxes, and the payment and withholding of social security and other payroll taxes, unemployment insurance, workers' compensation insurance payments and disability benefits.

(b) Prior to any Contractor Personnel performing any Services, Contractor will:

(i) ensure that such Contractor Personnel have the legal right to work in the United States;
(ii) upon request, require such Contractor Personnel to execute written agreements, in form and substance acceptable to CSC Leon, that bind such Contractor Personnel to confidentiality provisions that are at least as protective of CSC Leon's information (including all Confidential Information) as those contained in this Contract; and
(iii) upon request, or as otherwise specified in a Statement of Work, perform background checks on all Contractor Personnel prior to their assignment. The scope is at the discretion of CSC Leon and documentation must be provided as requested. Contractor is responsible for all costs associated with the requested background checks. CSC Leon, in its sole discretion, may also perform background checks.

(c) Contractor and all Contractor Personnel will comply with all rules, regulations, and policies of CSC Leon that are communicated to Contractor in writing, including security procedures concerning systems and data and remote access, building security procedures, including the restriction of access by CSC Leon to certain areas of its premises or systems, and general health and safety practices and procedures.

(d) CSC Leon reserves the right to require the removal of any Contractor Personnel found, in the judgment of CSC Leon, to be unacceptable. CSC Leon’s request must be written with reasonable detail outlining the reasons for the removal request. Replacement personnel for the removed person must be fully qualified for the position. If CSC Leon exercises this right, and Contractor cannot immediately replace the removed personnel, CSC Leon agrees to negotiate an equitable adjustment in schedule or other terms that may be affected by CSC Leon’s required removal.

2.4 Contractor Project Manager. Throughout the Term of this Contract, Contractor must maintain a Contractor employee acceptable to CSC Leon to serve as Contractor Project Manager, who will be considered Key Personnel of Contractor.

(a) Contractor Project Manager must:

(i) have the requisite authority, and necessary skill, experience, and qualifications, to perform in such capacity;
(ii) be responsible for overall management and supervision of Contractor’s performance under this Contract; and
(iii) be CSC Leon’s primary point of contact for communications with respect to this Contract, including with respect to giving and receiving all day-to-day approvals and consents.

(b) Contractor Project Manager must attend all regularly scheduled meetings as set forth in the Implementation Plan and will otherwise be available as set forth in a Statement of Work.

(c) Contractor will maintain the same Contractor Project Manager throughout the Term of this Contract, unless:

(i) CSC Leon requests in writing the removal of Contractor Project Manager;
(ii) CSC Leon consents in writing to any removal requested by Contractor in writing;
(iii) Contractor Project Manager ceases to be employed by Contractor, whether by resignation, involuntary termination or otherwise.

(d) Contractor will promptly replace its Contractor Project Manager on the occurrence of any event set forth in **Section 2.5**. Such replacement will be subject to CSC Leon's prior written approval.

2.5 <u>Contractor’s Key Personnel</u>.

(a) CSC Leon has the right to recommend and approve in writing the initial assignment, as well as any proposed reassignment or replacement, of any Key Personnel. Before assigning an individual to any Key Personnel position, Contractor will notify CSC Leon of the proposed assignment, introduce the individual to CSC Leon Program Managers or their designees, and provide CSC Leon with a resume and any other information about the individual reasonably requested by CSC Leon. CSC Leon reserves the right to interview the individual before granting written approval. In the event CSC Leon finds a proposed individual unacceptable, CSC Leon will provide a written explanation including reasonable detail outlining the reasons for the rejection.

(b) Contractor will not remove any Key Personnel from their assigned roles on this Contract without the prior written consent of CSC Leon. The Contractor’s removal of Key Personnel without the prior written consent of CSC Leon is an unauthorized removal (“Unauthorized Removal”). An Unauthorized Removal does not include replacing Key Personnel for reasons beyond the reasonable control of Contractor, including illness, disability, leave of absence, personal emergency circumstances, resignation, or for cause termination of the Key Personnel’s employment. Any Unauthorized Removal may be considered by CSC Leon to be a material breach of this Contract, in respect of which CSC Leon may elect to terminate this Contract for cause under **Section 16.1**.

(c) It is further acknowledged that an Unauthorized Removal will interfere with the timely and proper completion of this Contract, to the loss and damage of CSC Leon, and that it would be impracticable and extremely difficult to determine and remedy the actual damage sustained by CSC Leon as a result of any Unauthorized Removal. Therefore, Contractor and CSC Leon agree that in the case of any Unauthorized Removal in respect of which CSC Leon does not elect to exercise its rights under Section 16, Contractor will issue to CSC Leon an amount equal to $25,000 per individual (each, an “Unauthorized Removal Credit”).

(d) Contractor acknowledges and agrees that each of the Unauthorized Removal Credits assessed under **SECTION XX** above: (i) is a reasonable estimate of and compensation for the anticipated or actual harm to CSC Leon that may arise from the Unauthorized Removal, which would be impossible or very difficult to accurately estimate; and (ii) may, at CSC Leon’s option, be credited or set off against any Fees or other charges payable to Contractor under this Contract.

2.6 Subcontractors. Contractor must obtain prior written approval of CSC Leon, which consent may be given or withheld in CSC Leon's sole discretion, before engaging any Permitted Subcontractor to provide Services to CSC Leon under this Contract. Third parties otherwise retained by Contractor to provide Contractor or other clients of contractor with services are not Permitted Subcontractors, and therefore do not require prior approval by CSC Leon.

Engagement of any subcontractor or Permitted Subcontractor by Contractor does not relieve Contractor of its representations, warranties or obligations under this Contract. Without limiting the foregoing, Contractor will:

(a) be responsible and liable for the acts and omissions of each such subcontractor (including such Permitted Subcontractor and Permitted Subcontractor's employees who, to the extent providing Services or Deliverables, will be deemed Contractor Personnel) to the same extent as if such acts or omissions were by Contractor or its employees;

(b) name CSC Leon a third-party beneficiary under Contractor's Contract with each Permitted Subcontractor with respect to the Services;

(c) be responsible for all fees and expenses payable to, by or on behalf of each Permitted Subcontractor in connection with this Contract, including, if applicable, withholding of income taxes, and the payment and withholding of social security and other payroll taxes, unemployment insurance, workers' compensation insurance payments and disability benefits; and

(d) notify CSC Leon of the location of the Permitted Subcontractor and indicate if it is located within the continental United States.

3. Notices.

All notices and other communications required or permitted under this Contract must be in writing and will be considered given and received: (a) when verified by written receipt if sent by courier; (b) when actually received if sent by mail without verification of receipt; or (c) when verified by automated receipt or electronic logs if sent by facsimile or email.

If to CSC Leon:	If to Contractor:
Jacinta Clay, Administrative Services Manager P.O. Box 1816	[Name] [Street Address] [City, State, Zip]

Tallahassee, FL 32302	

4. Insurance.

Contractor must maintain the minimum insurances identified in the Insurance Schedule attached as **Schedule C**.

5. Software License.

5.1 Perpetual License. If Contractor is providing CSC Leon with a license to use its Software indefinitely, then Contractor hereby grants to CSC Leon and its Authorized Users a nonexclusive, royalty-free, perpetual, irrevocable right and license to use the Software and Documentation in accordance with the terms and conditions of this Contract, provided that:

(a) CSC Leon is prohibited from reverse engineering or decompiling the Software, making derivative works, modifying, adapting or copying the Software except as is expressly permitted by this Contract or required to be permitted by law;
(b) CSC Leon is authorized to make copies of the Software for backup, disaster recovery, and archival purposes;
(c) CSC Leon is authorized to make copies of the Software to establish a test environment to conduct Acceptance Testing;
(d) Title to and ownership of the Software shall at all times remain with Contractor
(e) and/or it’s licensors, as applicable; and
(f) Except as expressly agreed in writing, CSC Leon is not permitted to sub-license the use of the Software or any accompanying Documentation.

5.2 Subscription License. If the Software is Contractor Hosted and Contractor is providing CSC Leon access to use its Software during the Term of the Contract only, then:

(a) Contractor hereby grants to CSC Leon, exercisable by and through its Authorized Users, a nonexclusive, royalty-free, irrevocable right and license during the Term and such additional periods, if any, as Contractor is required to perform Services under this Contract or any Statement of Work, to:

(i) access and use the Software, including in operation with other software, hardware, systems, networks and services, for CSC Leon’s business purposes, including for Processing CSC Leon Data;
(ii) generate, print, copy, upload, download, store and otherwise Process all GUI, audio, visual, digital and other output, displays and other content as may result from any access to or use of the Software;

(iii) prepare, reproduce, print, download and use a reasonable number of copies of the Specifications and Documentation for any use of the Software under this Contract; and

(iv) access and use the Software for all such non-production uses and applications as may be necessary or useful for the effective use of the Software hereunder, including for purposes of analysis, development, configuration, integration, testing, training, maintenance, support and repair, which access and use will be without charge and not included for any purpose in any calculation of CSC Leon's or its Authorized Users' use of the Software, including for purposes of assessing any Fees or other consideration payable to Contractor or determining any excess use of the Software as described in **Section 5.2(c)** below.

(b) *License Restrictions*. CSC Leon will not: (a) rent, lease, lend, sell, sublicense, assign, distribute, publish, transfer or otherwise make the Software available to any third party, except as expressly permitted by this Contract or in any Statement of Work; or (b) use or authorize the use of the Software or Documentation in any manner or for any purpose that is unlawful under applicable Law.

(c) *Use*. CSC Leon will pay Contractor the corresponding Fees set forth in a Statement of Work or Pricing Schedule for all Authorized Users access and use of the Software. Such Fees will be Contractor's sole and exclusive remedy for use of the Software, including any excess use.

5.3 Certification. To the extent that a License granted to CSC Leon is not unlimited, Contractor may request written certification from CSC Leon regarding use of the Software for the sole purpose of verifying compliance with this SECTION XX. Such written certification may occur no more than once in any 24 month period during the Term of the Contract. CSC Leon will respond to any such request within 45 calendar days of receipt. If CSC Leon's use is greater than contracted, Contractor may invoice CSC Leon for any unlicensed use (and related support) pursuant to the terms of this Contract at the rates set forth in Schedule B, and the unpaid license and support fees shall be payable in accordance with the terms of the Contract. Payment under this provision shall be Contractor's sole and exclusive remedy to cure these issues.

5.4 CSC Leon License Grant to Contractor. CSC Leon hereby grants to Contractor a limited, non-exclusive, non- transferable license (i) to use CSC Leon's name, trademarks, service marks or logos, solely in accordance with CSC Leon's specifications, and (ii) to display, reproduce, distribute and transmit in digital form CSC Leon's name, trademarks, service marks or logos in connection with promotion of the Services as communicated to Contractor by CSC Leon. Use of CSC Leon's name, trademarks, service marks or logos will be specified in the applicable Statement of Work**.** Contractor is provided a limited license to CSC Leon Materials for the sole and exclusive purpose of providing the

Services.

6. Third Party Components.

At least 30 days prior to adding new Third-Party Components, Contractor will provide CSC Leon with notification information identifying and describing the addition. Throughout the Term, on an annual basis, Contractor will provide updated information identifying and describing any Approved Third-Party Components included in the Software.

7. Intellectual Property Rights.

7.1 Ownership Rights in Software.

(a) For purposes of this section only, the term "Software" does not include Customizations.

(b) Subject to the rights and licenses granted by Contractor in this Contract and the provisions of SECTION XX(c):

(i) Contractor reserves and retains its entire right, title and interest in and to all Intellectual Property Rights arising out of or relating to the Software; and

(ii) none of CSC Leon or Authorized Users acquire any ownership of Intellectual Property Rights in or to the Software or Documentation as a result of this Contract.

(c) As between CSC Leon, on the one hand, and Contractor, on the other hand, CSC Leon has, reserves and retains, sole and exclusive ownership of all right, title and interest in and to CSC Leon Materials, User Data, including all Intellectual Property Rights arising therefrom or relating thereto.

7.2 CSC Leon is and will be the sole and exclusive owner of all right, title, and interest in and to all Work Product developed exclusively for CSC Leon under this Contract, including all Intellectual Property Rights. In furtherance of the foregoing:

(a) Contractor will create all Work Product as work made for hire as defined in Section 101 of the Copyright Act of 1976; and

(b) to the extent any Work Product, or Intellectual Property Rights do not qualify as, or otherwise fails to be, work made for hire, Contractor hereby:

(i) assigns, transfers, and otherwise conveys to CSC Leon, irrevocably and in perpetuity, throughout the universe, all right, title, and interest in and to such Work Product, including all Intellectual Property Rights; and

(ii) irrevocably waives any and all claims Contractor may now or hereafter have in any jurisdiction to so-called “moral rights” or rights of *droit moral* with respect to the Work Product.

8. Software Implementation.

8.1 Implementation. Contractor will as applicable; deliver, install, configure, integrate, and otherwise provide and make fully operational the Software on or prior to the applicable Milestone Date in accordance with the criteria set forth in a Statement of Work and the Implementation Plan.

8.2 Site Preparation. Unless otherwise set forth in a Statement of Work, Contractor is responsible for ensuring the relevant Operating Environment is set up and in working order to allow Contractor to deliver and install the Software on or prior to the applicable Milestone Date. Contractor will provide CSC Leon with such notice as is specified in a Statement of Work, prior to delivery of the Software to give CSC Leon sufficient time to prepare for Contractor’s delivery and installation of the Software. If CSC Leon is responsible for Site preparation, Contractor will provide such assistance as CSC Leon requests to complete such preparation on a timely basis.

9. Software Acceptance Testing.

9.1 Acceptance Testing.

(a) Unless otherwise specified in a Statement of Work, upon installation of the Software, or in the case of Contractor Hosted Software, when Contractor notifies CSC Leon in writing that the Hosted Services are ready for use in a production environment, Acceptance Tests will be conducted as set forth in this section to ensure the Software conforms to the requirements of this Contract, including the applicable Specifications and Documentation.

(b) All Acceptance Tests will take place at the designated Site(s) in the Operating Environment described in a Statement of Work, commence on the Business Day following installation of the Software, or the receipt by CSC Leon of the notification and be conducted diligently for up to 30 Business Days, or such other period as may be set forth in a Statement of Work (the “**Testing Period**”). Acceptance Tests will be conducted by the Party responsible as set forth in a Statement of Work or, if a Statement of Work does not specify, CSC Leon, provided that:

(i) for Acceptance Tests conducted by CSC Leon, if requested by CSC Leon, Contractor will make suitable Contractor Personnel available to observe or participate in such Acceptance Tests; and

(ii) for Acceptance Tests conducted by Contractor, CSC Leon has the right to observe or participate in all or any part of such Acceptance Tests.

9.2 Contractor is solely responsible for all costs and expenses related to Contractor’s performance of, participation in, and observation of Acceptance Testing.

(a) Upon delivery and installation of any application programming interfaces, Configuration or Customizations, or any other applicable Work Product, to the Software under a Statement of Work, additional Acceptance Tests will be performed on the modified Software as a whole to ensure full operability, integration, and compatibility among all elements of the Software (“Integration Testing”). Integration Testing is subject to all procedural and other terms and conditions set forth in this section.

(b) CSC Leon may suspend Acceptance Tests and the corresponding Testing Period by written notice to Contractor if CSC Leon discovers a material Non-Conformity in the tested Software or part or feature of the Software. In such event, Contractor will immediately, and in any case within 10 Business Days, correct such Non-Conformity, whereupon the Acceptance Tests and Testing Period will resume for the balance of the Testing Period.

9.3 Notices of Completion, Non-Conformities, and Acceptance. Within 15 Business Days following the completion of any Acceptance Tests, including any Integration Testing, the Party responsible for conducting the tests will prepare and provide to the other Party written notice of the completion of the tests. Such notice must include a report describing in reasonable detail the tests conducted and the results of such tests, including any uncorrected Non-Conformity in the tested Software.

(a) If such notice is provided by either Party and identifies any Non-Conformities, the Parties’ rights, remedies, and obligations will be as set forth in **Section 2.**

(b) If such notice is provided by CSC Leon, is signed by CSC Leon Program Managers or their designees, and identifies no Non-Conformities, such notice constitutes CSC Leon's Acceptance of such Software.

(c) If such notice is provided by Contractor and identifies no Non-Conformities, CSC Leon will have 30 Business Days to use the Software in the Operating Environment and determine, in the exercise of its sole discretion, whether it is satisfied that the Software contains no Non-Conformities, on the completion of which CSC Leon will, as appropriate:

(i) notify Contractor in writing of Non-Conformities CSC Leon has observed in the Software and of CSC Leon’s non-acceptance thereof, whereupon the Parties' rights, remedies and obligations will be as set forth in **SECTION XX** and **SECTION XX**; or

(ii) provide Contractor with a written notice of its Acceptance of such Software, which must be signed by CSC Leon Project Manager or their designees.

9.4 Failure of Acceptance Tests. If Acceptance Tests identify any Non-Conformities, Contractor, at Contractor's sole cost and expense, will remedy all such Non-Conformities and re-deliver the Software, in accordance with the requirements set forth in the Contract. Redelivery will occur as promptly as commercially possible and, in any case, within 30 Business Days following, as applicable, Contractor's:

(a) completion of such Acceptance Tests, in the case of Acceptance Tests conducted by Contractor; or

(b) receipt of CSC Leon's notice, identifying any Non-Conformities.

9.5 Repeated Failure of Acceptance Tests. If Acceptance Tests identify any Non-Conformity in the Software after a second or subsequent delivery of the Software, or Contractor fails to redeliver the Software on a timely basis, CSC Leon may, in its sole discretion, by written notice to Contractor:

(a) continue the process set forth in this **SECTION XX**;

(b) accept the Software as a nonconforming deliverable, in which case the Fees for such Software will be reduced equitably to reflect the value of the Software as received relative to the value of the Software had it conformed; or

(c) deem the failure to be a non-curable material breach of this Contract and a Statement of Work and terminate this Contract for cause in accordance with **Section 16.1**.

9.6 Acceptance. Acceptance ("Acceptance") of the Software (subject, where applicable, to CSC Leon's right to Integration Testing) will occur on the date that is the earliest of CSC Leon's delivery of a notice accepting the Software under **SECTION XX**, or **SECTION XX**.

10. Non-Software Acceptance.

10.1 All other non-Software Services and Deliverables are subject to inspection and testing by CSC Leon within 30 calendar days of CSC Leon's receipt of them ("State Review Period"), unless otherwise provided in Statement of Work. If the non-Software Services and Deliverables are not fully accepted by CSC Leon, CSC Leon will notify Contractor by the end of CSC Leon Review Period that either: (a) the non-Software Services and

Deliverables are accepted but noted deficiencies must be corrected; or (b) the non-Software Services and Deliverables are rejected. If CSC Leon finds material deficiencies, it may: (i) reject the non-Software Services and Deliverables without performing any further inspections; (ii) demand performance at no additional cost; or (iii) terminate this Contract in accordance with **Section 16.1**, Termination for Cause.

10.2 Within 10 business days from the date of Contractor's receipt of notification of acceptance with deficiencies or rejection of any non-Software Services and Deliverables, Contractor must cure, at no additional cost, the deficiency and deliver unequivocally acceptable non-Software Services and Deliverables to CSC Leon. If acceptance with deficiencies or rejection of the non-Software Services and Deliverables impacts the content or delivery of other noncompleted non-Software Services and Deliverables, the Parties' respective Program Managers must determine an agreed to number of days for re-submission that minimizes the overall impact to the Contract. However, nothing herein affects, alters, or relieves Contractor of its obligations to correct deficiencies in accordance with the time response standards set forth in this Contract.

10.3 If Contractor is unable or refuses to correct the deficiency within the time response standards set forth in this Contract, CSC Leon may cancel the order in whole or in part. CSC Leon, or a third party identified by CSC Leon, may provide the non-Software Services and Deliverables and recover the difference between the cost to cure and the Contract price plus an additional 10% administrative fee.

11. Assignment.

Contractor may not assign this Contract to any other party without the prior approval of CSC Leon. Upon notice to Contractor, CSC Leon, in its sole discretion, may assign in whole or in part, its rights or responsibilities under this Contract to any other party. If CSC Leon determines that a novation of the Contract to a third party is necessary, Contractor will agree to the novation and provide all necessary documentation and signatures.

12. Change of Control.

Contractor will notify CSC Leon, within 30 days of any public announcement or otherwise once legally permitted to do so, of a change in Contractor's organizational structure or ownership. For purposes of this Contract, a change in control means any of the following:

(a) a sale of more than 50% of Contractor's stock;
(b) a sale of substantially all of Contractor's assets;
(c) a change in a majority of Contractor's board members;
(d) consummation of a merger or consolidation of Contractor with any other entity;
(e) a change in ownership through a transaction or series of transactions;
(f) or the board (or the stockholders) approves a plan of complete liquidation.

A change of control does not include any consolidation or merger effected exclusively to change the domicile of Contractor, or any transaction or series of transactions principally for bona fide equity financing purposes. In the event of a change of control, Contractor must require the successor to assume this Contract and all of its obligations under this Contract.

13. Invoices and Payment.

13.1 Invoices must conform to the requirements communicated from time-to-time by CSC Leon. All undisputed amounts are payable within 45 days of CSC Leon's receipt. Contractor may only charge for Services and Deliverables provided as specified in Statement(s) of Work. Invoices must include an itemized statement of all charges.

13.2 CSC Leon has the right to withhold payment of any disputed amounts until the Parties agree as to the validity of the disputed amount. CSC Leon will notify Contractor of any dispute within a reasonable time. Payment by CSC Leon will not constitute a waiver of any rights as to Contractor's continuing obligations, including claims for deficiencies or substandard Services and Deliverables. Contractor's acceptance of final payment by CSC Leon constitutes a waiver of all claims by Contractor against CSC Leon for payment under this Contract, other than those claims previously filed in writing on a timely basis and still disputed.

13.3 Payment of invoices is governed by the Local Government Prompt Payment Act, sections 281.70 *et seq*., Florida Statutes.

13.4 <u>Right of Setoff</u>. Without prejudice to any other right or remedy it may have, CSC Leon reserves the right to set off at any time any amount then due and owing to it by Contractor against any amount payable by CSC Leon to Contractor under this Contract.

13.5 <u>Taxes</u>. CSC Leon is exempt from State sales tax for direct purchases and may be exempt from federal excise tax, if Services or Deliverables purchased under this Contract are for CSC Leon's exclusive use. Notwithstanding the foregoing, all Fees are exclusive of taxes, and Contractor is responsible for all sales, use and excise taxes, and any other similar taxes, duties and charges of any kind imposed by any federal, state, or local governmental entity on any amounts payable by CSC Leon under this Contract.

13.6 <u>Pricing/Fee Changes</u>. All Pricing set forth in this Contract will not be increased, except as otherwise expressly provided in this Section.

(a) The Fees will not be increased at any time except for the addition of additional licenses, the fees for which licenses will also remain firm in accordance with the Pricing set forth in the Pricing Schedule.

(b) Excluding federal government charges and terms. Contractor warrants and agrees that each of the Fees, economic or product terms or warranties granted pursuant to this Contract are comparable to or better than the equivalent fees, economic or product term or warranty being offered to any commercial or government customer (including any public educational institution within the State) of Contractor. If Contractor enters into any arrangements with another customer of Contractor to provide the products or services, available under this Contract, under more favorable prices, as the prices may be indicated on Contractor's current U.S. and International price list or comparable document, then this Contract will be deemed amended as of the date of such other arrangements to incorporate those more favorable prices, and Contractor will immediately notify CSC Leon of such Fee and formally memorialize the new pricing in a Change Notice.

14. Liquidated Damages.

14.1 The Parties understand and agree that any liquidated damages (which includes but is not limited to applicable credits) set forth in this Contract are reasonable estimates of CSC Leon's damages in accordance with applicable law.

14.2 The Parties acknowledge and agree that Contractor could incur liquidated damages for more than one event.

14.3 The assessment of liquidated damages will not constitute a waiver or release of any other remedy CSC Leon may have under this Contract for Contractor's breach of this Contract, including without limitation, CSC Leon's right to terminate this Contract for cause under **Section 16.1** and CSC Leon will be entitled in its discretion to recover actual damages caused by Contractor's failure to perform its obligations under this Contract. However, CSC Leon will reduce such actual damages by the amounts of liquidated damages received for the same events causing the actual damages.

14.4 Amounts due CSC Leon as liquidated damages may be set off against any Fees payable to Contractor under this Contract, or CSC Leon may bill Contractor as a separate item and Contractor will promptly make payments on such bills.

15. Stop Work Order.

CSC Leon may suspend any or all activities under the Contract at any time. CSC Leon will provide Contractor a written stop work order detailing the suspension. Contractor must comply with the stop work order upon receipt. Within 90 calendar days, or any longer period agreed to by Contractor, CSC Leon will either:

(a) issue a notice authorizing Contractor to resume work, or

(b) terminate the Contract or delivery order. CSC Leon will not pay for activities that have been suspended, Contractor's lost profits, or any additional compensation during a stop work period.

16. Termination, Expiration, Transition.

CSC Leon may terminate this Contract, the Support Services, or any Statement of Work, in accordance with the following:

16.1 Termination for Cause. In addition to any right of termination set forth elsewhere in this Contract:

(a) CSC Leon may terminate this Contract for cause, in whole or in part, if Contractor, as determined by CSC Leon:

(i) endangers the value, integrity, or security of CSC Leon Systems, CSC Leon Data, or CSC Leon's facilities or personnel;

(ii) becomes insolvent, petitions for bankruptcy court proceedings, or has an involuntary bankruptcy proceeding filed against it by any creditor; or

(iii) breaches any of its material duties or obligations under this Contract. Any reference to specific breaches being material breaches within this Contract will not be construed to mean that other breaches are not material.

(b) If CSC Leon terminates this Contract under this **Section 16.1**, CSC Leon will issue a termination notice specifying whether Contractor must:

(i) cease performance immediately. Contractor must submit all invoices for Services accepted by CSC Leon within 30 days of the date of termination. Failure to submit an invoice within that timeframe will constitute a waiver by Contractor for any amounts due to Contractor for Services accepted by CSC Leon under this Contract, or

(ii) continue to perform for a specified period. If it is later determined that Contractor was not in breach of this Contract, the termination will be deemed to have been a termination for convenience, effective as of the same date, and the rights and obligations of the Parties will be limited to those provided in **Section 16.2**.

(c) CSC Leon will only pay for amounts due to Contractor for Services accepted by CSC Leon on or before the date of termination, subject to CSC Leon's right to set off any amounts owed by the Contractor for CSC Leon's reasonable costs in terminating this Contract. Contractor must promptly reimburse to CSC Leon any Fees prepaid by CSC Leon prorated to the date of such termination, including any prepaid Fees. Contractor must pay all reasonable costs incurred by CSC Leon in terminating this Contract for cause, including administrative costs, attorneys' fees, court costs, transition costs, and any costs CSC Leon incurs to procure the Services from other sources.

16.2 <u>Termination for Convenience</u>. CSC Leon may immediately terminate this Contract in whole or in part, without penalty and for any reason or no reason, including but not limited to, appropriation or budget shortfalls. The termination notice will specify whether Contractor must:

(a) cease performance immediately. Contractor must submit all invoices for Services accepted by CSC Leon within 30 days of the date of termination. Failure to submit an invoice within that timeframe will constitute a waiver by Contractor for any amounts due to Contractor for Services accepted by CSC Leon under this Contract, or

(b) continue to perform in accordance with **Section 16.3**. If CSC Leon terminates this Contract for convenience, CSC Leon will pay all reasonable costs, as determined by CSC Leon, for CSC Leon approved Transition Responsibilities to the extent the funds are available.

16.3 <u>Transition Responsibilities</u>.

(a) Upon termination or expiration of this Contract for any reason, Contractor must, for a period of time specified by CSC Leon (not to exceed 90 calendar days; the "**Transition Period**"), provide all reasonable transition assistance requested by CSC Leon, to allow for the expired or terminated portion of the Contract to continue without interruption or adverse effect, and to facilitate the orderly transfer of the Services to CSC Leon or its designees. Such transition assistance may include but is not limited to:

(i) continuing to perform the Services at the established Contract rates;

(ii) taking all reasonable and necessary measures to transition performance of the work, including all applicable Services to CSC Leon or CSC Leon's designee;

(iii) taking all necessary and appropriate steps, or such other action as CSC Leon may direct, to preserve, maintain, protect, and comply with **Section 22.5** regarding the return or destruction of CSC Leon Data at the conclusion of the Transition Period; and

(iv) preparing an accurate accounting from which CSC Leon and Contractor may reconcile all outstanding accounts (collectively, the "**Transition Responsibilities**"). The Term of this Contract is automatically extended through the end of the Transition Period.

(b) Contractor will follow the transition plan attached as **Schedule G** as it pertains to both transition in and transition out activities.

17. Indemnification

17.1 General Indemnification. Contractor must defend, indemnify and hold CSC Leon, its officers, and employees harmless, without limitation, from and against any and all actions, claims, losses, liabilities, damages, costs, attorney fees, and expenses (including those required to establish the right to indemnification), arising out of or relating to:

(a) any breach by Contractor (or any of Contractor's employees, agents, subcontractors, or by anyone else for whose acts any of them may be liable) of any of the promises, agreements, representations, warranties, or insurance requirements contained in this Contract;

(b) any infringement, misappropriation, or other violation of any Intellectual Property Right or other right of any third party;

(c) any bodily injury, death, or damage to real or tangible personal property occurring wholly or in part due to action or inaction by Contractor (or any of Contractor's employees, agents, subcontractors, or by anyone else for whose acts any of them may be liable); and

(d) any acts or omissions of Contractor (or any of Contractor's employees, agents, subcontractors, or by anyone else for whose acts any of them may be liable).

17.2 Indemnification Procedure. CSC Leon will notify Contractor in writing if indemnification is sought; however, failure to do so will not relieve Contractor, except to the extent that Contractor is materially prejudiced. Contractor must, to the satisfaction of CSC Leon, demonstrate its financial ability to carry out these obligations. CSC Leon is entitled to:

(a) regular updates on proceeding status;
(b) participate in the defense of the proceeding;
(c) employ its own counsel; and to
(d) retain control of the defense, at its own cost and expense, if CSC Leon deems necessary. Contractor will not, without CSC Leon's prior written consent (not to be unreasonably withheld), settle, compromise, or consent to the entry of any judgment in or otherwise seek to terminate any claim, action, or proceeding.

18. Infringement Remedies.

18.1 The remedies set forth in this Section are in addition to, and not in lieu of, all other remedies that may be available to CSC Leon under this Contract or otherwise, including CSC Leon's right to be indemnified for such actions.

18.2 If any Software or any component thereof, other than CSC Leon Materials, is found to be infringing or if any use of any Software or any component thereof is enjoined, threatened to be enjoined or otherwise the subject of an infringement claim, Contractor must, at Contractor's sole cost and expense:

(a) procure for CSC Leon the right to continue to use such Software or component thereof to the full extent contemplated by this Contract; or

(b) modify or replace the materials that infringe or are alleged to infringe ("**Allegedly Infringing Materials**") to make the Software and all of its components non-infringing while providing fully equivalent features and functionality.

18.3 If neither of the foregoing is possible notwithstanding Contractor's best efforts, then Contractor may direct CSC Leon to cease any use of any materials that have been enjoined or finally adjudicated as infringing, provided that Contractor will:

(a) refund to CSC Leon all amounts paid by CSC Leon in respect of such Allegedly Infringing Materials and any other aspects of the Software provided under a Statement of Work for the Allegedly Infringing Materials that CSC Leon cannot reasonably use as intended under this Contract; and

(b) in any case, at its sole cost and expense, secure the right for CSC Leon to continue using the Allegedly Infringing Materials for a transition period of up to 6 months to allow CSC Leon to replace the affected features of the Software without disruption.

18.4 If Contractor directs CSC Leon to cease using any Software under **Section 18.3,** CSC Leon may terminate this Contract for cause under **Section 16.1**. Unless the claim arose against the Software independently of any of the actions specified below, Contractor will have no liability for any claim of infringement arising solely from:

(a) Contractor's compliance with any designs, specifications, or instructions of CSC Leon; or

(b) modification of the Software by CSC Leon without the prior knowledge and approval of Contractor.

19. Disclaimer of Damages and Limitation of Liability.

19.1 CSC Leon's Disclaimer of Damages. CSC LEON WILL NOT BE LIABLE, REGARDLESS OF THE FORM OF ACTION, WHETHER IN CONTRACT, TORT, NEGLIGENCE, STRICT LIABILITY OR BY STATUTE OR OTHERWISE, FOR ANY CLAIM RELATED TO OR ARISING UNDER THIS CONTRACT FOR CONSEQUENTIAL, INCIDENTAL, INDIRECT, OR SPECIAL DAMAGES, INCLUDING WITHOUT LIMITATION LOST PROFITS AND LOST BUSINESS OPPORTUNITIES.

19.2 CSC Leon's Limitation of Liability. IN NO EVENT WILL CSC LEON'S AGGREGATE LIABILITY TO CONTRACTOR UNDER THIS CONTRACT, REGARDLESS OF THE FORM OF ACTION, WHETHER IN CONTRACT, TORT, NEGLIGENCE, STRICT LIABILITY OR BY STATUTE OR OTHERWISE, FOR ANY CLAIM RELATED TO OR ARISING UNDER THIS CONTRACT, EXCEED THE MAXIMUM AMOUNT OF FEES PAYABLE UNDER THIS CONTRACT.

20. Disclosure of Litigation, or Other Proceeding.

Contractor must notify CSC Leon within 14 calendar days of receiving notice of any litigation, investigation, arbitration, or other proceeding (collectively, "**Proceeding**") involving Contractor, a Permitted Subcontractor, or an officer or director of Contractor or Permitted Subcontractor, that arises during the term of the Contract, including:

(a) a criminal Proceeding;
(b) a parole or probation Proceeding;
(c) a Proceeding under the Sarbanes-Oxley Act;
(d) a civil Proceeding involving:

(i) a claim that might reasonably be expected to adversely affect Contractor's viability or financial stability; or
(ii) a governmental or public entity's claim or written allegation of fraud; or
(iii) a Proceeding involving any license that Contractor is required to possess in order to perform under this Contract.

21. CSC Leon Data.

21.1 Ownership. CSC Leon's data ("**CSC Leon Data**"), which will be treated by Contractor as Confidential Information, includes:

(a) User Data; and
(b) any other data collected, used, Processed, stored, or generated in connection with the Services, including but not limited to:
(i) personally identifiable information ("**PII**") collected, used, Processed, stored, or generated as the result of the Services,

including, without limitation, any information that identifies an individual, such as an individual's social security number or other government-issued identification number, date of birth, address, telephone number, biometric data, mother's maiden name, email address, credit card information, or an individual's name in combination with any other of the elements here listed; and

(ii) protected health information ("**PHI**") collected, used, Processed, stored, or generated as the result of the Services, which is defined under the Health Insurance Portability and Accountability Act ("**HIPAA**") and its related rules and regulations.

21.2 CSC Leon Data is and will remain the sole and exclusive property of CSC Leon and all right, title, and interest in the same is reserved by CSC Leon.

21.3 Contractor Use of CSC Leon Data. Contractor is provided a limited license to CSC Leon Data for the sole and exclusive purpose of providing the Services, including a license to collect, process, store, generate, and display CSC Leon Data only to the extent necessary in the provision of the Services. Contractor must:

(a) keep and maintain CSC Leon Data in strict confidence, using such degree of care as is appropriate and consistent with its obligations as further described in this Contract and applicable law to avoid unauthorized access, use, disclosure, or loss;

(b) use and disclose CSC Leon Data solely and exclusively for the purpose of providing the Services, such use and disclosure being in accordance with this Contract, any applicable Statement of Work, and applicable law;

(c) keep and maintain CSC Leon Data in the continental United States and

(d) not use, sell, rent, transfer, mine, distribute, commercially exploit, or otherwise disclose or make available CSC Leon Data for Contractor's own purposes or for the benefit of anyone other than CSC Leon without CSC Leon's prior written consent. Contractor's misuse of CSC Leon Data may violate state or federal laws, including but not limited to sections 668.081, 815.01, and 817.568, Florida Statutes.

21.4 Discovery. Contractor will immediately notify CSC Leon upon receipt of any requests which in any way might reasonably require access to CSC Leon Data or CSC Leon's use of the Software and Hosted Services, if applicable. Contractor will notify CSC Leon Program Managers or their designees by the fastest means available and also in writing. In no event will Contractor provide such notification more than twenty-four (24) hours after Contractor receives the request. Contractor will not respond to subpoenas, service of process, public record requests, and other legal requests related to CSC Leon without first notifying CSC Leon and obtaining CSC Leon's prior approval of Contractor's proposed responses. Contractor agrees to provide its completed responses to CSC Leon with adequate time for CSC Leon review, revision and approval.

IF THE CONTRACTOR HAS QUESTIONS REGARDING THE APPLICATION OF CHAPTER 119, FLORIDA STATUTES, TO THE CONTRACTOR'S DUTY TO PROVIDE PUBLIC RECORDS RELATING TO THIS CONTRACT, CONTACT THE CUSTODIAN OF PUBLIC RECORDS AT (telephone number, e-mail address, and mailing address).

21.5 Loss or Compromise of Data. In the event of any act, error or omission, negligence, misconduct, or breach on the part of Contractor that compromises or is suspected to compromise the security, confidentiality, integrity, or availability of CSC Leon Data or the physical, technical, administrative, or organizational safeguards put in place by Contractor that relate to the protection of the security, confidentiality, or integrity of CSC Leon Data, Contractor must, as applicable:

(a) notify CSC Leon as soon as practicable but no later than 24 hours of becoming aware of such occurrence;

(b) cooperate with CSC Leon in investigating the occurrence, including making available all relevant records, logs, files, data reporting, and other materials required to comply with applicable law, including but not limited to section 501.171, Florida Statutes, or as otherwise required by CSC Leon;

(c) in the case of PII or PHI, at CSC Leon's sole election:

(i) with approval and assistance from CSC Leon, notify the affected individuals who comprise the PII or PHI as soon as practicable but no later than is required to comply with applicable law, or, in the absence of any legally required notification period, within 5 calendar days of the occurrence; or

(ii) reimburse CSC Leon for any costs in notifying the affected individuals;

(d) in the case of PII, provide third-party credit and identity monitoring services to each of the affected individuals who comprise the PII for the period required to comply with applicable law, or, in the absence of any legally required monitoring services, for no less than 24 months following the date of notification to such individuals;

(e) perform or take any other actions required to comply with applicable law as a result of the occurrence;

(f) pay for any costs associated with the occurrence, including but not limited to any costs incurred by CSC Leon in investigating and resolving the occurrence, including reasonable attorney's fees associated with such investigation and resolution;

(g) without limiting Contractor's obligations of indemnification as further described in this Contract, indemnify, defend, and hold harmless CSC Leon for any and all claims, including reasonable attorneys' fees, costs, and incidental expenses, which may be suffered by, accrued against, charged to, or recoverable from CSC Leon in connection with the occurrence;

(h) be responsible for recreating lost CSC Leon Data in the manner and on the schedule set by CSC Leon without charge to CSC Leon; and

(i) provide to CSC Leon a detailed plan within 10 calendar days of the occurrence describing the measures Contractor will undertake to prevent a future occurrence. Notification to affected individuals, as described above, must comply with applicable law, be written in plain language, not be tangentially used for any solicitation purposes, and contain, at a minimum: name and contact information of Contractor's representative; a description of the nature of the loss; a list of the types of data involved; the known or approximate date of the loss; how such loss may affect the affected individual; what steps Contractor has taken to protect the affected individual; what steps the affected individual can take to protect himself or herself; contact information for major credit card reporting agencies; and, information regarding the credit and identity monitoring services to be provided by Contractor. CSC Leon will have the option to review and approve any notification sent to affected individuals prior to its delivery. Notification to any other party, including but not limited to public media outlets, must be reviewed and approved by CSC Leon in writing prior to its dissemination.

21.6 The Parties agree that any damages relating to a breach of this **Section 21.5** are to be considered direct damages and not consequential damages.

22. Non-Disclosure of Confidential Information.

The Parties acknowledge that each Party may be exposed to or acquire communication or data of the other Party that is confidential, privileged communication not intended to be disclosed to third Parties.

22.1 Meaning of Confidential Information. For the purposes of this Contract, the term "**Confidential Information**" means all information and documentation of a Party that: (a) has been marked "confidential" or with words of similar meaning, at the time of disclosure by such party; (b) if disclosed orally or not marked "confidential" or with words of similar meaning, was subsequently summarized in writing by the disclosing Party and marked “confidential” or with words of similar meaning; and, (c) should reasonably be recognized as confidential information of the disclosing Party. The term “Confidential Information” does not include any information or documentation that was: (a) subject to disclosure under the State public records law; (b) already in the possession of the receiving Party without an obligation of confidentiality; (c) developed independently by the receiving Party, as demonstrated by the receiving Party, without violating the disclosing Party’s proprietary rights; (d) obtained from a source other than the disclosing Party without an obligation of confidentiality; or, (e) publicly available when received, or thereafter became publicly available (other than through any unauthorized disclosure by, through, or on behalf of, the receiving Party). For purposes of this Contract, in all cases and for all matters, CSC Leon Data is deemed to be Confidential Information.

22.2 Obligation of Confidentiality. The Parties agree to hold all Confidential Information in strict confidence and not to copy, reproduce, sell, transfer, or otherwise dispose of, give or disclose such Confidential Information to third parties other than employees, agents, or subcontractors of a Party who have a need to know in connection with this Contract or to use such Confidential Information for any purposes whatsoever other than the performance of this Contract. The Parties agree to advise and require their respective employees, agents, and subcontractors of their obligations to keep all Confidential Information confidential. Disclosure to the Contractor’s subcontractor is permissible where:

(a) the subcontractor is a Permitted Subcontractor;

(b) the disclosure is necessary or otherwise naturally occurs in connection with work that is within the Permitted Subcontractor's responsibilities; and

(c) Contractor obligates the Permitted Subcontractor in a written contract to maintain CSC Leon’s Confidential Information in confidence. At CSC Leon’s request, any of the Contractor’s and Permitted Subcontractor’s Representatives may be required to execute a separate agreement to be bound by the provisions of this **Section 22.2**.

22.3 Cooperation to Prevent Disclosure of Confidential Information. Each Party must use its best efforts to assist the other Party in identifying and preventing any unauthorized use or disclosure of any Confidential Information. Without limiting the foregoing, each Party must advise the other Party immediately in the event either Party learns or has reason to believe that any person who has had access to Confidential Information has violated or intends to violate the terms of this Contract. Each Party will cooperate with the other Party in seeking injunctive or other equitable relief against any such person.

Exhibit 1
Page 31

22.4 Remedies for Breach of Obligation of Confidentiality. Each Party acknowledges that breach of its obligation of confidentiality may give rise to irreparable injury to the other Party, which damage may be inadequately compensable in the form of monetary damages. Accordingly, a Party may seek and obtain injunctive relief against the breach or threatened breach of the foregoing undertakings, in addition to any other legal remedies which may be available, to include, in the case of CSC Leon, at the sole election of CSC Leon, the immediate termination, without liability to CSC Leon, of this Contract or any Statement of Work corresponding to the breach or threatened breach.

22.5 Surrender of Confidential Information upon Termination. Upon termination or expiration of this Contract or a Statement of Work, in whole or in part, each Party must, within 5 Business Days from the date of termination, return to the other Party any and all Confidential Information received from the other Party, or created or received by a Party on behalf of the other Party, which are in such Party's possession, custody, or control. Upon confirmation from CSC Leon, of receipt of all data, Contractor must permanently sanitize or destroy CSC Leon's Confidential Information, including CSC Leon Data, from all media including backups using National Security Agency ("NSA") and/or National Institute of Standards and Technology ("NIST") (NIST Guide for Media Sanitization 800-88) data sanitization methods or as otherwise instructed by CSC Leon. If CSC Leon determines that the return of any Confidential Information is not feasible or necessary, Contractor must destroy the Confidential Information as specified above. The Contractor must certify the destruction of Confidential Information (including CSC Leon Data) in writing within 5 Business Days from the date of confirmation from CSC Leon.

23. Records Maintenance, Inspection, Examination, and Audit.

23.1 Right of Audit. To preserve the public interest in the prudent expenditure of public funds, CSC Leon or its designee may audit Contractor to verify compliance with this Contract. Contractor must retain and provide to CSC Leon or its designee upon request, all financial and accounting records related to this Contract through the Term of this Contract and for 4 years after the latter of termination, expiration, or final payment under this Contract or any extension ("**Financial Audit Period**"). If an audit, litigation, or other action involving the records is initiated before the end of the Financial Audit Period, Contractor must retain the records until all issues are resolved.

23.2 Right of Inspection. Within 10 calendar days of providing notice, CSC Leon and its authorized representatives or designees have the right to enter and inspect Contractor's premises or any other places where Services are being performed, and examine, copy, and audit all records related to this Contract. Contractor must cooperate and provide reasonable assistance. If financial errors are revealed, the amount in error must be reflected as a credit or debit on subsequent invoices until the amount is paid or refunded. Any remaining balance at the end of this Contract must be paid or refunded within 45 calendar days.

23.3 Application. This **Section 23** applies to Contractor, any Affiliate, and any Permitted Subcontractor that performs Services in connection with this Contract.

24. Support Services.

Contractor will provide CSC Leon with the Support Services described in the Service Level Agreement attached as **Schedule D** to this Contract. Such Support Services will be provided:

(a) Free of charge during the Warranty Period.

(b) Thereafter, for so long as CSC Leon elects to receive Support Services for the Software, in consideration of CSC Leon's payment of Fees for such services in accordance with the rates set forth in the Pricing Schedule.

25. Data Security Requirements.

25.1 Florida Cybersecurity Standards. Throughout the Term and at all times in connection with its actual or required performance of the Services, Contractor will maintain and enforce an information security program including safety and physical and technical security policies and procedures with respect to its Processing of CSC Leon’s Confidential Information that comply with the Florida Cybersecurity Standards promulgated in chapter 60GG-2 of the Florida Administrative Code, *Information Technology Security*, which is hereby incorporated by reference and deemed part of this Contract as if fully set forth herein. For these purposes, CSC Leon is deemed an “agency” and all of Contractor’s Services for CSC Leon shall comply with the standards, but no submittals to a State agency are required.

25.2 Off-Shoring Prohibited. All Services will be performed within the continental United States. All data related to or arising from the Contractor’s performance of the Services shall remain in, and be maintained in, the continental United States. Neither the Contractor nor any subcontractor shall access such data from outside of the continental United States, nor will they send any such data outside the continental United States. For purposes of this requirement, “data” means a subset of structured information in a format that allows such information to be electronically retrieved and transmitted.

26. Training.

Contractor will provide, at no additional charge, training on all uses of the Software permitted hereunder in accordance with the times, locations and other terms set forth in a Statement of Work. Upon CSC Leon's request, Contractor will timely provide training for additional Authorized Users or other additional training on all uses of the Software for which CSC Leon requests such training, at such reasonable times and locations and pursuant to such rates and other terms as are set forth in the Pricing Schedule.

27. Maintenance Releases; New Versions.

27.1 Maintenance Releases. Provided that CSC Leon is current on its Fees, during the Term, Contractor will provide CSC Leon, at no additional charge, with all Maintenance Releases, each of which will constitute Software and be subject to the terms and conditions of this Contract.

27.2 New Versions. Provided that CSC Leon is current on its Fees, during the Term, Contractor will provide CSC Leon, at no additional charge, with all New Versions, each of which will constitute Software and be subject to the terms and conditions of this Contract.

27.3 Installation. CSC Leon has no obligation to install or use any Maintenance Release or New Versions. If CSC Leon wishes to install any Maintenance Release or New Version, CSC Leon will have the right to have such Maintenance Release or New Version installed, in CSC Leon's discretion, by Contractor or other authorized party as set forth in a Statement of Work. Contractor will provide CSC Leon, at no additional charge, adequate Documentation for installation of the Maintenance Release or New Version, which has been developed and tested by Contractor and Acceptance Tested by CSC Leon. CSC Leon's decision not to install or implement a Maintenance Release or New Version of the Software will not affect its right to receive Support Services throughout the Term of this Contract.

28. Source Code Escrow.

28.1 Escrow Contract. The Parties may enter into a separate intellectual property escrow agreement. Such escrow agreement will govern all aspects of Source Code escrow and release. The cost of the escrow will be the sole responsibility of Contractor.

28.2 Deposit. Within 30 business days of the Effective Date, Contractor will deposit with the escrow agent, pursuant to the procedures of the escrow agreement, the Source Code for the Software, as well as the Documentation and names and contact information for each author or other creator of the Software. Promptly after release of any update, upgrade, patch, bug fix, enhancement, new version, or other revision to the Software, Contractor will deposit updated Source Code, documentation, names, and contact information with the escrow agent.

28.3 Verification. At State's request and expense, the escrow agent may at any time verify the Deposit Material, including without limitation by compiling Source Code, comparing it to the Software, and reviewing the completeness and accuracy of any and all material.

In the event that the Deposit Material does not conform to the requirements of **Section 28.2** above:

(a) Contractor will promptly deposit conforming Deposit Material; and

(b) Contractor will pay the escrow agent for subsequent verification of the new Deposit Material. Any breach of the provisions of this **Section 28.3** will constitute material breach of this Contract, and no further payments will be due from CSC Leon until such breach is cured, in addition to other remedies CSC Leon may have.

28.4 Deposit Material License. Contractor hereby grants CSC Leon a license to use, reproduce, and create derivative works from the Deposit Material, provided CSC Leon may not distribute or sublicense the Deposit Material or make any use of it whatsoever except for such internal or governmental uses as necessary to maintain and support the Software. Copies of the Deposit Material created or transferred pursuant to this Contract are licensed, not sold, and CSC Leon receives no title to or ownership of any copy or of the Deposit Material itself. The Deposit Material constitutes Confidential Information of Contractor pursuant to **Section 22** (Non-disclosure of Confidential Information) of this Contract (provided no provision of **Section 22.4** calling for return of Confidential Information before termination of this Contract will apply to the Deposit Material).

29. Contractor Representations and Warranties.

29.1 Authority. Contractor represents and warrants to CSC Leon that:

(a) It is duly organized, validly existing, and in good standing as a corporation or other entity as represented under this Contract under the laws and regulations of its jurisdiction of incorporation, organization, or chartering;

(b) It has the full right, power, and authority to enter into this Contract, to grant the rights and licenses granted under this Contract, and to perform its contractual obligations;

(c) There is no pending or threatened action, proceeding, or investigation, or any other legal or financial condition, that would in any way prohibit, restrain, or diminish the Contractor's ability to satisfy its Contract obligations;

(d) The execution of this Contract by its Representative has been duly authorized by all necessary organizational action;

(e) When executed and delivered by Contractor, this Contract will constitute the legal, valid, and binding obligation of Contractor, enforceable against Contractor in accordance with its terms;

(f) Contractor is neither currently engaged in nor will engage in the boycott of a person based in or doing business with a strategic partner as described in 22 USC 8601 to 8606;

(g) Neither Contractor nor any Affiliate is currently on the convicted vendor list maintained pursuant to section 287.133, Florida Statutes, or on any similar list maintained by any other state or the federal government; and

(h) Contractor shall immediately notify CSC Leon in writing if Contractor's ability to perform is compromised in any manner during the term of the Contract.

29.2 Proposal. Contractor represents and warrants to CSC Leon that:

(a) The prices proposed by Contractor were arrived at independently, without consultation, communication, or agreement with any other Respondent for the purpose of restricting competition; the prices quoted were not knowingly disclosed by Contractor to any other Respondent to the RFP; and no attempt was made by Contractor to induce any other Person to submit or not submit a proposal for the purpose of restricting competition;

(b) All written information furnished to CSC Leon by or for Contractor in connection with this Contract, including the Proposal, is true, accurate, and complete, and contains no untrue statement of material fact or omits any material fact necessary to make the information not misleading;

(c) Contractor is not in material default or breach of any other contract or agreement that it may have with CSC Leon. Contractor further represents and warrants that it has not been a party to any contract with CSC Leon that was terminated by CSC Leon within the previous 5 years for the reason that Contractor failed to perform or otherwise breached an obligation of the contract; and

(d) If any of the certifications, representations, or disclosures made in the Proposal change after contract award, the Contractor is required to report those changes immediately to the Contract Administrator.

29.3 Software Representations and Warranties. Contractor further represents and warrants to CSC Leon that:

(a) it is the legal and beneficial owner of the entire right, title and interest in and to the Software, including all Intellectual Property Rights relating thereto;

(b) it has, and throughout the license term, will retain the unconditional and irrevocable right, power and authority to grant and perform the license hereunder;

(c) it has, and throughout the Term and any additional periods during which Contractor does or is required to perform the Services will have, the unconditional and irrevocable right, power and authority, including all permits and licenses required, to provide the Services and grant and perform all rights and licenses granted or required to be granted by it under this Contract;

(d) the Software, and CSC Leon's use thereof, is and throughout the license term will be free and clear of all encumbrances, liens and security interests of any kind;

(e) neither its grant of the license, nor its performance under this Contract does or to its knowledge will at any time:

> (i) conflict with or violate any applicable law;
> (ii) require the consent, approval or authorization of any governmental or regulatory authority or other third party; or
> (iii) require the provision of any payment or other consideration to any third party;

(f) when used by CSC Leon or any Authorized User in accordance with this Contract and the Documentation, the Software, the Hosted Services, if applicable, or Documentation as delivered or installed by Contractor does not or will not:

> (i) infringe, misappropriate, or otherwise violate any Intellectual Property Right or other right of any third party; or
> (ii) fail to comply with any applicable law;

(g) as provided by Contractor, the Software and Services do not and will not at any time during the Term contain any:

> (i) Harmful Code; or
> (ii) Third party or Open-Source Components that operate in such a way that it is developed or compiled with or linked to any third party or Open-Source Components, other than Approved Third Party Components specifically described in a Statement of Work.

(h) all Documentation is and will be complete and accurate in all material respects when provided to CSC Leon such that at no time during the license term will the Software have any material undocumented feature; and

(i) it will perform all Services in a timely, skillful, professional and workmanlike manner in accordance with commercially reasonable industry standards and practices for similar services, using personnel with the requisite skill, experience and qualifications, and will devote adequate resources to meet its obligations under this Contract.

(j) when used in the Operating Environment (or any successor thereto) in accordance with the Documentation, all Software as provided by Contractor, will be fully operable, meet all applicable specifications, and function in all respects, in conformity with this Contract and the Documentation;

(k) Contractor acknowledges that CSC Leon will not indemnify any third parties, including but not limited to any third-party software providers that provide software that will be incorporated in or otherwise used in conjunction with the Services, and that notwithstanding anything to the contrary contained in any third-party software license agreement or end user license agreement, CSC Leon will not indemnify any third party software provider for any reason whatsoever;

(l) no Maintenance Release or New Version, when properly installed in accordance with this Contract, will have a material adverse effect on the functionality or operability of the Software.

(m) all Configurations or Customizations made during the Term will be forward compatible with future Maintenance Releases or New Versions and be fully supported without additional costs.

(n) If Contractor Hosted:

(i) Contractor will not advertise through the Hosted Services (whether with adware, banners, buttons or other forms of online advertising) or link to external web sites that are not approved in writing by CSC Leon;

(ii) the Software and Services will in all material respects conform to and perform in accordance with the Specifications and all requirements of this Contract, including the Availability and Availability Requirement provisions set forth in the Service Level Agreement; and

(iii) all Specifications are, and will be continually updated and maintained so that they continue to be, current, complete and accurate and so that they do and will continue to fully describe the Hosted Services in all material respects such that at no time during the Term or any additional periods during which Contractor does or is required to perform the Services will the Hosted Services have any material undocumented feature.

(o) During the Term of this Contract, any audit rights contained in any third-party software license agreement or end user license agreement for third-party software incorporated in or otherwise used in conjunction with the Software or with the Hosted Services, if applicable, will apply solely to Contractor or its Permitted Subcontractors. Regardless of anything to the contrary contained in any third-party software license agreement or end user license agreement, third-party software providers will have no audit rights whatsoever against CSC Leon Systems or networks.

29.4 Disclaimer. EXCEPT FOR THE EXPRESS WARRANTIES SET FORTH IN THIS CONTRACT, CONTRACTOR HEREBY DISCLAIMS ALL WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE, WITH RESPECT TO THIS CONTRACT.

30. Offers of Employment.

During the first 12 months of the Contract, Contractor shall not hire an employee of CSC Leon, without prior written consent of CSC Leon, who has substantially worked on any project covered by this Contract. The Contractor will be billed for 50% of the employee's annual salary in effect at the time of separation.

31. Conflicts and Ethics.

Contractor will uphold high ethical standards and is prohibited from: (a) holding or acquiring an interest that would conflict with this Contract; (b) doing anything that creates an appearance of impropriety with respect to the award or performance of the Contract; (c) attempting to influence or appearing to influence any CSC Leon employee by the direct or indirect offer of anything of value; or (d) paying or agreeing to pay any person, other than employees and consultants working for Contractor, any consideration contingent upon the award of the Contract. Contractor must immediately notify CSC Leon of any violation or potential violation of these standards. This Section applies to Contractor, any parent, affiliate, or subsidiary organization of Contractor, and any Permitted Subcontractor that provides Services and Deliverables in connection with this Contract.

32. Compliance with Laws.

Contractor, its subcontractors, including Permitted Subcontractors, and their respective Representatives must comply with all laws in connection with this Contract.

33. Nondiscrimination.

Contractor and its subcontractors will not discriminate unlawfully and will comply with all applicable laws, including but not limited to the Florida Civil Rights Act of 1992, the Americans with Disabilities Act of 1990, and the federal Civil Rights Act of 1964. Breach of this covenant is a material breach of the Contract.

34. E-Verify.

CSC Leon is a public employer as defined in section 448.095, Florida Statutes. Therefore, the Contractor must register with and use the E-Verify system to verify the work authorization status of all newly hired employees (see https://www.e-verify.gov/). Any subcontractors engaged by the Contractor to provide Services for work on the Contract must provide the Contractor with an affidavit stating that the subcontractor does not employ, contract with, or subcontract with an unauthorized alien and the Contractor shall maintain a copy of such affidavit for the duration of the Contract.

35. Governing Law.

This Contract is governed, construed, and enforced in accordance with Florida law, excluding choice-of-law principles, and all claims relating to or arising out of this Contract are governed by Florida law, excluding choice-of-law principles. Any dispute arising from this Contract must be resolved in the appropriate State court in Leon County, Florida.

Contractor waives any objections, such as lack of personal jurisdiction or *forum non conveniens*. Contractor must appoint an agent in Florida to receive service of process.

36. Non-Exclusivity.

Nothing contained in this Contract is intended nor is to be construed as creating any requirements contract with Contractor, nor does it provide Contractor with a right of first refusal for any future work. This Contract does not restrict CSC Leon from acquiring similar, equal, or like Services from other sources.

37. Force Majeure

37.1 Force Majeure Events. Neither Party will be liable or responsible to the other Party, or be deemed to have defaulted under or breached the Contract, for any failure or delay in fulfilling or performing any term hereof, when and to the extent such failure or delay is caused by: acts of God, flood, fire or explosion, war, terrorism, invasion, riot or other civil unrest, embargoes or blockades in effect on or after the date of the Contract, national or regional emergency, adverse weather conditions (including but not limited to tropical storms and hurricanes), epidemic, pandemic or any passage of law or governmental order, rule, regulation or direction, or any action taken by a governmental or public authority, including imposing an embargo, export or import restriction, quota or other restriction or prohibition (each of the foregoing, a "**Force Majeure Event**"), in each case provided that: (a) such event is outside the reasonable control of the affected Party; (b) the affected Party gives prompt written notice to the other Party, stating the period of time the occurrence is expected to continue; (c) the affected Party uses diligent efforts to end the failure or delay and minimize the effects of such Force Majeure Event.

37.2 CSC Leon Performance; Termination. In the event of a Force Majeure Event affecting Contractor’s performance under the Contract, CSC Leon may suspend its performance hereunder until such time as Contractor resumes performance. CSC Leon may terminate the Contract by written notice to Contractor if a Force Majeure Event affecting Contractor’s performance hereunder continues substantially uninterrupted for a period of 5 Business Days or more. Unless CSC Leon terminates the Contract pursuant to the preceding sentence, any date specifically designated for Contractor’s performance under the Contract will automatically be extended for a period up to the duration of the Force Majeure Event.

37.3 Exclusions; Non-suspended Obligations. Notwithstanding the foregoing or any other provisions of the Contract or this Schedule:

(a) in no event will any of the following be considered a Force Majeure Event:

(i) shutdowns, disruptions or malfunctions of Hosted Services or any of Contractor’s telecommunication or internet services other than as a result of general and widespread internet or telecommunications failures that are not limited to the Hosted Services; or

(ii) the delay or failure of any Contractor Personnel to perform any obligation of Contractor hereunder unless such delay or failure to perform is itself by reason of a Force Majeure Event.

(b) no Force Majeure Event modifies or excuses Contractor’s obligations under **Sections** Error! Reference source not found. (CSC Leon Data), Error! Reference source not found. (Non-Disclosure of Confidential Information), or Error! Reference source not found. (Indemnification) of the Contract, Disaster Recovery and Backup requirements set forth in the Service Level Agreement, Availability Requirement (if Contractor Hosted) defined in the Service Level Agreement, or any data retention or security requirements under the Contract.

38. Dispute Resolution.

The Parties will endeavor to resolve any Contract dispute in accordance with this provision. The dispute will be referred to the Parties' respective Contract Administrators or Program Managers. Such referral must include a description of the issues and all supporting documentation. The Parties must submit the dispute to a senior executive if unable to resolve the dispute within 15 business days. The Parties will continue performing while a dispute is being resolved, unless the dispute precludes performance. A dispute involving payment does not preclude performance. Litigation to resolve the dispute will not be instituted until after the dispute has been elevated to the Parties’ senior executive and either concludes that resolution is unlikely or fails to respond within 15 business days. The Parties are not prohibited from instituting formal proceedings: (a) to avoid the expiration of statute of limitations period; (b) to preserve a superior position with respect to creditors; or (c) where a Party makes a determination that a temporary restraining order or other injunctive relief is the only adequate remedy. This Section does not limit CSC Leon's right to terminate the Contract.

39. Media Releases.

News releases (including promotional literature and commercial advertisements) pertaining to this Contract or project to which it relates must not be made without the prior written approval of CSC Leon, and then only in accordance with the explicit written instructions of CSC Leon.

40. Severability.

If any part of this Contract is held invalid or unenforceable, by any court of competent jurisdiction, that part will be deemed deleted from this Contract and the severed part will be replaced by agreed upon language that achieves the same or similar objectives. The remaining Contract will continue in full force and effect.

41. Waiver.

Failure to enforce any provision of this Contract will not constitute a waiver.

42. Survival.

Any right, obligation, or condition that, by its express terms or nature and context is intended to survive, will survive the termination or expiration of this Contract; such rights, obligations, or conditions include, but are not limited to, those related to transition responsibilities; indemnification; disclaimer of damages and limitations of liability; CSC Leon Data; non-disclosure of Confidential Information; representations and warranties; insurance and bankruptcy.

43. Term.

The Contract effective date shall be ______, __, 2022, or the date on which the last Party has signed the Contract, whichever is later ("**Effective Date**"). The Contract term shall begin on the Effective Date and shall end on ______, __, 202_, unless the Contract is terminated earlier or renewed as provided herein (the "**Term**"). CSC Leon's performance and obligation to pay under this Contract is contingent upon an annual appropriation. CSC Leon shall not be obligated to pay for costs incurred related to the Contract prior to its Effective Date or after its ending date.

44. Contract Modification.

This Contract may not be amended except by signed agreement between the Parties (a "**Contract Change Notice**"). Notwithstanding the foregoing, no subsequent Statement of Work or Contract Change Notice executed after the Effective Date will be construed to amend this Contract unless it specifically states its intent to do so and cites the section or sections amended.

45. HIPAA Compliance.

CSC Leon and Contractor must comply with all obligations under HIPAA and its accompanying regulations, including but not limited to entering into a business associate agreement, if reasonably necessary to keep CSC Leon and Contractor in compliance with HIPAA.

46. Accessibility Requirements.

46.1 All Software provided by Contractor under this Contract, including associated content and documentation, must conform to WCAG 2.0 Level AA. Contractor must provide a description of conformance with WCAG 2.0 Level AA specifications by providing a completed PAT for each product provided under the Contract. At a minimum, Contractor must comply with the WCAG 2.0 Level AA conformance claims it made to CSC Leon, including the level of conformance provided in any PAT. Throughout the Term of the Contract, Contractor must:

(a) maintain compliance with WCAG 2.0 Level AA and meet or exceed the level of conformance provided in its written materials, including the level of conformance provided in each PAT;

(b) comply with plans and timelines approved by CSC Leon to achieve conformance in the event of any deficiencies;

(c) ensure that no Maintenance Release, New Version, update or patch, when properly installed in accordance with this Contract, will have any adverse effect on the conformance of Contractor's Software to WCAG 2.0 Level AA;

(d) promptly respond to and resolve any complaint CSC Leon receives regarding accessibility of Contractor's Software; and

(e) upon CSC Leon's written request, provide evidence of compliance with this Section by delivering to CSC Leon Contractor's most current PAT for each product provided under the Contract.

46.2 <u>Warranty</u>. Contractor warrants that all WCAG 2.0 Level AA conformance claims made by Contractor pursuant to this Contract, including all information provided in any PAT Contractor provides to CSC Leon, are true and correct. If CSC Leon determines such conformance claims provided by the Contractor represent a higher level of conformance than what is actually provided to CSC Leon, Contractor will, at its sole cost and expense, promptly remediate its Software to align with Contractor's stated WCAG 2.0 Level AA conformance claims in accordance with plans and timelines that are approved in writing by CSC Leon. If Contractor is unable to resolve such issues in a manner acceptable to CSC Leon, in addition to all other remedies available to CSC Leon, CSC Leon may terminate

Exhibit 1
Page 43

this Contract for cause under **Section 16.1**.

46.3 Contractor must, without limiting Contractor's obligations of indemnification as further described in this Contract, indemnify, defend, and hold harmless CSC Leon for any and all claims, including reasonable attorneys' fees, costs, and incidental expenses, which may be suffered by, accrued against, charged to, or recoverable from CSC Leon arising out of its failure to comply with the foregoing accessibility standards.

46.4 Failure to comply with the requirements in this **Section 47** shall constitute a material breach of this Contract.

47. Further Assurances.

Each Party will, upon the reasonable request of the other Party, execute such documents and perform such acts as may be necessary to give full effect to the terms of this Contract.

48. Relationship of the Parties.

The relationship between the Parties is that of independent contractors. Contractor, its employees, and agents will not be considered employees of CSC Leon. No partnership or joint venture relationship is created by virtue of this Contract.

Contractor, and not CSC Leon, is responsible for the payment of wages, benefits and taxes of Contractor's employees and any subcontractors. Prior performance does not modify Contractor's status as an independent contractor. Neither Party has authority to contract for nor bind the other Party in any manner whatsoever.

49. Headings.

The headings in this Contract are for reference only and do not affect the interpretation of this Contract.

50. No Third-party Beneficiaries.

This Contract is for the sole benefit of the Parties and their respective successors and permitted assigns. Nothing herein, express or implied, is intended to or will confer on any other person or entity any legal or equitable right, benefit or remedy of any nature whatsoever under or by reason of this Contract.

51. Equitable Relief.

Each Party to this Contract acknowledges and agrees that (a) a breach or threatened breach by such Party of any of its obligations under this Contract may give rise to irreparable harm to the other Party for which monetary damages would not be an adequate remedy and (b) in the event of a breach or a threatened breach by such Party of any such obligations, the other Party hereto is, in addition to any and all other rights and remedies that may be available to such Party at law, at equity or otherwise in respect of such breach, entitled to equitable relief, including a temporary restraining order, an injunction, specific performance and any other relief that may be available from a court of competent jurisdiction, without any requirement to post a bond or other security, and without any requirement to prove actual damages or that monetary damages will not afford an adequate remedy. Each Party to this Contract agrees that such Party will not oppose or otherwise challenge the appropriateness of equitable relief or the entry by a court of competent jurisdiction of an order granting equitable relief, in either case, consistent with the terms of this Section.

52. Effect of Contractor Bankruptcy.

All rights and licenses granted by Contractor under this Contract are and will be deemed to be rights and licenses to “intellectual property,” and all Software and Deliverables are and will be deemed to be “embodiments” of “intellectual property,” for purposes of, and as such terms are used in and interpreted under, Section 365(n) of the United States Bankruptcy Code (the “**Code**”). If Contractor or its estate becomes subject to any bankruptcy or similar proceeding, CSC Leon retains and has the right to fully exercise all rights, licenses, elections, and protections under this Contract, the Code and all other applicable bankruptcy, insolvency, and similar laws with respect to all Software and other Deliverables. Without limiting the generality of the foregoing, Contractor acknowledges and agrees that, if Contractor or its estate will become subject to any bankruptcy or similar proceeding:

(a) all rights and licenses granted to CSC Leon under this Contract will continue subject to the terms and conditions of this Contract, and will not be affected, even by Contractor’s rejection of this Contract; and

(b) CSC Leon will be entitled to a complete duplicate of (or complete access to, as appropriate) all such intellectual property and embodiments of intellectual property comprising or relating to any Software or other Deliverables, and the same, if not already in CSC Leon’s possession, will be promptly delivered to CSC Leon, unless Contractor elects to and does in fact continue to perform all of its obligations under this Contract.

53. Schedules.

All Schedules that are referenced herein and attached hereto are hereby incorporated by reference. The following Schedules are attached hereto and incorporated herein:

Schedule A	Statement of Work
Schedule B	Pricing Schedule

Schedule C	Insurance Schedule
Schedule D	Service Level Agreement
Schedule E	Rule 60-GG
Schedule F	Disaster Recovery Plan (if Contractor Hosted)
Schedule G	Transition Plan

54. Counterparts.

This Contract may be executed in counterparts, each of which will be deemed an original, but all of which together are deemed to be one and the same agreement and will become effective and binding upon the Parties as of the Effective Date at such time as all the signatories hereto have signed a counterpart of this Contract. A signed copy of this Contract delivered by facsimile, e-mail or other means of electronic transmission (to which a signed copy is attached) is deemed to have the same legal effect as delivery of an original signed copy of this Contract.

55. Entire Agreement.

These terms and conditions, including all Statements of Work and other Schedules and Exhibits (again collectively the "Contract") constitutes the sole and entire agreement of the Parties to this Contract with respect to the subject matter contained herein, and supersedes all prior and contemporaneous understandings and agreements, representations and warranties, both written and oral, with respect to such subject matter. The Parties have had an opportunity to negotiate this Contract and to consult with counsel; accordingly, the rule of interpretation known as "construction against the drafter" will not apply to this Contract. In the event of any inconsistency between statements made in the terms and conditions, the Schedules, Exhibits, and a Statement of Work, the following order of precedence governs: (a) first, these terms and conditions and (b) second, chapter 60GG-2 of the Florida Administrative Code, *Information Technology Security*, and (c) third, each Statement of Work; and (d) fourth, the remaining Exhibits and Schedules to this Contract.

NO TERMS ON CONTRACTOR'S INVOICES, WEBSITE, BROWSE-WRAP, SHRINK-WRAP, CLICK-WRAP, CLICKTHROUGH OR OTHER NON-NEGOTIATED TERMS AND CONDITIONS PROVIDED WITH ANY OF THE SERVICES, OR DOCUMENTATION HEREUNDER, EVEN IF ATTACHED TO CSC LEON'S DELIVERY OR PURCHASE ORDER, WILL CONSTITUTE A PART OR AMENDMENT OF THIS CONTRACT OR IS BINDING ON CSC LEON OR ANY AUTHORIZED USER FOR ANY PURPOSE. ALL SUCH OTHER TERMS AND CONDITIONS HAVE NO FORCE AND EFFECT AND ARE DEEMED REJECTED BY CSC LEON AND THE AUTHORIZED USER, EVEN IF ACCESS TO OR USE OF SUCH SERVICE OR DOCUMENTATION REQUIRES AFFIRMATIVE ACCEPTANCE OF SUCH TERMS AND CONDITIONS.

IN WITNESS WHEREOF, each Party has caused this Contract to be executed by its duly authorized representatives.

CHILDREN’S SERVICES COUNCIL OF LEON COUNTY

____

By:

Its:

Date: December ___, 2022

[CONTRACTOR NAME]

____

By:

Its:

Date: December ___, 2022

SCHEDULE A – STATEMENT OF WORK

SECTION 1 – INTRODUCTION

This schedule identifies the anticipated requirements of any Contract resulting from this RFP. As used during the solicitation phase, the term "Vendor" in this document refers to a Respondent to the RFP.

The Vendor must respond to each requirement or question and explain how it will fulfill each requirement. Attach any supplemental information and appropriately reference within your response.

A. Purpose and Goals

The Children's Services Council of Leon County ("CSC Leon") seeks an integrated information system to manage specific functions efficiently and maximize data analysis capabilities. Specifically, CSC Leon seeks to:

1. Develop a grant making and contract management system with a comprehensive solution for supporting programmatic functions, including performance measurement and reporting,
2. Integrate with the current CSC Leon accounting software (Bill.com),
3. Introduce an integrated customer relationship management (CRM) solution to enhance community engagement efforts, and
4. Work with existing community partner database systems to develop data sharing agreements and processes to better serve clients.

Specifically, CSC Leon is seeking a Vendor Hosted Software Solution and applicable services, utilizing Commercial-Off-the-Shelf Software (COTS) with customizations as needed. CSC Leon is not seeking a fully custom designed system. A primary purpose is to upgrade CSC Leon's current technology environment as described below, and to support future growth of the organization.

CSC Leon's goals are to:

1. Acquire a solution that supports CSC Leon's immediate plans for information systems integration and near-term plans for electronic data exchange with external stakeholders.
2. Acquire a platform that will allow CSC Leon to collect aggregated program-level data and eventually include the collection of individual client-level data.
3. Integrate specific business processes/systems and eliminate manual/redundant entry of information.
4. Acquire and implement a software solution that meets CSC Leon's needs using as much COTS functionality as possible.

5. Support the current business process needs of the primary functions within the organization, updating software system functionality, where needed.

6. Establish the foundation for future reporting, analysis and budgeting needs.

7. Ensure all stakeholder classes have ready access to accurate and timely information to improve operational productivity and customer service.

8. Enhance functionality to provide more efficient and effective reporting in specific areas of the business.

9. Implement a stable and inter-connected set of systems capable of accommodating both internal stakeholder and external stakeholder needs.

10. Acquire a well-supported system from a reliable Vendor with adequate resources to support, upgrade, and maintain the package over the long-term.

11. Acquire a system with robust architecture that has capability to effectively and efficiently integrate with other vendor solutions.

12. Partner with a Vendor that can architect and provide a flexible and phased implementation approach.

13. Improve stakeholder collaboration and build good inter-department processes, (e.g., task flow management).

14. Either strategically migrate or archive the historic record of transactions currently maintained in multiple applications serving as systems of record.

B. Business Modules

CSC Leon believes the goals stipulated above can be made by the integrated deployment of the following three software modules into a single solution:

1. *Grant Making & Contract Management*
   a. Design and publish competitive procurements and community funding opportunities (grants)
   b. Management of application process by external stakeholders with the ability to "save as you go" and flexible budget templates
   c. Task management (workflows) and decision support for application review and scoring by internal and external stakeholders
   d. Contract award, signature and execution
   e. Contract and fund management
   f. Integrate with other modules

2. *Performance Measurement and Information Management*
   a. Robust data management tool to collect, organize, analyze and display specific services and activities by multiple external stakeholders including:

        i. Programmatic data (demographics, attendance, process measures, etc.)
        ii. Fiscal activity reporting and tracking (budgets, expenditures, staffing, etc.)
        iii. Performance indicators (impact measurement tools, etc.) including change over time
    b. Ability to build intelligent processes to acquire third-party, publicly available data and integrate into display and comparison functions over time (e.g., U.S. Census Bureau, Florida Department of Health, etc.)
    c. Ability to analyze data and easily create visualization of service distribution by type, zip code, and other filters
    d. Integrate with other modules

3. *Customer Relationship Management*
    a. Store contact and demographic details for a multitude of stakeholders including community investment partners, applicants, volunteers, general interest, media, council members, funders, donors, etc.
    b. Record requests for information, technical assistance, training, etc. with ability to assign tasks and track follow-up
    c. Design and publish sign ups/registration and track participation/attendance with the ability to issue certificates post event/training
    d. Design and publish community outreach campaigns
    e. Integrate with other modules

C. Current Technology Environment

1. Office Location & Description

CSC Leon has one location in Tallahassee, Florida, which includes both office and meeting space for 7 staff members and a 10-member council along with a family resource room and training facility. The onsite meeting and training facility is well-equipped with multiple smart screens, the ability to live stream and simulcast, and an IP-based system in place for visitors to connect devices.

2. Current Software Solutions

a. CSC Leon maintains a Microsoft Office 365 G3 subscription for all internal users. This license includes Word, Outlook, Excel, PowerPoint, OneNote, and Access. CSC Leon also has a single Power BI license and 10 Microsoft Office 356 G1 (Outlook only) subscriptions for its council members.
b. CSC Leon currently utilizes Share Point under its Microsoft 365 G3 subscription in lieu of a business server.
c. CSC Leon currently uses a combination of cloud-based survey tools (e.g., Survey Monkey, Google Forms, etc.) and Office 356 applications for grant application completion, reporting and data storage. CSC Leon currently has 5 internal users and 29 external users at outside agencies operating 30 individual programs.

d. CSC Leon contracts with an outside CPA, Grayson Accounting & Consulting, P.A., who uses cloud-based QuickBooks to manage most of the finance and accounting operations.

e. CSC Leon uses Bill.com and Paychex for its remaining accounting functions. It maintains 3 user licenses for each currently.

f. CSC Leon uses Wordpress to maintain a basic website that includes a single lead generation widget for Send in Blue. To date, CSC Leon has not fully deployed Send in Blue for the purposes of a customer relations management tool nor for marketing or communications. We currently maintain an active list of approximately 300 contacts. We anticipate this to grow substantially.

3. Hardware and Connectivity

a. CSC Leon currently has 4 laptop computers, 2 networked Toshiba MFP copier/scanner/fax machines and 2 networked HP color laser printers that are used by its staff members for daily operations.

b. A hardwired firewall is in use between the local network and the internet. Both an internal wireless network and a guest wireless network are available.

c. CSC Leon’s Internet connection will be provided by Comcast – Business Internet Bundle 300 MB download with 5 static IPs, 1 voice line, and basic cable tv. A VOIP phone system will be in use.

4. Managed Services

a. CSC Leon does not currently contract with a managed service provider but is exploring local options for IT support.

5. External Stakeholders

a. All external agencies that apply for funding from CSC Leon will be expected to use several elements of the newly developed modules or system applications. Currently, approximately 60 agencies have previously applied for funding. Out of those applicants, 28 agencies received funding. The number of new agencies applying for funding is expected to increase each year.

b. Agencies request funding for the services offered to the community, which are referred to as “programs.” Of the 28 agencies that received funding thus far, there are 30 programs. Most times, an agency will run a single program. There are agencies that run multiple programs. There are a few programs that are managed by multiple agencies; in these instances, CSC Leon will provide funding to a designated primary agency. Each of the agencies has varying access to current technology and each possesses varying degrees of technological capacity (operating knowledge). Many agencies are small non-profits with limited technical infrastructure and abilities.

6. *Future Software Solutions*
   a. CSC Leon desires to work with existing community partner database systems to develop data sharing agreements and processes to better serve clients. While this explicit function is not covered in the parameters of this specific RFP, CSC Leon desires to select a vendor that is open to developing these relationships and providing cost-effective integration services in the future. These partners and their respective systems include:
      i. 2-1-1 of the Big Bend (Well Sky)
      ii. Leon County Sheriff's Office (SPIRIT)
      iii. Leon County and City of Tallahassee Community Human Services Partnership
      iv. Capital Area Healthy Start Coalition (Healthy Start Monitoring and Evaluation Data System)
      v. Early Learning Coalition of the Big Bend (WELS)
      vi. Leon County Schools (multiple)

SECTION 2 – VENDOR IT ENVIRONMENT RESPONSIBILITIES

To be effective, the technological infrastructure, policies, and practices deployed by the Vendor and its associated solution(s) must meet specific criteria.

A. Vendor Hosted

Confirm that the proposal is for a Vendor Hosted solution. **Response:**

B. Data Security, Retention and Removal

The data collected and stored in the solution may contain sensitive information and therefore require specific data security measures.

Describe how identified components will maintain compliance with requirements in the **SCHEDULE E - Data Security Requirements**. **Response:**

With reference to Rule 60GG-2.003, explain how Respondent will meet the requirements for Access Control and Authentication.

Response:

C. Data Retention and Removal

CSC Leon will need to retain all data beyond the length of the Contract unless otherwise directed by CSC Leon. It may need the ability to delete data, even data that may be stored off-line or in backups. More importantly, CSC Leon will need to the ability to retrieve data, even data that may be stored off-line or in backups.

Explain how the data retention, deletion and retrieval requirements will be met and describe data management capabilities (storage limitations, duration, etc.).

Response:

Explain how Vendor will be able to support the current and future growth of the proposed solution's data capacity.

Response:

D. Disaster Recovery Plan

SCHEDULE F – Disaster Recovery Plan; Vendor must provide CSC Leon with a detailed Disaster Recovery Plan that details how the following minimum data security areas will be handled.

- Back-up and Recovery:
    1. Organization policy and procedures authorizing this activity.
    2. The roles and responsibilities within the organization and the integration of activities with any affiliated organizations also responsible for back-up and recovery.
    3. Training and awareness of staff and contracted employees.
    4. The most recent back up/fail-over test date at the time of submission.
    5. Priority for the recovery and reconstitution of activities.

- Incident Handling:
    1. Organization policy and procedures authorizing this activity and covering the areas of preparation, detection and analysis, containment, eradication, reporting and recovery.
    2. Roles and responsibilities with the organization and affiliated organizations.
    3. Training and awareness of staff and contracted employees.
    4. Description of the implementation of secure communications such as a description of software tool(s) used for tracking and documenting the incident or disaster.
- Disaster Recovery Planning:
    1. Identification of the organization’s business functions, recovery objectives, restoration priorities, and metrics of evaluation.
    2. Organization policy and procedures authorizing this activity and covers the areas of preparation, detection and analysis, containment, eradication, and recovery.
    3. Roles and responsibilities with the organization and affiliated organizations.
    4. Training and awareness practices of staff and contracted employees.
    5. The most recent disaster recovery/contingency plan test date at time of submission.
    6. Methods used to identify deficiencies and corrective actions from the most recent disaster/contingency plan test and the status of corrective actions.
    7. Description of the implementation of secure communications such as a description of software tool(s) used for tracking and documenting the incident or disaster.
    8. Identification and use of alternate storage and process sites for business continuity.
    9. Protections and recovery planning for ransomware attacks.

Response:

Submit the above supporting documentation with the Proposal. If considered “trade secret” or otherwise confidential, label accordingly.

E. Component Matrix

Describe each of the components maintained by the Vendor in its IT environment that would be specifically utilized to support the proposed solution(s).	
Facilities – Physical buildings containing Infrastructure and supporting services, including physical access security, power connectivity and generators, HVAC systems, communications connectivity access and safety systems such as fire suppression.	**Response:**
Infrastructure – Hardware, firmware, software, and networks, provided to develop, test, deliver, monitor, manage, and support IT services which are not included under Platform and Application.	**Response:**
Platform – Computing server software components including operating system (OS), middleware (e.g., Java runtime, .NET runtime, integration, etc.), database and other services to host applications.	**Response:**
Application – Software programs which provide functionality for end user and Vendor services.	**Response:**

Storage – Physical data storage devices, usually implemented using virtual partitioning, which store software and data for IT system operations.	**Response:**
Backup – Storage and services that provide online and offline redundant copies of software and data.	**Response:**
Development - Process of creating, testing and maintaining software components.	**Response:**
Identify any subcontractor(s) used for the components in the table above. Provide additional information if the table above does not adequately identify the division of responsibilities. **Response:**	

SECTION 3 – ADA COMPLIANCE

All websites, applications, software, and associated content and documentation provided by the Vendor as part of the Solution must comply with Level AA of the World Wide Web Consortium (W3C) Web Content Accessibility Guidelines (WCAG) 2.0.

Provide a description of conformance with WCAG 2.0 Level AA specifications by providing a completed Product Accessibility Template (PAT) for the Solution. If the Solution is comprised of multiple products, provide a PAT for each product (or verification of conformance certified by an industry-recognized third-party). If including any third-party products in the Solution, obtain and provide the third-party PATs as well. Each PAT must state exactly how the product meets the specifications. Explain fully any “Not Applicable” (N/A) responses. Address each standard individually and with specificity. Clarify whether conformance is achieved throughout the entire product (for example – user functionality, administrator functionality, and reporting), or only in limited areas. Describe the evaluation methods used to support WCAG 2.0 Level AA conformance claims, including, if applicable, any third-party testing.

For each product that does not fully conform to WCAG 2.0 Level AA, provide detailed information regarding the plan to achieve conformance, including timelines. Provide details of how they will meet these requirements.

Response:

SECTION 4 – USER TYPE AND CAPACITY

The proposed solution(s) must be able to support the number of concurrent users as defined below, and the ability to restrict access permissions by user and report type. Solution must meet the expected number of concurrent Users.

Type of User	Access Type	Number of Users	Number of Concurrent Users
Applicant	Read and write	Unlimited	Unknown
Grantee	Read, write, and edit	60	60
Reviewer	Read and write	20	20
Evaluator	Read, write, and edit	8	5
Staff	Read, write, edit, assign users, assign controls	10	5
Administrator	Full administrative rights	3	2

A. **Concurrent Users**

Explain how the solution will be able to support the expected number of concurrent users. Explain whether the solution can scale up or down without affecting performance.

Response:

B. **Latency**

Provide details regarding latency response time (e.g., Generate Page Load, standardized reporting, ad hoc reporting). Identify what network connectivity or equipment will CSC Leon be required to have to meet the expected latency response time.

Response:

SECTION 5 – END USER AND CLIENT OPERATING ENVIRONMENT

The Vendor must accommodate the latest browser versions (including mobile browsers) as well as some pre-existing browsers. To ensure that users with older browsers are still able to access online services, applications must, at a minimum, display and function correctly in standards-compliant browsers without the use of special plugins or extensions.

A. Optimal Environment

Describe the optimal IT environment based on the environment choices set forth above.

Response:

B. System Access

Describe any CSC Leon system access requirements that are necessary for Vendor to perform its obligations on a timely basis, including but not limited to, physical or remote access to CSC Leon networks, servers, or individual workstations.

Response:

C. Use of Plug-Ins

Identify any plug-ins necessary for the proposed solution(s) to meet the system requirements of this request.

Response:

D. Mobile Responsiveness

Describe the level of responsive design practices deployed by the Vendor to maximize use of the proposed solution across devices.

Response:

E. Change Communications

Describe how Vendor communicates changes to its software and architecture.

Response:

F. Collaborative Decision-Making

Describe how customers collaborate with Vendor in the decision-making process for upgrades, maintenance, and change control.

Response:

SECTION 6 – BUSINESS MODULES

The proposal must include an integrated solution for the specific business functions identified in Section 1.B.

A. Grant Making & Contract Management

Describe in detail the proposed solution(s), including, but not limited to, a description of the Software (name, type, version, release number, etc.), its functionality including the information architecture and functional design of the system, such as functionality maps, architectural maps, training materials, visual aids including screen shots, actions performed by the system, and any behind the scenes processing, optional add-on modules and plugins.

The level of detail provided should be such so that anyone is able to read it and understand how the software works.

Clearly define the Vendor's services and the solution's ability to be rapidly configured or scaled as CSC Leon's business or technical demands change.

Response:

B. Performance Measurement and Information Management

Describe in detail the proposed solution(s), including, but not limited to, a description of the Software (name, type, version, release number, etc.), its functionality including the information architecture and functional design of the system, such as functionality maps, architectural maps, training materials, visual aids including screen shots, actions performed by the system, and any behind the scenes processing, optional add-on modules and plugins.

The level of detail provided should be such so that anyone is able to read it and understand how the software works.

Clearly define the Vendor's services and the solution's ability to be rapidly configured or scaled as CSC Leon's business or technical demands change.

Response:

C. Customer Relationship Management

Describe in detail the proposed solution(s), including, but not limited to, a description of the Software (name, type, version, release number, etc.), its functionality including the information architecture and functional design of the system, such as functionality maps, architectural maps, training materials, visual aids including screen shots, actions performed by the system, and any behind the scenes processing, optional add-on modules and plugins.

The level of detail provided should be such so that anyone is able to read it and understand how the software works.

Clearly define the Vendor's services and the solution's ability to be rapidly configured or scaled as CSC Leon's business or technical demands change.

Response:

D. Unique Software Requirements

Identify any unique software requirements to fulfill the terms of the Contract.

Response:

E. Unique System Requirements

Describe any unique system access requirements that are necessary for Vendor to perform its obligations on a timely basis, including but not limited to, physical or remote access to CSC Leon networks, servers, or individual workstations.

Response:

F. Licensing Structure

Describe the licensing structure for each software title required to fulfill the terms of the Contract.

Response:

G. Third Party Components

Identify any third-party components, including open-source components included with or used in connection with the proposed solution.

Response:

H. Mobile Responsiveness

Provide list of features that can be performed via a mobile device, identifying, if applicable, which mobile browsers are compatible.

Response:

I. Additional Products and Services

Describe additional solution functionality, products or services that the CSC Leon specifications do not address but are necessary to implement and support this solution.

Response:

SECTION 7 – INTEGRATION SERVICES

The proposal must include specific details on how each business module integrates with each other business module, existing software, and the Vendor's approach to managing integration services, including legacy data migration.

A. Proposed Business Modules

Explain how the proposed solution(s) will integrate the required business modules to each other. Include the proposed architectural map between modules.

Response:

B. BILL.COM

Current Technology	BILL.COM
Current Business Function	Accounts payable
Desired Business Integration	Task flow Management
Volume of Data	Approximately 15 months of weekly, monthly and one-time transactions
Format of the input & export files	Raw data (.CSV, .XLS)

Explain how the proposed solution(s) will integrate to this existing thirty-party solution. **Response:**
Explain in detail how and what services are required to migrate the data from the current technology. **Response:**

C. Microsoft Office 365

Current Technology	MS Office including Outlook, Word, Excel, Powerpoint, Planner
Business Function	Basic office management, email communication, data processing, storage, task flow management
Desired Business Integration	Customer interaction tracking, specifically for help requests, deliverables, applications, etc.
Volume of Data	18 months of email data, attachments, files, presentations, etc.
Format of the input & export files	Varies
Explain how the proposed solution(s) will integrate to this existing thirty-party solution. **Response:**	
Explain in detail how and what services are required to migrate the data from the current technology. **Response:**	

D. Wordpress

<table>
<tr><td>Current Technology</td><td>Wordpress</td></tr>
<tr><td>Business Function</td><td>Public facing web presence used to communicate announcements, job postings, procurement opportunities, and public information repository</td></tr>
<tr><td>Desired Business Integration</td><td>Customer interaction portal access for applications, trainings, newsletters, public information, etc.</td></tr>
<tr><td>Volume of Data</td><td>18 months of meeting information, press and procurement announcements</td></tr>
<tr><td>Format of the input & export files</td><td>Primarily PDF, text and image-based files</td></tr>
<tr><td colspan="2">Explain how the proposed solution(s) will integrate to this existing thirty-party solution.

Response:</td></tr>
<tr><td colspan="2">Explain in detail how and what services are required to migrate the data from the current technology.

Response:</td></tr>
</table>

E. General Integration Services

Explain how Vendor will be able to support CSC Leon's future goals of the proposed solution's ability to integrate with other third-party systems. Include descriptions of relevant experience. Provide the cost for such services in the price sheet.

Response:

SECTION 8 – TRAINING SERVICES

Vendor must provide administration and end-user training for implementation, go-live support, and transition to User self-sufficiency.

Describe available training options and include details such as: typical class size, materials to be provided, class duration, on-site or web based. Provide a training plan for go-live support and transition to self-support, including options and details such as the number of dedicated personnel, staff location, hours available and duration of go-live support.

Response:

Provide details on, and examples of, clearly written instructions and documentation to enable CSC Leon administrators and end Users to successfully operate the Solution without needing to bring in additional Vendor support.

Response:

SECTION 9 – DOCUMENTATION

Vendor must provide all user manuals, operating manuals, technical manuals and any other instructions, specifications, documents or materials, in any form or media, that describe the functionality, installation, testing, operation, use, maintenance, support, technical or other components, features or requirements of the Software.

Vendor must develop and submit for CSC Leon approval complete, accurate, and timely Solution documentation to support all Users, and must update any discrepancies, or errors through the life of the Contract.

Vendor's user documentation must provide detailed information about all software features and functionality, enabling CSC Leon to resolve common questions and issues prior to initiating formal support requests.

Provide details on, and examples of, documentation to meet the requirements set forth in this section.

Response:

SECTION 10 – VENDOR PERSONNEL

CSC Leon recognizes that a strong implementation team is critical to the success of this Contract. Please complete each section in its entirety and include an organizational chart identifying, at minimum, all listed team members.

A. Contract Administrator

Please identify the individual who is responsible to (a) administer the terms of this Contract, and (b) approve and execute any Change Notices under this Contract.

Name:
Address:
Phone:
Email:

B. Key Personnel

The Vendor's Project Manager, Implementation Leader, and Security Officer are designated as Key Personnel. Provide the names, contact details and resumes for these positions.

Vendor Project Manager. Vendor resource who serves as the primary contact with regard to all services and has authority to act on behalf of the Vendor in matters pertaining to the implementation and technical assistance services.

Name:
Address:
Phone:
Email:

Vendor Implementation Leader. Vendor resource who serves as the primary contact with regard to technical implementation services. This individual will gain advanced knowledge of CSC Leon's business needs in order to facilitate the development, customization, and/or configuration of necessary components to implement a fully conforming and robust solution(s).

Name:
Address:
Phone:
Email:

Vendor Security Officer. Vendor resource who is responsible to respond to CSC Leon inquiries regarding the security of the Vendor's solution(s). This individual must have sufficient knowledge of the security of the solution(s) and the authority to act on behalf of Vendor in security matters.

Name:
Address:
Phone:
Email:

C. Other Personnel

In addition to the Key Personnel roles, the Vendor's implementation team must possess sufficient skills, experience, and availability to successfully implement the Solution. Using the table below as a guide, describe the roles, responsibilities, and the skillsets of the team that will implement the solution. Provide names in third column and include resumes in sufficient detail to demonstrate capability to develop and implement a successful solution.

Classification	Responsibility/Skill Set	Name/Years of Experience/ Applicable Experience
Business Analyst	Under the direction of the Implementation Leader will participate in analysis and discovery activities.	
Data Architect	Provides data base architecture, design, and overall data-related solutioning. Provides data mapping for migration	
Technology Related Developers	Under the direction of the Implementation Leader will develop the Solution	
Testing Personnel	Develops test plans, test cases and manages and performs testing activities.	
Training Technical Lead	Develops and delivers training materials and conducts training sessions.	

User Interface and User Experience (UI/UX) Specialist	Ensures that vendor's solution meets CSC Leon's web standards for look-and-feel and accessibility.	
Customer Success Specialist	Responds to queries and requests for technical assistance in a timely and supportive manner	

D. Background Checks

Upon contract award, Vendor must present certifications evidencing satisfactory background checks for all staff identified for assignment to this project. Vendor will pay for all costs associated with ensuring its staff meets all requirements.

SECTION 11 – DISCLOSURE OF SUBCONTRACTORS

If the Vendor intends to utilize subcontractors, the Vendor must disclose the following:

- The legal business name; address; telephone number; a description of subcontractor's organization and the services it will provide; and information concerning subcontractor's ability to provide the Contract Activities.
- The relationship of the subcontractor to the Vendor.
- Whether the Vendor has a previous working experience with the subcontractor. If yes, provide details of that previous relationship.
- A complete description of the Contract activities that will be performed or provided by the subcontractor.
- CSC Leon strongly supports and encourages diversity and participation of historically disadvantaged business enterprises in contracting, as evidenced in the CSC Leon Purchasing Policy. Attach any evidence of firm certification by the *Minority, Women, and Small Business Enterprise Division of the Office of Economic Vitality* or comparable public body and identify the qualifying individuals. Non-certified firms may highlight individual investments, e.g., the number and percentage of professionals who are minorities or women.

Confirm review of the above requirements by completing the table below (use “none” where appropriate).	
The legal business name, address, telephone number of the subcontractor(s).	Response:
A description of subcontractor’s organization and the services it will provide and information concerning subcontractor’s ability to provide the Contract activities.	Response:
The relationship of the subcontractor to Vendor.	Response:
Whether Vendor has a previous working experience with the subcontractor. If yes, provide the details of that previous relationship.	Response:
A complete description of the Contract activities that will be performed or provided by the subcontractor.	Response:
Of the total bid, the price of the subcontractor’s work.	Response:
Minority, Women, and Small Business Enterprise details.	Response:

SECTION 12 – CSC LEON RESOURCES/RESPONSIBILITIES

CSC Leon will provide the following resources as part of the implementation and ongoing support of the Solution.

CSC Leon Contract Administrator. The CSC Leon Contract Administrator will (a) administer the terms of this Contract, and (b) approve and execute any Change Notices under this Contract.

CSC Leon Contract Administrator
Name: Dina Snider Email: dsnider@cscleon.org

CSC Leon Project Manager. The CSC Leon Project Manager will approve all Deliverables and day-to-day activities.

CSC Leon Project Manager
Name: Holly McPhail **Email: hmcphail@cscleon.org**

SECTION 13 – PROJECT MANAGEMENT

A. Methodology

CSC Leon is requesting an implementation approach that closely aligns with Agile Scrum Methodology and includes comparable artifacts and ceremonies that are properly implemented. An approach with iterative build and review cycles and core team involvement are more likely to meet CSC Leon's expectations and will provide greater overall project success. The State of Florida has invested significant effort in developing project management resources, which CSC Leon deems are suitable for this project, and which are available at: https://www.dms.myflorida.com/other_programs/project_management_and_oversight

Describe the Vendor's Project Management and Implementation Approach and explain how the selected methodology will guide the development of each business module from kick-off to go-live and beyond. Highlight the key elements and personnel responsibilities in detail, including expectations for CSC Leon team members and stakeholders. **Response:**
Describe use of project management and application lifecycle management tools, including activity assignment and tracking. **Response:**

B. Meetings

At start of the engagement, the Vendor Project Manager must facilitate a project kick off meeting with the support from the CSC Leon Project Manager and any other identified CSC Leon resources to review the approach to accomplishing the project, schedule tasks and identify related timing, and identify any risks or issues related to the planned approach. From project kick-off until final acceptance and go-live, the Vendor Project Manager must facilitate weekly meetings (or more if determined necessary by the parties) to provide updates on the project implementation progress. Following go-live, Vendor must facilitate monthly meetings (or more or less if determined necessary by the parties) to ensure ongoing support success.

Vendor must attend the following meetings, at a location and time as identified by CSC Leon, at no additional cost to CSC Leon:

1. Kick off meeting
2. Project planning sessions
3. Discovery/Requirements and analysis meetings
4. Ongoing collaborative team meetings to facilitate discovery and development (e.g., team meetings, sprint planning, sprint reviews, sprint retrospectives, user story workshops, backlog grooming, etc.)
5. All other meetings needed to successfully implement the Solution.
6. Security plan assessment and review sessions

C. Project Control and Reports

Once the Project Kick-Off meeting has occurred, the Vendor Project Manager and Implementation Lead will monitor the project implementation progress and report on a weekly basis to the CSC Leon Project Manager the following:

1. Progress to completed milestones, comparing forecasted completion dates to planned and actual completion dates.
2. Accomplishments during the reporting period, what was worked on and what was completed during the current reporting period.
3. Indicate the number of hours expended during the past week, and the cumulative total to date for the project.
4. Tasks planned for the next reporting period.
5. Identify any existing issues which are impacting the project and the steps being taken to address those issues.
6. Identify any new risks and describe progress in mitigating high impact/high probability risks previously identified.
7. Indicate the amount of funds expended during the current reporting period, and the cumulative total to date for the project.

The report will include other information relevant for the delivery of the program as may be agreed upon between the Vendor Project Manager and the CSC Leon Project Manager within the project management plan.

Describe specific reports the Vendor will provide after contract execution and during the lifecycle of the contract, including all required scheduled reporting and details around the how and when metrics are captured/validated.

Response:

D. Discovery Phase

The implementation approach should include a comprehensive discovery phase resulting in a design and development roadmap demonstrating a complete understanding of CSC Leon business processes and RFP goals.

Detail the discovery phase process including requirements validation and tracing, analysis, design, and product backlog development leading to the publication of a design and development roadmap to meet the project requirements.

Response:

E. Change Requests

Once the development roadmap is set, any items later added or removed from the Baseline Product Backlog will be considered a change. Change is defined as a New Product Backlog Item or Change to Existing Product Backlog Item.

Changes to scope, schedule or cost must be addressed through a formal extraordinary change request process with CSC Leon and Vendor to ensure understanding, agreement and approval of authorized parties to the change and clearly identify the impact to the overall project.

1. **Standard Product Backlog Change Process.** Vendor and CSC Leon will address standard changes within the Agile framework without impact to the overall project by re-prioritization of the Product Backlog. For example, if a new high priority user story is identified during a sprint, CSC Leon can request the new user story be added to a future sprint as long as user story(ies) of equivalent size (level of effort, hours, story points, and sizing factors) are removed from the Product Backlog. Changes to the backlog that increase the overall project scope, level of effort, or timelines for the Go Live, that are not offset by compensating reductions, must be approved following the Extraordinary Change Request process set forth below.

2. **Extraordinary Change Request Process.** If a change will cause the Product Backlog to exceed the baseline Product Backlog size (as defined by story points, level of effort, or other agreed upon sizing factors), then Extraordinary Change Process will conform to the Change Control Process as set forth in the Contract Section 2.2(b) Change Control Process and may require a contract change amendment.

Describe approach to Product Backlog management and Standard Product Backlog changes. **Response:**

F. Testing & Data Migration

The implementation approach should include a comprehensive testing phase and lifecycle data migration as part of its Go Live plan for each business module deployment.

Describe the Vendor’s testing phase including interface design, training, user acceptance, data migration, and all other activities required to complete the project. **Response:**
Describe how Vendor will work with the CSC Leon to configure fields, statuses, test cases, and other items to allow lifecycle management data of each business module to be migrated at prescribed intervals and at project completion. **Response:**

G. Authority to Operate

During the development of the system and prior to go-live, a security accreditation process, resulting in an “Authority to Operate,” will be performed. Vendor will assist with this comprehensive process, at no cost to CSC Leon, and provide answers to the vendor-specific and solution-specific questions.   The Implementation Approach must also consider the Americans with Disabilities Act Compliance as described in Section 5 and include the review and mitigation activities also at no cost to CSC Leon.

H. Milestone Schedule

The Vendor Project Manager will be responsible for maintaining a project schedule (or approved alternative) identifying tasks, durations, forecasted dates and resources required from both the Vendor and CSC Leon to meet the timeframes as agreed to by both Parties.

To aid in the full project schedule development, the CSC Leon's proposed milestone schedule and associated deliverables from each sprint are set forth on the following page. An "X" indicates which of the three business modules are associated with the relevant milestone deliverable listed.

1. Grant Making & Contract Management
2. Performance Measurement and Information Management
3. Customer Relationship Management

While the schedule lists a final deliverable for each milestone phase or sprint, it is important to note that each milestone phase or sprint should also include standard artifacts associated with agile scrum methodology or a similar project management methodology including daily scrums, backlog clearing, testing, training, data migration (as needed), implementation, etc. It is also important to note that because CSC Leon requires an incremental implementation schedule, that a final go/no go phase commonly associated with software development is not present in the schedule below. However, for the purposes of the solution warranty, the "go live" release date of the final function would serve as the final production date and trigger the 90-day warranty period.

Milestone Event	Milestone Deliverable(s)	Associated Business Module(s)			Schedule	Date
		1	2	3		
Project Planning & Team Assembly	Project Kickoff Meeting	X	X	X	Contract Execution + 10 calendar days	December 10
Discovery	Design and Development Roadmap Including Baseline Backlogs for Each Business Module	X	X	X	Contract Execution + 30 calendar days	December 31
Sprint 0	OTS Release of Basic CRM and Event Sign Up/Tracking			X	2 weeks	January 16
Sprint 1	OTS Release of Grant Application Function	X			2 weeks	January 30
Sprint 2	OTS Request for Technical Assistance with Task Flow Management			X	2 weeks	February 13
Sprint 3	Release of Demographic and Basic Client Data Collection Portal	X	X	X	3 weeks	March 6
Sprint 4	OTS Release of Task Management/Decision Support/Application Review Function	X		X	2 weeks	March 20
Sprint 5	Release of Fiscal Activity Tracking and Reporting Function; Release of Campaign Management Tool	X	X	X	4 weeks	April 17

Sprint 6	Release of Contract Award and Execution Function, Release of Contract Deliverable Tracking Function	X		X	2 weeks	May 1
Sprint 7	Release of Performance Data Collection Portal	X	X	X	2 weeks	May 15
Sprint 8	Release of Post-event Certificate Issuance Function	X		X	1 week	May 22
Sprint 9	Release of Performance Measurement Reporting Function		X		4 weeks	June 19
Sprint 10	Release of Performance Measurement Display Function		X	X	3 weeks	July 10
Sprint 11	Release of 3rd Party Data Acquistion Tool		X		5 weeks	August 14
Sprint 12	Release of Community Data Comparison Tool		X	X	3 weeks	September 1
Post Production	Warranty	X	X	X	Production + 90 calendar days	November 30
Project Closeout	No Open Issues Remain	X	X	X	15 days	December 15
Integration Services	As needed	X	X	X	Ongoing	As needed
Maintenance & Support	As needed	X	X	X	Ongoing	Annual Renewal

Vendor may propose alternative timeframes and deliverables but must provide an explanation as to why CSC Leon’s schedule and associated deliverables are not feasible.

Response:

Provide a Work Breakdown Structure (WBS) or similar tool that corresponds with the milestone dates set forth above (or with alternatively proposed schedule). The WBS must be detailed enough to identify all CSC Leon and Vendor responsibilities.

Response:

SECTION 14 – ADDITIONAL INFORMATION

CSC Leon reserves the right to purchase any additional services or products from Vendor during the duration of the Contract.

CSC LEON INTEGRATED INFORMATION MANAGEMENT SOLUTION PRICING SHEET

VENDOR(S):	
PRODUCT(S):	
	PRICING ESTIMATE
INITIAL LICENSING - PRIMARY APPLICATION (INSERT NEW LINES TO ITEMIZE AS NEEDED)	
TOTAL Licensing - Primary Application	**$ -**
INITIAL LICENSING - SECONDARY ACCOMPANYING APPLICATIONS (INSERT NEW LINES TO ITEMIZE AS NEEDED)	
TOTAL Licensing - Accompanying Applications	**$ -**
IT ENVIRONMENT - HW & CLOUD (INSERT NEW LINES TO ITEMIZE AS NEEDED)	
TOTAL - Hardware & Infrastructure	**$ -**
LICENSING - SERVER AND OS (INSERT NEW LINES TO ITEMIZE AS NEEDED)	
TOTAL Licensing - Server and OS	**$ -**
VENDOR/PARTNER PROFESSIONAL SERVICES & EXPENSES INCLUDING PROJECT MANAGEMENT, TRAINING, INTEGRATION SERVICES, DATA MIGRATION, ETC. (INSERT NEW LINES TO ITEMIZE AS NEEDED)	
TOTAL - Vendor Professional Services & Expenses	**$ -**

ON SITE WORK TRAVEL EXPENSES (INSERT NEW LINES TO ITEMIZE AS NEEDED)	
Airfare	
Ground Transportation & Parking	
Accomodations	
Other -OR- Aggregated Travel Estimates	
In Route Travel Expenses	
TOTAL - On Site Work Travel Expenses	**$ -**
DISCOUNTS BEING EXTENDED	
TOTAL - Discounts Being Extended	**$ -**
ANNUAL FEES - LICENSING (INSERT NEW LINES TO ITEMIZE AS NEEDED)	
TOTAL Annual Fees - Maintenance & Hosting	**$ -**
ANNUAL FEES - MAINTENANCE & HOSTING (INSERT NEW LINES TO ITEMIZE AS NEEDED)	
TOTAL Annual Fees - Maintenance & Hosting	**$ -**
ESTIMATED FEES - CONTIGENCY, FUTURE INTEGRATION SERVICES AND/OR ONGOING IMPROVEMENTS (INSERT NEW LINES TO ITEMIZE AS NEEDED)	
TOTAL - Estimated Other Personnel/Support	**$ -**

TOTAL PROJECT COST	
INITIAL LICENSING - PRIMARY APPLICATION (INSERT NEW LINES TO ITEMIZE AS NEEDED)	$ -
INITIAL LICENSING - SECONDARY ACCOMPANYING APPLICATIONS (INSERT NEW LINES TO ITEMIZE AS NEEDED)	$ -
IT ENVIRONMENT - HW & CLOUD (INSERT NEW LINES TO ITEMIZE AS NEEDED)	$ -
LICENSING - SERVER AND OS (INSERT NEW LINES TO ITEMIZE AS NEEDED)	$ -
VENDOR/PARTNER PROFESSIONAL SERVICES & EXPENSES INCLUDING PROJECT MANAGEMENT, TRAINING, INTEGRATION SERVICES, DATA MIGRATION, ETC. (INSERT NEW LINES TO ITEMIZE AS NEEDED)	$ -
ON SITE WORK TRAVEL EXPENSES (INSERT NEW LINES TO ITEMIZE AS NEEDED)	$ -
DISCOUNTS BEING EXTENDED	$ -
Total Project Cost (Initial or 1-Year Total Cost of Ownership)	**$ -**
ANNUAL FEES - LICENSING (INSERT NEW LINES TO ITEMIZE AS NEEDED)	$ -
ANNUAL FEES - MAINTENANCE & HOSTING (INSERT NEW LINES TO ITEMIZE AS NEEDED)	$ -
ESTIMATED FEES - CONTIGENCY, FUTURE INTEGRATION SERVICES AND/OR ONGOING IMPROVEMENTS (INSERT NEW LINES TO ITEMIZE AS NEEDED)	$ -

SCHEDULE C - INSURANCE REQUIREMENTS

a. **General Requirements.** Contractor, at its sole expense, must maintain the insurance coverage as specified herein for the duration of the Term. Minimum limits may be satisfied by any combination of primary liability, umbrella or excess liability, and self-insurance coverage. To the extent damages are covered by any required insurance, Contractor waives all rights against CSC Leon for such damages. Failure to maintain required insurance does not limit this waiver.

b. **Qualification of Insurers.** Except for self-insured coverage, all policies must be written by an insurer with an A.M. Best rating of A- VII or higher unless otherwise approved by CSC Leon.

c. **Primary and Non-Contributory Coverage.** All policies for which CSC Leon is required to be named as an additional insured must be on a primary and non-contributory basis.

d. **Claims-Made Coverage.** If any required policies provide claims-made coverage, Contractor must:

   a. Maintain coverage and provide evidence of coverage for at least 3 years after the later of the expiration or termination of the Contract or the completion of all its duties under the Contract;

   b. Purchase extended reporting coverage for a minimum of 3 years after completion of work if coverage is cancelled or not renewed, and not replaced with another claims-made policy form with a retroactive date prior to the Effective Date of this Contract.

e. **Proof of Insurance.**

   a. Insurance certificates showing evidence of coverage as required herein must be submitted to CSC Leon within 10 days of the Contract Effective Date.

   b. Renewal insurance certificates must be provided on annual basis or as otherwise commensurate with the effective dates of coverage for any insurance required herein.

   c. Insurance certificates must be in the form of a standard ACORD Insurance Certificate unless otherwise approved by CSC Leon.

   d. All insurance certificates must clearly identify the Contract Number (e.g., notated under the Description of Operations on an ACORD form).

   e. CSC Leon may require additional proofs of insurance or solvency, including but not limited to policy declarations, policy endorsements, policy schedules, self-insured certification/authorization, and balance sheets.

   f. In the event any required coverage is cancelled or not renewed, Contractor must provide written notice to CSC Leon no later than 5 business days following such cancellation or nonrenewal.

f. **Subcontractors.** Contractor is responsible for ensuring its subcontractors carry and maintain insurance coverage.

g. **Limits of Coverage & Specific Endorsements.**

Required Limits	Additional Requirements
Commercial General Liability Insurance	
Minimum Limits: **$1,000,000 Each Occurrence** **$1,000,000 Personal & Advertising Injury** **$2,000,000 Products/Completed Operations** **$2,000,000 General Aggregate**	Contractor must have policy endorsed to add "the Children's Service Council of Leon County, its officers, employees, and agents" as additional insureds using endorsement CG 20 10 11 85, or both CG 20 10 12 19 and CG 20 37 12 19.
Automobile Liability Insurance	
If a motor vehicle is used in relation to Contractor's performance, Contractor must have vehicle liability insurance on the motor vehicle for bodily injury and property damage as required by law.	
Workers' Compensation Insurance	
Minimum Limits: **Coverage according to applicable laws governing work activities.**	Waiver of subrogation, except where waiver is prohibited by law.
Privacy and Security Liability (Cyber Liability) Insurance	
Minimum Limits: **$1,000,000 Each Occurrence** **$1,000,000 Annual Aggregate**	Contractor policy must cover information security and privacy liability, privacy notification costs, regulatory defense and penalties, and website media content liability.
Professional Liability (Errors and Omissions) Insurance	
Minimum Limits: **$3,000,000 Each Occurrence** **$3,000,000 Annual Aggregate**	

h. **Non-Waiver.** This Schedule C is not intended to and is not to be construed in any manner as waiving, restricting or limiting the liability of either party for any obligations under this Contract, including any provisions hereof requiring Contractor to indemnify, defend and hold harmless CSC Leon.

SCHEDULE D – SERVICE LEVEL AGREEMENT

1. Definitions

For purposes of this Schedule, the following terms have the meanings set forth below. All initial capitalized terms in this Schedule that are not defined in this **Schedule** shall have the respective meanings given to them in the Contract. "**Actual Uptime**" means the total minutes in the Service Period that the Hosted Services are Available.

"**Availability**" has the meaning set forth in **Section** Error! Reference source not found..

"**Availability Requirement**" has the meaning set forth in **Section** Error! Reference source not found..

"**Available**" has the meaning set forth in **Section** Error! Reference source not found..

"**Contact List**" means a current list of Contractor contacts and telephone numbers set forth in the attached **Schedule D – Attachment 1** to this Schedule to enable CSC Leon to escalate its Support Requests, including: (a) the first person to contact; and (b) the persons in successively more qualified or experienced positions to provide the support sought.

"**Corrective Action Plan**" has the meaning set forth in **Section 3.9**.

"**Critical Service Error**" has the meaning set forth in **Section 3.5**.

"**Exceptions**" has the meaning set forth in **Section 2.2**.

"High Service Error" has the meaning set forth in **Section 3.5.**

"**Low Service Error**" has the meaning set forth in **Section 3.5**.

"**Medium Service Error**" has the meaning set forth in **Section 3.5**.

"**Resolve**" has the meaning set forth in **Section 3.6**.

"**RPO**" or "**Recovery Point Objective**" means the maximum amount of potential data loss in the event of a disaster.

"RTO" or **"Recovery Time Objective**" means the maximum period of time to fully restore the Hosted Services in the case of a disaster.

"**Scheduled Downtime**" has the meaning set forth in **Section 2.3**.

"**Scheduled Uptime**" means the total minutes in the Service Period.

"**Service Availability Credits**" has the meaning set forth in **Section 2.6**.

"**Service Error**" means any failure of any Hosted Service to be Available or otherwise perform in accordance with this Schedule.

"**Service Level Credits**" has the meaning set forth in **Section 3.8**.

"**Service Level Failure**" means a failure to perform the Software Support Services fully in compliance with the Support Service Level Requirements.

"**Service Period**" has the meaning set forth in **Section 2.1**.

"**Software Support Services**" has the meaning set forth in **Section 3**.

"**CSC Leon Systems**" means the information technology infrastructure, including the computers, software, databases, electronic systems (including database management systems) and networks, of CSC Leon or any of its designees.

"**Support Hours**" means 8:00 a.m. to 5:00 p.m. ET.

"**Support Request**" has the meaning set forth in **Section 3.5**.

"**Support Service Level Requirements**" has the meaning set forth in **Section 3.4.**

2. Service Availability and Service Availably Credits.

2.1 Availability Requirement. Contractor will make the Hosted Services and Software Available, as measured over the course of each calendar month during the Term and any additional periods during which Contractor does or is required to perform any Hosted Services (each such calendar month, a "**Service Period**"), at least 99.98% of the time, excluding only the time the Hosted Services are not Available solely as a result of one or more Exceptions (the "**Availability Requirement**"). "**Available**" means the Hosted Services and Software are available and operable for access and use by CSC Leon and its Authorized Users over the Internet in material conformity with the Contract. "**Availability**" has a correlative meaning. The Hosted Services and Software are not considered Available in the event of a material performance degradation or inoperability of the Hosted Services and Software, in whole or in part. The Availability Requirement will be calculated for the Service Period as follows: (Actual Uptime – Total Minutes in Service Period Hosted Services or Software are not Available Due to an Exception) ÷ (Scheduled Uptime – Total Minutes in Service Period Hosted Services or Software are not Available Due to an Exception) x 100 = Availability.

2.2 Exceptions. No period of Hosted Services degradation or inoperability will be included in calculating Availability to the extent that such downtime or degradation is due to any of the following ("**Exceptions**"):

a. Failures of CSC Leon's or its Authorized Users' internet connectivity;

b. Scheduled Downtime as set forth in **Section 2.3**.

2.3 <u>Scheduled Downtime.</u> Contractor must notify CSC Leon at least twenty-four (24) hours in advance of all scheduled outages of the Hosted Services or Software in whole or in part ("**Scheduled Downtime**"). All such scheduled outages will: (a) last no longer than five (5) hours; (b) be scheduled between the hours of 12:00 a.m. and 5:00 a.m., Eastern Time; and (c) occur no more frequently than once per week; provided that Contractor may request CSC Leon to approve extensions of Scheduled Downtime above five (5) hours, and such approval by CSC Leon may not be unreasonably withheld or delayed.

Standard 1 – Production Online Application Availability

Application	**Hours of Availability**	
Non-Public Facing	7am - 6pm Business Days	8am - 5pm Saturdays and Sundays
Public-Facing	24/7	

Sliding Scale Service Availability Credit Structure				
Service Availability Credits	**None**	**10%**	**25%**	**50%**
Service Rate	>=99.5%	<99.5% But >=99%	<99% But >=95%	<95%

2.4 <u>Software Response Time.</u> Software response time, defined as the interval from the time the end user sends a transaction to the time a visual confirmation of transaction completion is received, must be less than two (2) seconds for 98% of all transactions. Unacceptable response times shall be considered to make the Software unavailable and will count against the Availability Requirement.

Standard 2– Online Response Time

Both online inquiry and online update transactions must be achieved within the cumulative transaction response times specified below:

Standard | Metric

A: <2 sec | 91%

B: <3 sec | 93%

C: <4 sec | 95%

D: <5 sec | 97%

Sliding Scale Service Availability Credit Structure				
Service Availability Credits	**None**	**10%**	**25%**	**50%**
Service Rate	100%	N/A	<100%	N/A

2.5 Service Availability Reports. Within thirty (30) days after the end of each Service Period, Contractor will provide to CSC Leon a report describing the Availability and other performance of the Hosted Services and Software during that calendar month as compared to the Availability Requirement. The report must be in electronic or such other form as CSC Leon may approve in writing and shall include, at a minimum: (a) the actual performance of the Hosted Services and Software relative to the Availability Requirement; and (b) if Hosted Service performance has failed in any respect to meet or exceed the Availability Requirement during the reporting period, a description in sufficient detail to inform CSC Leon of the cause of such failure and the corrective actions the Contractor has taken and will take to ensure that the Availability Requirement are fully met.

2.6 Remedies for Service Availability Failures.

a. If the actual Availability of the Hosted Services and Software is less than the Availability Requirement for any Service Period, such failure will constitute a Service Error for which Contractor will issue to CSC Leon the following credits on the fees payable for Hosted Services and Software provided during the Service Period ("**Service Availability Credits**"):

Availability	**Credit of Fees**

≥99.98%	None
<99.98% but ≥99.0%	15%
<99.0% but ≥95.0%	50%
<95.0%	100%

b. Any Service Availability Credits due under this **Section 2.6** will be applied in accordance with payment terms of the Contract.

c. If the actual Availability of the Hosted Services and Software is less than the Availability Requirement in any two (2) of four (4) consecutive Service Periods, then, in addition to all other remedies available to CSC Leon, CSC Leon may terminate the Contract on written notice to Contractor with no liability, obligation or penalty to CSC Leon by reason of such termination.

3. Support and Maintenance Services. Contractor will provide IT Environment Service and Software maintenance and support services (collectively, "**Software Support Services**") in accordance with the provisions of this **Section 3**. The Software Support Services are included in the Services, and Contractor may not assess any additional fees, costs or charges for such Software Support Services.

3.1 Support Service Responsibilities. Contractor will:

a. correct all Service Errors in accordance with the Support Service Level Requirements, including by providing defect repair, programming corrections and remedial programming;

b. provide unlimited telephone support, Monday - Friday, 8:00 a.m. to 5:00 p.m ET.

c. provide unlimited online support 24 hours a day, seven days a week;

d. provide online access to technical support bulletins and other user support information and forums, to the full extent Contractor makes such resources available to its other customers; and

e. respond to and Resolve Support Requests as specified in this **Section 3.**

3.2 Service Monitoring and Management. Contractor will continuously monitor and manage the Hosted Services and Software to optimize Availability that meets or exceeds the Availability Requirement. Such monitoring and management includes:

a. proactively monitoring on a twenty-four (24) hour by seven (7) day basis all Hosted Service functions, servers, firewall and other components of Hosted Service security;

b. if such monitoring identifies, or Contractor otherwise becomes aware of, any circumstance that is reasonably likely to threaten the Availability of the Hosted Service, taking all necessary and reasonable remedial measures to promptly eliminate such threat and ensure full Availability; and

c. if Contractor receives knowledge that the Hosted Service or any Hosted Service function or component is not Available (including by written notice from CSC Leon pursuant to the procedures set forth herein):

(i.) confirming (or disconfirming) the outage by a direct check of the associated facility or facilities;

(ii.) If Contractor's facility check in accordance with clause (i) above confirms a Hosted Service outage in whole or in part: (A) notifying CSC Leon in writing pursuant to the procedures set forth herein that an outage has occurred, providing such details as may be available, including a Contractor trouble ticket number, if appropriate, and time of outage; and (B) working all problems causing and caused by the outage until they are Resolved as Critical Service Errors in accordance with the Support Request Classification set forth in **Section 3.5 and 3.6**, or, if determined to be an internet provider problem, open a trouble ticket with the internet provider; and

(iii) Notifying CSC Leon that Contractor has fully corrected the outage and any related problems, along with any pertinent findings or action taken to close the trouble ticket.

3.3 Service Maintenance. Contractor will continuously maintain the Hosted Services and Software to optimize Availability that meets or exceeds the Availability Requirement. Such maintenance services include providing to CSC Leon and its Authorized Users:

a. all updates, bug fixes, enhancements, Maintenance Releases, New Versions and other improvements to the Hosted Services and Software, including the Software, that Contractor provides at no additional charge to its other similarly situated customers; provided that Contractor shall consult with CSC Leon and is required to receive CSC Leon approval prior to modifying or upgrading Hosted Services and Software, including Maintenance Releases and New Versions of Software; and

b. all such services and repairs as are required to maintain the Hosted Services and Software or are ancillary, necessary or otherwise related to CSC Leon's or its Authorized Users' access to or use of the Hosted Services and Software, so that the Hosted Services and Software operate properly in accordance with the Contract and this Schedule.

3.4 Support Service Level Requirements. Contractor will correct all Service Errors and respond to and Resolve all Support Requests in accordance with the required times and other terms and conditions set forth in this **Section 3** ("**Support Service Level Requirements**"), and the Contract.

3.5 Support Requests. CSC Leon will classify its requests for Service Error corrections in accordance with the descriptions set forth in the chart below (each a "**Support Request**"). CSC Leon will notify Contractor of Support Requests by email, telephone or such other means as the Parties may hereafter agree to in writing.

Support Request Classification	**Description:** **Any Service Error Comprising or Causing any of the Following Events or Effects**
Critical Service Error	• Issue affecting entire system or single critical production function; • System down or operating in materially degraded state; • Data integrity at risk; • Declared a Critical Support Request by CSC Leon; or • Widespread access interruptions.
High Service Error	• Primary component failure that materially impairs its performance; or • Data entry or access is materially impaired on a limited basis.
Medium Service Error	• IT Environment Services and Software is operating with minor issues that can be addressed with an acceptable (as determined by CSC Leon) temporary work around.

Support Request Classification	**Description:** **Any Service Error Comprising or Causing any of the Following Events or Effects**
Low Service Error	• Request for assistance, information, or services that are routine in nature.

3.6 Response and Resolution Time Service Levels. Response and Resolution times will be measured from the time Contractor receives a Support Request until the respective times Contractor has (i) responded to, in the case of response time and (ii) Resolved such Support Request, in the case of Resolution time. "**Resolve**" (including "**Resolved**", "**Resolution**" and correlative capitalized terms) means that, as to any Service Error, Contractor has provided CSC Leon the corresponding Service Error correction and CSC Leon has confirmed such correction and its acceptance thereof. Contractor will respond to and Resolve all Service Errors within the following times based on the severity of the Service Error.

Support Request Classification	**Service Level Metric** **(Required Response Time)**	**Service Level Metric** **(Required Resolution Time)**	**Service Level Credits** **(For Failure to Respond to any Support Request Within the Corresponding Response Time)**	**Service Level Credits** **(For Failure to Resolve any Support Request Within the Corresponding Required Resolution Time)**
Critical Service Error	Thirty (30) minutes	Three (3) hours	Five percent (5%) of the Fees for the month in which the initial Service Level Failure begins and five percent (5%) of such monthly Fees for each additional hour or portion thereof that the corresponding Service Error is not	Five percent (5%) of the Fees for the month in which the initial Service Level Failure begins and five percent (5%) of such monthly Fees for the first additional hour or portion thereof that the corresponding Service Error remains un-Resolved, which amount will thereafter

Support Request Classification	**Service Level Metric** **(Required Response Time)**	**Service Level Metric** **(Required Resolution Time)**	**Service Level Credits** **(For Failure to Respond to any Support Request Within the Corresponding Response Time)**	**Service Level Credits** **(For Failure to Resolve any Support Request Within the Corresponding Required Resolution Time)**
			responded to within the required response time.	double for each additional one-hour increment.
High Service Error	One (1) hour	Four (4) hours	Three percent (3%) of the Fees for the month in which the initial Service Level Failure begins and three percent (3%) of such monthly Fees for each additional hour or portion thereof that the corresponding Service Error is not responded to within the required response time.	Three percent (3%) of the Fees for the month in which the initial Service Level Failure begins and three percent (3%) of such monthly Fees for the first additional hour or portion thereof that the corresponding Service Error remains un-Resolved, which amount will thereafter double for each additional one-hour increment.
Medium Service Error	Three (3) hours	Two (2) Business Days	N/A	N/A
Low Service Error	Three (3) hours	Five (5) Business Days	N/A	N/A

3.7 Escalation. With respect to any Critical Service Error Support Request, until such Support Request is Resolved, Contractor will escalate that Support Request within sixty (60) minutes of the receipt of such Support Request by the appropriate Contractor support personnel, including, as applicable, the Contractor Project Manager and Contractor's management or engineering personnel, as appropriate.

3.8 Support Service Level Credits. Failure to achieve any of the Support Service Level Requirements for Critical and High Service Errors will constitute a Service Level Failure for which Contractor will issue to CSC Leon the corresponding service credits set forth in **Section 3.1** ("**Service Level Credits**") in accordance with payment terms set forth in the Contract.

3.9 Corrective Action Plan. If two or more Critical Service Errors occur in any thirty (30) day period during (a) the Term or (b) any additional periods during which Contractor does or is required to perform any Hosted Services, Contractor will promptly investigate the root causes of these Service Errors and provide to CSC Leon within five (5) Business Days of its receipt of notice of the second such Support Request an analysis of such root causes and a proposed written corrective action plan for CSC Leon's review, comment and approval, which, subject to and upon CSC Leon's written approval, shall be a part of, and by this reference is incorporated in, the Contract as the parties' corrective action plan (the "**Corrective Action Plan**"). The Corrective Action Plan must include, at a minimum: (a) Contractor's commitment to CSC Leon to devote the appropriate time, skilled personnel, systems support and equipment and other resources necessary to Resolve and prevent any further occurrences of the Service Errors giving rise to such Support Requests; (b) a strategy for developing any programming, software updates, fixes, patches, etc. necessary to remedy, and prevent any further occurrences of, such Service Errors; and (c) time frames for implementing the Corrective Action Plan. There will be no additional charge for Contractor's preparation or implementation of the Corrective Action Plan in the time frames and manner set forth therein.

4. Data Storage, Backup, Restoration and Disaster Recovery. Contractor must maintain or cause to be maintained backup redundancy and disaster avoidance and recovery procedures designed to safeguard CSC Leon Data and CSC Leon's other Confidential Information, Contractor's Processing capability and the availability of the IT Environment Services and Software, in each case throughout the Term and at all times in connection with its actual or required performance of the Services hereunder. All backed up CSC Leon Data shall be located in the continental United States. The force majeure provisions of this Contract do not limit Contractor's obligations under this section**.**

4.1 Data Storage. Contractor will provide sufficient storage capacity to meet the needs of CSC Leon at no additional cost.

4.2 Data Backup. Contractor will conduct, or cause to be conducted, daily back-ups of CSC Leon Data and perform, or cause to be performed, other periodic offline back-ups of CSC Leon Data on at least a weekly basis and store and retain such back-ups as specified in **Schedule A**. Contractor must, within five (5) Business Days of CSC Leon's request, provide CSC Leon, without charge and without any conditions or contingencies whatsoever (including but not limited to the payment of any fees due to Contractor), an extract of CSC Leon Data in the format specified by CSC Leon**.**

4.3 Data Restoration. If the data restoration is required due to the actions or inactions of Contractor or its subcontractors, Contractor will promptly notify CSC Leon and complete actions required to restore service to normal production operation. If requested, Contractor will restore data from a backup upon written notice from CSC Leon. Contractor will restore the data within one (1) Business Day of CSC Leon's request. Contractor will provide data restorations at its sole cost and expense.

4.4 Disaster Recovery. Throughout the Term and at all times in connection with its actual or required performance of the Services, Contractor will maintain and operate a backup and disaster recovery plan to achieve a Recovery Point Objective (RPO) of 8 hours, and a Recovery Time Objective (RTO) of 8 hours (the "**DR Plan**"), and implement such DR Plan in the event of any unplanned interruption of the Hosted Services. Contractor's current DR Plan, revision history, and any reports or summaries relating to past testing of or pursuant to the DR Plan are attached as **Schedule F**. Contractor will actively test, review and update the DR Plan on at least an annual basis using industry best practices as guidance. Contractor will provide CSC Leon with copies of all such updates to the Plan within fifteen (15) days of its adoption by Contractor. All updates to the DR Plan are subject to the requirements of this **Section 4**; and provide CSC Leon with copies of all reports resulting from any testing of or pursuant to the DR Plan promptly after Contractor's receipt or preparation. If Contractor fails to reinstate all material Hosted Services and Software within the periods of time set forth in the DR Plan, CSC Leon may, in addition to any other remedies available under this Contract, in its sole discretion, immediately terminate this Contract as a non-curable default.

SCHEDULE D – ATTACHMENT 1 – CONTACT LIST

*[See definitions: "**Contact List**" means a current list of Contractor contacts and telephone numbers …to enable CSC Leon to escalate its Support Requests, including: (a) the first person to contact; and (b) the persons in successively more qualified or experienced positions to provide the support sought.]*

SCHEDULE E – DATA SECURITY REQUIREMENTS

This Schedule E reproduces *verbatim* the Florida Cybersecurity Standards promulgated in chapter 60GG-2 of the Florida Administrative Code, *Information Technology Security*. Neither CSC Leon nor Contractor is an “agency” as defined below, and the Contract does not impose on CSC Leon any of the duties or obligations that the standards below impose on agencies. The Contract does not require any submittals to DMS or any other State agency. The Parties agree, however, that this Schedule otherwise expresses the standards that will apply to and guide all of Contractor’s Services for CSC Leon. The Parties intend that Contractor’s performance of Services will be at least as secure as State agencies performance of similar services.

CHAPTER 60GG-2
INFORMATION TECHNOLOGY SECURITY

60GG-2.001 Purpose and Applicability; Definitions

(1) Purpose and Applicability.

(a) Rules 60GG-2.001 through 60GG-2.006, F.A.C., will be known as the Florida Cybersecurity Standards (FCS).

(b) This rule establishes cybersecurity standards for information technology (IT) resources. These standards are documented in Rules 60GG-2.001 through 60GG-2.006, F.A.C. State Agencies must comply with these standards in the management and operation of state IT resources. This rule is modeled after the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, and the Federal Information Security Management Act of 2002 (44 U.S.C. §3541, et seq.). For the convenience of the reader cross-references to these documents and Special Publications issued by the NIST are provided throughout the FCS as they may be helpful to agencies when drafting their security procedures. The Florida Cybersecurity Standards:

1. Establish minimum standards to be used by state agencies to secure IT resources. The FCS consist of five high-level functions: Identify, Protect, Detect, Respond, and Recover. These functions support lifecycle management of IT risk. The functions identify underlying key categories and subcategories for each function. Subcategories contain specific IT controls. The FCS is visually represented as follows:

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management

PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness & Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes & Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies & Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Category Unique Identifier subcategory references are detailed in Rules 60GG-2.002 – 60GG-2.006, F.A.C., and are used throughout the FCS as applicable.

2. Define minimum management, operational, and technical security controls to be used by state agencies to secure IT resources.

3. Allow authorizing officials to employ compensating security controls or deviate from minimum standards when the agency is unable to implement a security standard or the standard is not cost-effective due to the specific nature of a system or its environment. The agency shall document the reasons why the minimum standards cannot be satisfied and the compensating controls to be employed. After the agency analyzes the issue and related risk a compensating security control or deviation may be employed if the agency documents the analysis and risk steering workgroup accepts the associated risk. This documentation is exempt from Section 119.07(1), F.S., pursuant to Sections 282.318 (4)(d), and (4)(e), F.S., and, shall be securely submitted to DMS upon acceptance.

(2) Each agency shall:

(a) Perform an assessment that documents the gaps between requirements of this rule and controls that are in place.

(b) Submit the assessment to DMS with the agency's strategic and operational plan.

(c) Reassess annually and update the ASOP to reflect progress toward compliance with this rule.

(3) Definitions.

(a) The following terms are defined:

1. Agency – shall have the same meaning as state agency, as provided in Section 282.0041, F.S., except that, per Section 282.318(2), F.S., the term also includes the Department of Legal Affairs, the Department of Agriculture and Consumer Services, and the Department of Financial Services.

2. Agency-owned (also agency-managed) – any device, service, or technology owned, leased, or managed by the agency for which an agency through ownership, configuration management, or contract has established the right to manage security configurations, including provisioning, access control, and

data management.

3. Authentication – A process of determining the validity of one or more credentials used to claim as digital identity.

4. Authentication protocol – see Rule 60GG-5.002, F.A.C.

5. Buyer – refers to the downstream people or organizations that consume a given product or service from an organization, including both for-profit and not-for-profit organizations.

6. Compensating controls – see Rule 60GG-5.001, F.A.C.

7. Complex password – a password sufficiently difficult to correctly guess, which enhances protection of data from unauthorized access. Complexity requires at least eight characters that are a combination of at least three of the following character types: uppercase letters, lowercase letters, numbers, and special characters (@, #, $, %, etc.).

8. Confidential information – records that, pursuant to Florida's public records laws or other controlling law, are exempt from public disclosure.

9. Critical infrastructure – systems and assets, whether physical or virtual so vital to the U.S. that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

10. Critical process – a process that is susceptible to fraud, cyberattack, unauthorized activity, or seriously impacting an agency's mission.

11. Customer – an entity in receipt of services or information rendered by a state agency. This term does not include state agencies with regard to information sharing activities.

12. Cybersecurity event – within the context of Rules 60GG-2.001 – 60GG-2.006, F.A.C., a cybersecurity event is a cybersecurity change that may have an impact on agency operations (including mission, capabilities, or reputation).

13. Data-at-rest – stationary data which is stored physically in any digital form.

14. External partners – non-state agency entities doing business with a state agency, including other governmental entities, third parties, contractors, vendors, suppliers and partners. External partners do not include customers.

15. Information Security Manager (ISM) – the person appointed pursuant to Section 282.318(4)(a), F.S.

16. Information system owner – the agency official responsible for the overall procurement, development, integration, modification, or operation and maintenance of the information system.

17. Industry sector(s) – the following major program areas of state government: Health and Human Services, Education, Government Operations, Criminal and Civil Justice, Agriculture and Natural Resources, and Transportation and Economic Development.

18. Information technology resources (IT resources) – see Section 282.0041(19), F.S.

19. Legacy applications – programs or applications inherited from languages, platforms, and techniques earlier than current technology. These applications may be at or near the end of their useful life but are still required to meet mission objectives or fulfill program area requirements.

20. Mobile Device – any computing device that can be conveniently relocated from one network to another.

21. Multi-Factor Authentication – see Rule 60GG-5.001, F.A.C.

22. Personal information – see Sections 501.171(1)(g)1., and 817.568, F.S.

23. Privileged user – a user that is authorized (and, therefore trusted) to perform security-relevant functions that ordinary users are not authorized to perform.

24. Privileged accounts – an information system account with authorizations of a privileged user.

25. Remote access – access by users (or information systems) communicating externally to an information security perimeter.

26. Removable Media – any data storage medium or device sufficiently portable to allow for convenient relocation from one network to another.

27. Separation of duties – an internal control concept of having more than one person required to complete a critical process. This is an internal control intended to prevent fraud, abuse, and errors.

28. Stakeholder – a person, group, organization, or state agency involved in or affected by a course of action related to state agency-owned IT resources.

29. Supplier (commonly referred to as "vendor") – encompasses upstream product and service providers used for an organization's internal purposes (e.g., IT infrastructure) or integrated into the products or services provided on the Buyer. These terms are applicable for both technology-based and non-technology-based products and services.

30. Token control – see Rule 60GG-5.001, F.A.C.

31. User – a worker or non-worker who has been provided access to a system or data.

32. Workforce – employees, contractors, volunteers, trainees, and other persons whose conduct, in the performance of work for the agency, is under the direct control of the agency, whether or not they are paid by the agency (see User; Worker).

33. Worker – a member of the workforce. A worker may or may not use IT resources. This includes employees, contractors, volunteers, trainees, and other persons whose conduct, in the performance of work for the agency, is under the direct control of the agency, whether or not they are paid by the agency.

(b) With the exception of the terms identified in subparagraphs 1.-4., the NIST Glossary of Key Information Security Terms, Revision 2, National Institute of Standards and Technology, U.S. Department of Commerce (May 2013), maintained at: http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf, is hereby incorporated by reference into this rule: http://www.flrules.org/Gateway/reference.asp?No=Ref-06494.

1. Risk assessment – see section 282.0041(28), F.S.

2. Continuity of Operations Plan (COOP) – disaster-preparedness plans created pursuant to Section 252.365(3), F.S.

3. Incident – see Section 282.0041(18), F.S.

4. Threat – see Section 282.0041(36), F.S.

Rulemaking Authority 282.318(11) FS. Law Implemented 282.318(3) FS. History–New 3-10-16, Amended 1-2-19, Formerly 74-2.001.

60GG-2.002 Identify.

The identify function of the FCS is visually represented as such:

Function	Category	Subcategory
Identify (ID)	Asset Management (AM)	ID.AM-1: Inventory agency physical devices and systems
		ID.AM-2: Inventory agency software platforms and applications
		ID.AM-3: Map agency communication and data flows
		ID.AM-4: Catalog interdependent external information systems
		ID.AM-5: Prioritize IT resources based on classification, criticality, and business value
		ID.AM-6: Establish cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders
	Business Environment (BE)	ID.BE-1: Identify and communicate the agency's role in the business mission/processes
		ID.BE-2: Identify and communicate the agency's place in critical

		infrastructure and its industry sector to workers
		ID.BE-3: Establish and communicate priorities for agency mission, objectives, and activities
		ID.BE-4: Identify dependencies and critical functions for delivery of critical services
		ID.BE-5: Implement resiliency requirements to support the delivery of critical services for all operating states (e.g., normal operations, under duress, during recovery)
	Governance (GV)	ID.GV-1: Establish and communicate an organizational cyber security policy
		ID.GV-2: Coordinate and align cybersecurity roles and responsibilities with internal roles and external partners
		ID.GV-3: Understand and manage legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations
		ID.GV-4: Ensure that governance and risk management processes address cybersecurity risks
	Risk Assessment (RA)	ID.RA-1: Identify and document asset vulnerabilities
		ID.RA-2: Receive cyber threat intelligence from information sharing forums and sources
		ID.RA-3: Identify and document threats, both internal and external
		ID.RA-4: Identify potential business impacts and likelihoods
		ID.RA-5: Use threats, vulnerabilities, likelihoods, and impacts to determine risk
		ID.RA-6: Identify and prioritize risk responses
	Risk Management Strategy (RM)	ID.RM-1: Establish, manage, and ensure organizational stakeholders understand the approach to be employed via the risk management processes
		ID.RM-2: Determine and clearly express organizational risk tolerance
		ID.RM-3: Ensure that the organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis
	Supply Chain Risk Management (SC)	ID.SC-1: Establish management processes to identify, establish, assess, and manage cyber supply chain risk which are agreed to by organizational stakeholders
		ID.SC-2: Identify, prioritize, and assess suppliers and third-party providers of information systems, components, and services using a cyber supply chain risk assessment process
		ID.SC-3: Require suppliers and third-party providers (by contractual requirement when necessary) to implement appropriate measures designed to meet the objectives of the organization's information security program or cyber supply chain risk management plan
		ID.SC-4: Routinely assess suppliers and third-party providers to confirm that they are meeting their contractual obligations by conducting reviews of audits, summaries of test results, or other equivalent evaluations of suppliers/providers

		ID.SC-5: Conduct response and recovery planning and testing with suppliers and third-party providers

(1) Asset Management. Each agency shall ensure that IT resources are identified and managed. Identification and management shall be consistent with the IT resource's relative importance to agency objectives and the organization's risk strategy. Specifically, each agency shall:

(a) Ensure that physical devices and systems within the organization are inventoried and managed (ID.AM-1).

(b) Ensure that software platforms and applications within the organization are inventoried and managed (ID.AM-2).

(c) Ensure that organizational communication and data flows are mapped and systems are designed or configured to regulate information flow based on data classification (ID.AM-3). Each agency shall:

1. Establish procedures that ensure only agency-owned or approved IT resources are connected to the agency internal network and resources.

2. Design and document its information security architecture using a defense-in-breadth approach. Design and documentation shall be assessed and updated periodically based on an agency-defined, risk-driven frequency that considers potential threat vectors (i.e., paths or tools that a threat actor may use to attack a target).

3. Consider diverse suppliers when designing the information security architecture.

(d) Each agency shall ensure that interdependent external information systems are catalogued (ID.AM-4). Agencies shall:

1. Verify or enforce required security controls on interconnected external IT resources in accordance with the information security policy or security plan.

2. Implement service level agreements for non-agency provided technology services to ensure appropriate security controls are established and maintained.

3. For non-interdependent external IT resources, execute information sharing or processing agreements with the entity receiving the shared information or hosting the external system in receipt of shared information.

4. Restrict or prohibit portable storage devices either by policy or a technology that enforces security controls for such devices.

5. Authorize and document inter-agency system connections.

6. Require that (e.g., contractually) external service providers adhere to agency security policies.

7. Document agency oversight expectations, and periodically monitor provider compliance.

(e) Each agency shall ensure that IT resources (hardware, data, personnel, devices and software) are categorized, prioritized, and documented based on their classification, criticality, and business value (ID.AM-5). Agencies shall:

1. Perform a criticality analysis for each categorized IT resource and document the findings of the analysis conducted.

2. Designate an authorizing official for each categorized IT resource and document the authorizing official's approval of the security categorization.

3. Create a contingency plan for each categorized IT resource. The contingency plan shall be based on resource classification and identify related cybersecurity roles and responsibilities.

4. Identify and maintain a reference list of exempt, and confidential and exempt agency information or software and the associated applicable state and federal statutes and rules.

(f) Establish cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (ID.AM-6). Each agency is responsible for:

1. Informing workers that they are responsible for safeguarding their passwords and other authentication methods.

2. Informing workers that they shall not share their agency accounts, passwords, personal identification numbers, security tokens, smart cards, identification badges, or other devices used for identification and authentication purposes.

3. Informing workers that use, or oversee or manage workers that use, IT equipment that they shall report suspected unauthorized activity, in accordance with agency-established incident reporting procedures.

4. Informing users that they shall take precautions that are appropriate to protect IT resources in their possession from loss, theft, tampering, unauthorized access, and damage. Consideration will be given to the impact that may result if the IT resource is lost, and safety issues relevant to protections identified in this subsection.

5. Informing users of the extent that they will be held accountable for their activities.

6. Informing workers that they have no reasonable expectation of privacy with respect to agency-owned or agency-managed IT resources.

7. Ensuring that monitoring, network sniffing, and related security activities are only to be performed by workers who have been assigned security-related responsibilities either via their approved position descriptions or tasks assigned to them.

8. Appointing an Information Security Manager (ISM). Agency responsibilities related to the ISM include:

a. Notifying the Department of Management Services (DMS) of ISM appointments and reappointments.

b. Specifying ISM responsibilities in the ISM position description.

c. Establishing an information security program that includes information security policies, procedures, standards, and guidelines; an information security awareness program; an information security risk management process, including the comprehensive risk assessment required by Section 282.318, F.S.; a Computer Security Incident Response Team; and a disaster recovery program that aligns with the agency's Continuity of Operations (COOP) Plan.

d. Each agency ISM shall be responsible for the information security program plan.

9. Performing background checks and ensuring that a background investigation is performed on all individuals hired as IT workers with access to information processing facilities, or who have system, database, developer, network, or other administrative capabilities for systems, applications, or servers with risk categorization of moderate-impact or higher. See paragraph 60GG-2.002(4)(a), F.A.C. These positions often, if not always, have privileged access. As such, in addition to agency-required background screening, background checks conducted by agencies shall include a federal criminal history check that screens for felony convictions that concern or involve the following:

a. Computer related or IT crimes;

b. Identity theft crimes;

c. Financially-related crimes, such as: fraudulent practices, false pretenses and frauds, credit card crimes;

d. Forgery and counterfeiting;

e. Violations involving checks and drafts;

f. Misuse of medical or personnel records; and,

g. Theft.

Each agency shall establish appointment selection disqualifying criteria for individuals hired as IT workers that will have access to information processing facilities, or who have system, database, developer, network, or other administrative capabilities for systems, applications, or servers with risk categorization of moderate-impact or higher.

(2) Business Environment. Each agency's cybersecurity roles, responsibilities, and IT risk management decisions shall align with the agency's mission, objectives, and activities. To accomplish this, agencies shall:

(a) Identify and communicate the agency's role in the business mission of the state (ID.BE-1).

(b) Identify and communicate the agency's place in critical infrastructure and its industry sector to inform internal stakeholders of IT strategy and direction (ID.BE-2).

(c) Establish and communicate priorities for agency mission, objectives, and activities (ID.BE-3).

(d) Identify system dependencies and critical functions for delivery of critical services (ID.BE-4).

(e) Implement information resilience requirements to support the delivery of critical services for all operating states (ID.BE-5).

(3) Governance. Each agency shall establish policies, procedures, and processes to manage and monitor the agency's operational IT requirements based on the agency's assessment of risk. Procedures shall address providing timely notification to management of cybersecurity risks. Agencies shall also:

(a) Establish and communicate a comprehensive cybersecurity policy (ID.GV-1).

(b) Coordinate and align cybersecurity roles and responsibilities with internal roles and external partners (ID.GV-2).

(c) Document and manage legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations (ID.GV-3).

(d) Ensure governance and risk management processes address cybersecurity risks (ID.GV-4).

(4) Risk Assessment.

(a) Approach. Each agency shall identify and manage the cybersecurity risk to agency operations (including mission, functions, image, or reputation), agency assets, and individuals using the following approach, that derives from the NIST Risk Management Framework (RMF) which may be found at: http://csrc.nist.gov/groups/SMA/fisma/framework.html. The Risk Assessment steps provided in the table below must be followed; however, agencies may identify and, based on the risk to be managed, consider other risk assessment security control requirements and frequency of activities necessary to manage the risk at issue.

Risk Assessments	
Categorize:	Categorize information systems and the information processed, stored, and transmitted by that system based on a security impact analysis.
Select:	Select baseline security for information systems based on the security categorization; tailoring and supplementing the security baseline as needed based on organization assessment of risk and local conditions.
Implement:	Implement the selected baseline security and document how the controls are deployed within information systems and environment of operation.
Assess:	Assess the baseline security using appropriate procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for systems.
Authorize:	Authorize information system operation based upon a determination of the risk to organizational operations and assets, individuals, other organizations and the state resulting from the operation of the information system and the decision that this risk is acceptable.

Monitor:	Monitor and assess selected baseline security in information systems on an ongoing basis including assessing control effectiveness, documenting changes to the system or environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of systems to appropriate agency officials.

Agencies are required to consider the following security objectives when assessing risk and determining what kind of assessment is required and when or how often an assessment is to occur: confidentiality, integrity and availability. When determining the potential impact to these security objectives agencies will use the following table, taken from the Federal Information Processing Standards (FIPS) Publication No. 199 (February 2004), which is hereby incorporated into this rule by reference and may be found at: http://www.flrules.org/Gateway/reference.asp?No=Ref-06498.

POTENTIAL IMPACT			
Security Objectives:	LOW	MODERATE	HIGH
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information.	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on

	operations, organizational assets, or individuals.	operations, organizational assets, or individuals.	organizational operations, organizational assets, or individuals.

In accordance with Section 282.318(4)(d), F.S., each agency shall complete and submit to DMS no later than July 31, 2017, and every three years thereafter, a comprehensive risk assessment. In completing the risk assessment agencies shall follow the six-step process ("Conducting the Risk Assessment") outlined in Section 3.2 of NIST Special Publication 800-30, utilizing the exemplary tables provided therein as applicable to address that particular agency's threat situation. NIST Special Publication 800-30, Guide for Conducting Risk Assessments, Revision 1 (September 2012) is hereby incorporated by reference and may be found at: http://www.flrules.org/Gateway/reference.asp?No=Ref-06499. When establishing risk management processes, it may be helpful for agencies to review NIST Risk Management Framework Special Publications – they can be downloaded from the following website: http://csrc.nist.gov/publications/PubsSPs.html. When assessing risk, agencies shall estimate the magnitude of harm resulting from unauthorized access, unauthorized modification or destruction, or loss of availability of a resource. Estimates shall be documented as low-impact, moderate-impact, or high-impact relative to the security objectives of confidentiality, integrity, and availability.

(b) Other agency risk management activities that agencies shall perform:

1. Identify and document asset vulnerabilities (ID.RA-1), business processes and protection requirements. Establish procedures to analyze systems and applications to ensure security controls are effective and appropriate.

2. Receive and manage cyber threat intelligence from information sharing forums and sources that contain information relevant to the risks or threats (ID.RA-2).

3. Identify and document internal and external threats (ID.RA-3).

4. Identify potential business impacts and likelihoods (ID.RA-4).

5. Use threats, vulnerabilities, likelihoods, and impacts to determine risk (ID.RA-5).

6. Identify and prioritize risk responses, implement risk mitigation plans, and monitor and document plan implementation (ID.RA-6).

(5) Risk Management. Each agency shall ensure that the organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions. Each agency shall:

(a) Establish risk management processes that are managed and agreed to by agency stakeholders and the agency head (ID.RM-1).

1. Establish a risk steering workgroup that ensures risk management processes are authorized by agency stakeholders. The risk steering workgroup must include a member of the agency IT unit and shall determine the appropriate meeting frequency and agency stakeholders.

(b) Identify and clearly document organizational risk tolerance based on the confidential and exempt nature of the data created, received, maintained, or transmitted by the agency; by the agency's role in critical infrastructure and sector specific analysis (ID.RM-2).

(c) Determine risk tolerance as necessary, based upon: analysis of sector specific risks; the agency's industry sector; agency-specific risks (e.g., Health Information Portability Accountability Act of 1996 compliance for agencies that maintain this information); and the agency's role in the state's mission (ID.RM-3).

(d) Establish parameters for IT staff participation in procurement activities.

(e) Identify the IT issues IT staff must address during procurement activities (e.g., system hardening, logging, performance, service availability, incident notification, and recovery expectations).

(f) Implement appropriate security controls for software applications obtained, purchased, leased, or developed to minimize risks to the confidentiality, integrity, and availability of the application, its data, and other IT resources.

(g) Prior to introducing new IT resources or modifying current IT resources, perform an impact analysis. The purpose of this analysis is to assess the effects of the technology or modifications on the existing environment. Validate that IT resources conform to agency standard configurations prior to implementation into the production environment.

(6) Supply Chain Risk Management. Each agency shall establish priorities, constraints, risk tolerances, and assumptions to support risk decisions associated with managing supply chain risk. Each agency shall:

(a) Establish management processes to identify, establish, assess, and manage cyber supply chain risks which are agreed to by organizational stakeholders (ID.SC-1).

(b) Identify, prioritize, and assess suppliers and third-party providers of information systems, components, and services using a cyber supply chain risk assessment process (ID.SC-2).

(c) Require suppliers and third-party providers (by contractual agreement when necessary) to implement appropriate measures designed to meet the objectives of the organization's information security program or cyber supply chain risk management plan (ID.SC-3).

(d) Routinely assess suppliers and third-party providers to confirm that they are meeting their contractual obligations by conducting reviews of audits, summaries of test results, or other equivalent evaluations of suppliers/providers (ID.SC-4).

(e) Conduct response and recovery planning and testing with suppliers and third-party providers (ID.SC-5).

Rulemaking Authority 282.318(11) FS. Law Implemented 282.318(3) FS. History–New 3-16-16, Amended 2-5-19, Formerly 74-2.002.

60GG-2.003 Protect.

The protect function of the FCS is visually represented as such:

Function	Category	Subcategory
Protect (PR)	Identity Management, Authentication, and Access Control (AC)	PR.AC-1: Issue, manage, verify, revoke, and audit identities and credentials for authorized devices, processes, and users
		PR.AC-2: Manage and protect physical access to assets
		PR.AC-3: Manage remote access
		PR.AC-4: Manage access permissions and authorizations, incorporate the principles of least privilege and separation of duties
		PR.AC-5: Protect network integrity, by incorporating network segregation and segmentation where appropriate
		PR.AC-6: Proof and bond identities to credentials, asserting in interactions when appropriate (see token control definition)
		PR.AC-7: Authenticate credentials assigned to users, devices, and other assets commensurate with the risk of the transaction.
	Awareness and Training (AT)	PR.AT-1: Inform and train all users
		PR.AT-2: Ensure that privileged users understand roles and responsibilities

		PR.AT-3: Ensure that third-party stakeholders understand roles and responsibilities
		PR.AT-4: Ensure that senior executives understand roles and responsibilities
		PR.AT-5: Ensure that physical and cybersecurity personnel understand their roles and responsibilities
	Data Security (DS)	PR.DS-1: Protect data-at-rest
		PR.DS-2: Protect data-in-transit
		PR.DS-3: Formally manage assets managed throughout removal, transfers, and disposition
		PR.DS-4: Ensure that adequate capacity is maintained to support availability needs
		PR.DS-5: Implement data leak protection measures
		PR.DS-6: Use integrity checking mechanisms to verify software, firmware, and information integrity
		PR.DS-7: Logically or physically separate the development and testing environment(s) from the production environment
		PR.DS-8: Use integrity checking mechanisms to verify hardware integrity
	Information Protection Processes and Procedures	PR.IP-1: Create and maintain a baseline configuration that incorporates all security principles for information technology/industrial control systems
		PR.IP-2: Implement a System Development Life Cycle (SDLC) to manage systems
		PR.IP-3: Establish configuration change control processes
		PR.IP-4: Conduct, maintain, and test backups of information
		PR.IP-5: Meet policy and regulatory requirements that are relevant to the physical operating environment for organizational assets
		PR.IP-6: Destroy data according to policy
		PR.IP-7: Continuously improve protection processes
		PR.IP-8: Share effectiveness of protection technologies with stakeholders that should or must receive this information
		PR.IP-9: Establish and manage response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery)
		PR.IP-10: Test response and recovery plans
		PR.IP-11: Include cybersecurity in human resources practices (e.g., deprovisioning, personnel screening)
		PR.IP-12: Develop and implement a vulnerability management plan
	Maintenance (MA)	PR.MA-1: Perform and log maintenance and repair of organizational assets, with approved and controlled tools
		PR.MA-2: Approve, log, and perform remote maintenance of agency assets in a manner that prevents unauthorized access
	Protective Technology (PT)	PR.PT-1: Determine, document, implement, and review audit/log records in accordance with policy
		PR.PT-2: Protect and restrict removable media usage according to

		policy
		PR.PT-3: Incorporate the principle of least functionality by configuring systems to provide only essential capabilities
		PR.PT-4: Protect communications and control networks
		PR.PT-5: Implement mechanisms (e.g., failsafe, load balancing, hot swap) to achieve resilience requirements in normal and adverse situations

(1) Access Control. Each agency shall ensure that access to IT resources is limited to authorized users, processes, or devices, and to authorized activities and transactions. Specifically:

(a) Each agency shall manage identities and credentials for authorized devices and users (PR.AC-1). Control measures shall, at a minimum include authentication token(s) unique to the individual.
Agencies shall:

1. Require that all agency-owned or approved computing devices, including mobile devices, use unique user authentication.

2. Require users to log off or lock their workstations prior to leaving the work area.

3. Require inactivity timeouts that log-off or lock workstations or sessions.

4. Locked workstations or sessions must be locked in a way that requires user authentication with an authentication token(s) unique to the individual user to disengage.

5. When passwords are used as the sole authentication token, require users to use complex passwords that are changed at least every 90 days.

6. Address responsibilities of information stewards that include administering access to systems and data based on the documented authorizations and facilitate periodic review of access rights with information owners. Frequency of reviews shall be based on system categorization or assessed risk.

7. Establish access disablement and notification timeframes for worker separations. The agency will identify the appropriate person in the IT unit to receive notification. Notification timeframes shall consider risks associated with system access post-separation.

8. Ensure IT access is removed when the IT resource is no longer required.

9. Require MFA for access to networks or applications that have a categorization of moderate, high, or contain exempt, or confidential and exempt, information. This excludes externally hosted systems designed to deliver services to agency customers where the agency documents the analysis and the risk steering workgroup accepts the associated risk.

10. Require MFA for access to privileged accounts.

(b) Each agency shall manage and protect physical access to assets (PR.AC-2). In doing so, agency security procedures or controls shall:

1. Address protection of IT resources from environmental hazards (e.g., temperature, humidity, air movement, dust, and faulty power) in accordance with manufacturer specifications.

2. Implement procedures to manage physical access to IT facilities and/or equipment.

3. Identify physical controls that are appropriate for the size and criticality of the IT resources.

4. Specify physical access to information resource facilities and/or equipment that is restricted to authorized personnel.

5. Detail visitor access protocols, including recordation procedures, and in locations housing systems categorized as moderate-impact or high-impact, require that visitors be supervised by authorized personnel.

6. Address how the agency will protect network integrity by incorporating network segregation.

(c) Each agency shall manage remote access (PR.AC-3). In doing so, agencies shall:

1. Address how the agency will securely manage and document remote access.

2. Specify that only secure, agency-managed, remote access methods may be used to remotely connect computing devices to the agency internal network.

3. For systems containing exempt, or confidential and exempt data, ensure written agreements and procedures are in place to ensure security for sharing, handling or storing confidential data with entities outside the agency.

(d) Each agency shall ensure that access permissions and authorizations, are managed, incorporating the principles of least privilege and separation of duties (PR.AC-4). In doing so, agencies shall:

1. Execute interconnection security agreements to authorize, document, and support continual management of inter-agency connected systems.

2. Manage access permissions by incorporating the principles of "least privilege" and "separation of duties."

3. Specify that all workers be granted access to agency IT resources based on the principles of "least privilege" and "need to know determination."

4. Specify that system administrators restrict and tightly control the use of system development utility programs that may be capable of overriding system and application controls.

(e) Each agency shall ensure that network integrity is protected, incorporating network segregation and segmentation where appropriate (PR.AC-5).

(f) Proof and bond identities to credentials and assert in interactions when appropriate (PR.AC-6).

(g) Authenticate users, devices, and other assets commensurate with the risk of the transaction (PR.AC-7).

(2) Awareness and Training. Agencies shall provide all their workers cybersecurity awareness education and training so as to ensure they perform their cybersecurity related duties and responsibilities consistent with agency policies and procedures. In doing so, each agency shall:

(a) Inform and train all workers (PR.AT-1).

(b) Ensure that privileged users understand their roles and responsibilities (PR.AT-2).

(c) Ensure that third-party stakeholders understand their roles and responsibilities (PR.AT-3).

(d) Ensure that senior executives understand their roles and responsibilities (PR.AT-4).

(e) Ensure that physical and cybersecurity personnel understand their roles and responsibilities (PR.AT-5).

(3) For each of the above subsections the following shall also be addressed:

(a) Appoint a worker to coordinate the agency information security awareness program. If an IT security worker does not coordinate the security awareness program, they shall be consulted for content development purposes. Agencies will ensure that all workers (including volunteer workers) are clearly notified of applicable obligations, established via agency policies, to maintain compliance with such controls.

(b) Establish a program that includes, at a minimum, annual security awareness training and on-going education and reinforcement of security practices.

(c) Provide training to workers within 30 days of start date.

(d) Include security policy adherence expectations for the following, at a minimum: disciplinary procedures and implications, acceptable use restrictions, data handling (procedures for handling exempt and confidential and exempt information), telework and cybersecurity incident reporting procedures. Incident reporting procedures shall:

1. Establish requirements for workers to immediately report loss of mobile devices, security tokens, smart cards, identification badges, or other devices used for identification and authentication purposes

according to agency reporting procedures.

(e) Where technology permits, provide training prior to system access. For specialized agency workers (e.g., law enforcement officers) who are required to receive extended off-site training prior to reporting to their permanent duty stations, initial security awareness training shall be provided within 30 days of the date they report to their permanent duty station.

(f) Require, prior to access, workers verify in writing that they will comply with agency IT security policies and procedures.

(g) Document parameters that govern personal use of agency IT resources and define what constitutes personal use. Personal use, if allowed by the agency, shall not interfere with the normal performance of any worker's duties, or consume significant or unreasonable amounts of state IT resources (e.g., bandwidth, storage).

(h) Inform workers of what constitutes inappropriate use of IT resources. Inappropriate use shall include, but may not be limited to, the following:

1. Distribution of malware.
2. Disablement or circumvention of security controls.
3. Forging headers.
4. Political campaigning or unauthorized fundraising.
5. Use for personal profit, benefit or gain.
6. Offensive, indecent, or obscene access or activities, unless required by job duties.
7. Harassing, threatening, or abusive activity.
8. Any activity that leads to performance degradation.
9. Auto-forwarding to external email addresses.
10. Unauthorized, non-work-related access to: chat rooms, political groups, singles clubs or dating services; peer-to-peer file sharing; material relating to gambling, weapons, illegal drugs, illegal drug paraphernalia, hate-speech, or violence; hacker web-site/software; and pornography and sites containing obscene materials.

(4) Data Security. Each agency shall manage and protect records and data, including data-at-rest, consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information. Agencies shall establish procedures, and develop and maintain agency cryptographic implementations. Key management processes and procedures for cryptographic keys used for encryption of data will be fully documented and will cover key generation, distribution, storage, periodic changes, compromised key processes, and prevention of unauthorized substitution. Also, key management processes must be in place and verified prior to encrypting data at rest, to prevent data loss and support availability. In protecting data security, agencies shall:

(a) Protect data-at-rest by establishing (PR.DS-1):

1. Procedures that ensure only agency-owned or approved IT resources are used to store confidential or exempt information.
2. Procedures that ensure agency-owned or approved portable IT resources containing confidential or mission critical data are encrypted.
3. Procedures that ensure agency-owned or approved portable IT resources that connect to the agency internal network use agency-managed security software.
4. Inform users not to store unique copies of agency data on workstations or mobile devices.

(b) Protect data-in-transit (PR.DS-2). Each agency shall:

1. Encrypt confidential and exempt information during transmission, except when the transport medium is owned or managed by the agency and controls are in place to protect the data during transit.
2. Ensure that wireless transmissions of agency data employ cryptography for authentication and

transmission.

3. Make passwords unreadable during transmission and storage.

4. Encrypt mobile IT resources that store, process, or transmit exempt, or confidential and exempt agency data.

(c) Formally manage assets throughout removal, transfer, and disposition (PR.DS-3).

1. Ensure any records stored on storage media to be disposed of or released for reuse, are sanitized or destroyed in accordance with organization-developed procedures and the State of Florida General Records Schedule GS1-SL for State and Local Government Agencies.

2. Destruction of confidential or exempt information shall be conducted such that the information is rendered unusable, unreadable, and indecipherable and not subject to retrieval or reconstruction.

3. Document procedures for sanitization of agency-owned IT resources prior to reassignment or disposal.

4. Equipment sanitization shall be performed such that confidential or exempt information is rendered unusable, unreadable, and indecipherable and not subject to retrieval or reconstruction. File deletion and media formatting are not acceptable methods of sanitization. Acceptable methods of sanitization include using software to overwrite data on computer media, degaussing, or physically destroying media.

(d) Maintain adequate capacity to ensure system availability and data integrity (PR.DS-4).

1. Ensure adequate audit/log capacity.

2. Protect against or limit the effects of denial of service attacks.

(e) Implement protections against data leaks or unauthorized data disclosures by establishing policies and procedures that address (PR.DS-5):

1. Appropriate handling and protection of exempt, and confidential and exempt, information. Policies shall be reviewed and acknowledged by all workers.

2. Retention and destruction of confidential and exempt information in accordance with the records retention requirements as provided in the State of Florida General Records Schedule GS1-SL for State and Local Government Agencies.

3. Access agreements for agency information systems.

4. Boundary protection.

5. Transmission confidentiality and integrity.

(f) Employ integrity checking mechanisms to verify software, firmware, and information integrity (PR.DS-6).

1. Application controls shall be established to ensure the accuracy and completeness of data, including validation and integrity checks, to detect data corruption that may occur through processing errors or deliberate actions.

(g) Physically or logically separate development and testing environment(s) from the production environment and ensure that production exempt, or confidential and exempt data is not used for development where technology permits. Production exempt, or confidential and exempt data may be used for testing if the data owner authorizes the use and regulatory prohibitions do not exist; the test environment limits access and access is audited; and production exempt, and confidential and exempt data is removed from the system when testing is completed. Data owner authorization shall be managed via technical means, to the extent practical (PR.DS-7).

(h) Use integrity checking mechanisms to verify hardware integrity (PR.DS-8). In doing so, agencies shall establish processes to protect against and/or detect unauthorized changes to hardware used to support systems with a categorization of high-impact.

(5) Information Protection Processes and Procedures. Each agency shall ensure that security policies, processes and procedures are maintained and used to manage protection of information systems and assets. Such policies, processes and procedures shall:

(a) Include a current baseline configuration of information systems which incorporate security principles (PR.IP-1). Baselines shall:

1. Specify standard hardware and secure standard configurations.

2. Include documented firewall and router configuration standards, and include a current network diagram.

3. Require that vendor default settings, posing security risks, are changed or disabled for agency-owned or managed IT resources, including encryption keys, accounts, passwords, and SNMP (Simple Network Management Protocol) community strings, and ensure device security settings are enabled where appropriate.

4. Allow only agency-approved software to be installed on agency-owned IT resources.

(b) Establish a System Development Life Cycle (SDLC) to manage system implementation and maintenance (PR.IP-2). In doing so, agencies shall:

1. Develop and implement processes that include reviews of security requirements and controls to ascertain effectiveness and appropriateness relative to new technologies and applicable state and federal regulations.

2. Ensure security reviews are approved by the ISM and Chief Information Officer (or designee) before new or modified applications or technologies are moved into production. For IT resources housed in a state data center, the security review shall also be approved by the data center before the new or modified applications or technologies are moved into production.

3. The application development team at each agency shall implement appropriate security controls to minimize risks to agency IT resources and meet the security requirements of the application owner. Agencies will identify in their policies, processes and procedures the security coding guidelines the agency will follow when obtaining, purchasing, leasing or developing software.

4. Where technology permits, the agency shall ensure anti-malware software is maintained on agency IT resources.

(c) Establish a configuration change control process to manage upgrades and modifications to existing IT resources (PR.IP-3). In doing so, agencies shall:

1. Determine types of changes that are configuration-controlled (e.g. emergency patches, releases, and other out-of-band security packages).

2. Develop a process to review and approve or disapprove proposed changes based on a security impact analysis (e.g., implementation is commensurate with the risk associated with the weakness or vulnerability).

3. Develop a process to document change decisions.

4. Develop a process to implement approved changes and review implemented changes.

5. Develop an oversight capability for change control activities.

6. Develop procedures to ensure security requirements are incorporated into the change control process.

(d) Ensure backups of information are conducted, maintained, and tested (PR.IP-4).

(e) Establish policy and regulatory expectations for protection of the physical operating environment for agency-owned or managed IT resources (PR.IP-5).

(f) Manage and dispose of records/data in accordance with the records retention requirements as provided in the State of Florida General Records Schedule GS1-SL for State and Local Government Agencies (PR.IP-6).

(g) Establish a policy and procedure review process that facilitates continuous improvement to protection processes (PR.IP-7). Each agency shall:

1. Ensure system security control selection occurs during the beginning of the SDLC and is documented in final design documentation.

2. Ensure system security plans shall document controls necessary to protect production data in the production environment and copies of production data used in non-production environments.

3. Ensure system security plans are confidential per Section 282.318, F.S., and shall be available to the agency ISM.

4. Require that each agency application or system with a categorization of moderate-impact or higher have a documented system security plan (SSP). For existing production systems that lack a SSP, a risk assessment shall be performed to determine prioritization of subsequent documentation efforts. The SSP shall include provisions that:

(I) Align the system with the agency's enterprise architecture.

(II) Define the authorization boundary for the system.

(III) Describe the mission-related business purpose.

(IV) Provide the security categorization, including security requirements and rationale (compliance, availability, etc.).

(V) Describe the operational environment, including relationships, interfaces, or dependencies on external services.

(VI) Provide an overview of system security requirements.

(VII) Identify authorizing official or designee, who reviews and approves prior to implementation.

5. Require information system owners (ISOs) to define application security-related business requirements using role-based access controls and rule-based security policies where technology permits.

6. Require ISOs to establish and authorize the types of privileges and access rights appropriate to system users, both internal and external.

7. Create procedures to address inspection of content stored, processed or transmitted on agency-owned or managed IT resources, including attached removable media. Inspection shall be performed where authorization has been provided by stakeholders that should or must receive this information.

8. Establish parameters for agency-managed devices that prohibit installation (without worker consent) of clients that allow the agency to inspect private partitions or personal data.

9. Require ISOs ensure segregation of duties when establishing system authorizations.

10. Establish controls that prohibit a single individual from having the ability to complete all steps in a transaction or control all stages of a critical process.

11. Require agency information owners to identify exempt, and confidential and exempt information in their systems.

(h) Ensure that effectiveness of protection technologies is shared with stakeholders that should or must receive this information (PR.IP-8).

(i) Develop, implement and manage response plans (e.g., Incident Response and Business Continuity) and recovery plans (e.g., Incident Recovery and Disaster Recovery) (PR.IP-9).

(j) Establish a procedure that ensures that agency response and recovery plans are regularly tested (PR.IP-10).

(k) Include cybersecurity in human resources practices (e.g., deprovisioning, personnel screening) (PR.IP-11).

(l) Each agency shall develop and implement a vulnerability management plan (PR.IP-12).

(6) Maintenance. Each agency shall perform maintenance and repairs of information systems and components consistent with agency-developed policies and procedures. Each agency shall:

(a) Perform and log maintenance and repair of IT resources, with tools that have been approved and are administered by the agency to be used for such activities (PR.MA-1).

(b) Approve, encrypt, log and perform remote maintenance of IT resources in a manner that prevents unauthorized access (PR.MA-2).

(c) Not engage in new development of custom authenticators. Agencies assess the feasibility of replacing agency-developed authenticators in legacy applications.

(7) Protective Technology. Each agency shall ensure that technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements. Specifically, each agency shall:

(a) Determine and document required audit/log records, implement logging of audit records, and protect and review logs in accordance with agency-developed policy. Agency-developed policy shall be based on resource criticality. Where possible, ensure that electronic audit records allow actions of users to be uniquely traced to those users so they can be held accountable for their actions. Maintain logs identifying where access to exempt, or confidential and exempt data was permitted. The logs shall support unique identification of individuals and permit an audit of the logs to trace activities through the system, including the capability to determine the exact confidential or exempt data accessed, acquired, viewed or transmitted by the individual (PR.PT-1).

(b) Protect and restrict removable media in accordance with agency-developed information security policy (PR.PT-2).

(c) Incorporate the principle of least functionality by configuring systems to only provide essential capabilities (PR.PT-3).

(d) Protect communications and control networks by establishing perimeter security measures to prevent unauthorized connections to agency IT resources (PR.PT-4). Agencies shall:

1. Place databases containing mission critical, exempt, or confidential and exempt data in an internal network zone, segregated from the demilitarized zone (DMZ).

2. Agencies shall require host-based (e.g., a system controlled by a central or main computer) boundary protection on mobile computing devices where technology permits (i.e., detection agent).

(e) Implement mechanisms (e.g., failsafe, load balancing across duplicated systems, hot swap) to achieve resilience requirements in normal and adverse situations (PR.PT-5).

Rulemaking Authority 282.318(11) FS. Law Implemented 282.318(3) FS. History–New 3-10-16, Amended 1-2-19, Formerly 74-2.003.

60GG-2.004 Detect.

The detect function of the FCS is visually represented as such:

Function	Category	Subcategory
Detect (DE)	Anomalies and Events (AE)	DE.AE-1: Establish and manage a baseline of network operations and expected data flows for users and systems
		DE.AE-2: Analyze detected cybersecurity events to understand attack targets and methods
		DE.AE-3: Collect and correlate cybersecurity event data from multiple sources and sensors
		DE.AE-4: Determine the impact of cybersecurity events
		DE.AE-5: Establish incident alert thresholds
	Security Continuous	DE.CM-1: Monitor the network to detect potential cybersecurity events

	Monitoring (CM)	DE.CM-2: Monitor the physical environment to detect potential cybersecurity events
		DE.CM-3: Monitor personnel activity to detect potential cybersecurity events
		DE.CM-4: Detect malicious code
		DE.CM-5: Detect unauthorized mobile code
		DE.CM-6: Monitor external service provider activity to detect potential cybersecurity events
		DE.CM-7: Monitor for unauthorized personnel, connections, devices, and software
		DE.CM-8: Perform vulnerability scans
	Detection Processes (DP)	DE.DP-1: Define roles and responsibilities for detection to ensure accountability
		DE.DP-2: Ensure that detection activities comply with all applicable requirements
		DE.DP-3: Test detection processes
		DE.DP-4: Communicate event detection information to stakeholders that should or must receive this information
		DE.DP-5: Continuously improve detection processes

(1) Anomalies and Events. Each agency shall develop policies and procedures that will facilitate detection of anomalous activity and that allow the agency to understand the potential impact of events. Such policies and procedures shall:

(a) Establish and manage a baseline of network operations and expected data flows for users and systems (DE.AE-1).

(b) Detect and analyze anomalous cybersecurity events to determine attack targets and methods (DE.AE-2).

1. Monitor for unauthorized wireless access points connected to the agency internal network, and immediately remove them upon detection.

2. Implement procedures to establish accountability for accessing and modifying exempt, or confidential and exempt, data stores to ensure inappropriate access or modification is detectable.

(c) Collect and correlate cybersecurity event data from multiple sources and sensors (DE.AE-3).

(d) Determine the impact of cybersecurity events (DE.AE-4).

(e) Establish incident alert thresholds (DE.AE-5).

(2) Security Continuous Monitoring. Each agency shall determine the appropriate level of monitoring that will occur regarding IT resources necessary to identify cybersecurity events and verify the effectiveness of protective measures. Such activities shall include:

(a) Monitoring the network to detect potential cybersecurity events (DE.CM-1).

(b) Monitoring for unauthorized IT resource connections to the internal agency network.

(c) Monitoring the physical environment to detect potential cybersecurity events (DE.CM-2).

(d) Monitoring user activity to detect potential cybersecurity events (DE.CM-3).

(e) Monitoring for malicious code (DE.CM-4).

(f) Monitoring for unauthorized mobile code (DE.CM-5).

(g) Monitoring external service provider activity to detect potential cybersecurity events (DE.CM-6).

(h) Monitoring for unauthorized personnel, connections, devices, and software (DE.CM-7).

(i) Performing vulnerability scans (DE.CM-8). These shall be a part of the System Development Life

Cycle (SDLC).

(3) Detection Processes. Each agency shall maintain and test detection processes and procedures to ensure awareness of anomalous events. These procedures shall be based on assigned risk and include the following:

(a) Defining roles and responsibilities for detection to ensure accountability (DE.DP-1).

(b) Ensuring that detection activities comply with all applicable requirements (DE.DP-2).

(c) Testing detection processes (DE.DP-3).

(d) Communicating event detection information to stakeholders that should or must receive this information (DE.DP-4).

(e) Continuously improving detection processes (DE.DP-5).

Rulemaking Authority 282.318(11) FS. Law Implemented 282.318(3) FS. History–New 3-10-16, Amended 1-2-19, Formerly 74-2.004.

60GG-2.005 Respond.

The respond function of the FCS is visually represented as such:

Function	Category	Subcategory
Respond (RS)	Response Planning (RP)	RS.RP-1: Execute response plan during or after an incident
	Communications (CO)	RS.CO-1: Ensure that personnel know their roles and order of operations when a response is needed
		RS.CO-2: Report incidents consistent with established criteria
		RS.CO-3: Share information consistent with response plans
		RS.CO-4: Coordinate with stakeholders consistent with response plans
		RS.CO-5: Engage in voluntary information sharing with external stakeholders to achieve broader cybersecurity situational awareness
	Analysis (AN)	RS.AN-1: Investigate notifications from detection systems
		RS.AN-2: Understand the impact of incidents
		RS.AN-3: Perform forensic analysis
		RS.AN-4: Categorize incidents consistent with response plans
		RS.AN-5: Establish processes to receive, analyze, and respond to vulnerabilities disclosed to the agency from internal and external sources
	Mitigation (MI)	RS.MI-1: Contain incidents
		RS.MI-2: Mitigate incidents
		RS.MI-3: Mitigate newly identified vulnerabilities or document accepted risks
	Improvements (IM)	RS.IM-1: Incorporate lessons learned in response plans
		RS.IM-2: Periodically update response strategies

(1) Response Planning. Each agency shall establish and maintain response processes and procedures and validate execution capability to ensure agency response for detected cybersecurity incidents. Each agency shall execute a response plan during or after an incident (RS.RP-1).

(a) Agencies shall establish a Computer Security Incident Response Team (CSIRT) to respond to cybersecurity incidents. CSIRT members shall convene immediately, upon notice of cybersecurity incidents. Responsibilities of CSIRT members include:

1. Convening a simple majority of CSIRT members at least quarterly to review, at a minimum, established processes and escalation protocols.

2. Receiving incident response training annually. Training shall be coordinated as a part of the information security program.

3. CSIRT membership shall include, at a minimum, a member from the information security team, the CIO (or designee), and a member from the Inspector General's Office who shall act in an advisory capacity. The CSIRT team shall report findings to agency management.

4. The CSIRT shall determine the appropriate response required for each cybersecurity incident.

5. The agency security incident reporting process must include notification procedures, established pursuant to Section 501.171, F.S., Section 282.318, F.S., and as specified in executed agreements with external parties. For reporting incidents to DMS and the Cybercrime Office (as established within the Florida Department of Law Enforcement via Section 943.0415, F.S.), agencies shall report observed incident indicators via the DMS Incident Reporting Portal to provide early warning and proactive response capability to other State of Florida agencies. Such indicators may include any known attacker IP addresses, malicious uniform resource locator (URL) addresses, malicious code file names and/or associated file hash values.

(2) Communications. Each agency shall coordinate response activities with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies. Each agency shall:

(a) Inform workers of their roles and order of operations when a response is needed (RS.CO-1).

(b) Require that incidents be reported consistent with established criteria and in accordance with agency incident reporting procedures. Criteria shall require immediate reporting, including instances of lost identification and authentication resources (RS.CO-2).

(c) Share information, consistent with response plans (RS.CO-3).

(d) Coordinate with stakeholders, consistent with response plans (RS.CO-4).

(e) Establish communications with external stakeholders to share and receive information to achieve broader cybersecurity situational awareness (RS.CO-5). Where technology permits, enable automated security alerts. Establish processes to receive, assess, and act upon security advisories.

(3) Analysis. Each agency shall conduct analysis to adequately respond and support recovery activities. Related activities include:

(a) Each agency shall establish notification thresholds and investigate notifications from detection systems (RS.AN-1).

(b) Each agency shall assess and identify the impact of incidents (RS.AN-2).

(c) Each agency shall perform forensics, where deemed appropriate (RS.AN-3).

(d) Each agency shall categorize incidents, consistent with response plans (RS.AN-4). Each incident report and analysis, including findings and corrective actions, shall be documented.

(e) Establish processes to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (RS.AN-5).

(4) Mitigation. Each agency shall perform incident mitigation activities. The objective of incident mitigation activities shall be to: attempt to contain and prevent recurrence of incidents (RS.MI-1); mitigate incident effects and resolve the incident (RS.MI-2); and address vulnerabilities or document as accepted risks.

(5) Improvements. Each agency shall improve organizational response activities by incorporating lessons learned from current and previous detection/response activities into response plans (RS.IM-1). Agencies shall update response strategies in accordance with agency-established policy (RS.IM-2).

Rulemaking Authority 282.318(11) FS. Law Implemented 282.318(3) FS. History–New 3-10-16, Amended 1-2-19, Formerly 74-2.005.

60GG-2.006 Recover.

The recover function of the FCS is visually represented as such:

Function	Category	Subcategory
Recover (RC)	Recovery Planning (RP)	RC.RP-1: Execute recovery plan during or after a cybersecurity incident
	Improvements (IM)	RC.IM-1: Incorporate lessons learned in recovery plans
		RC.IM-2: Periodically update recovery strategies
	Communications (CO)	RC.CO-1: Manage public relations
		RC.CO-2: Repair reputation after an event
		RC.CO-3: Communicate recovery activities to internal stakeholders and executive and management teams

(1) Recovery Planning. Each agency shall execute and maintain recovery processes and procedures to ensure restoration of systems or assets affected by cybersecurity incidents. Each agency shall:

(a) Execute a recovery plan during or after an incident (RC.RP-1).

(b) Mirror data and software, essential to the continued operation of critical agency functions, to an off-site location or regularly back up a current copy and store at an off-site location.

(c) Develop procedures to prevent loss of data, and ensure that agency data, including unique copies, are backed up.

(d) Document disaster recovery plans that address protection of critical IT resources and provide for the continuation of critical agency functions in the event of a disaster. Plans shall address shared resource systems, which require special consideration, when interdependencies may affect continuity of critical agency functions.

(e) IT disaster recovery plans shall be tested at least annually; results of the annual exercise shall document plan procedures that were successful and specify any modifications required to improve the plan.

(2) Improvements. Each agency shall improve recovery planning and processes by incorporating lessons learned into future activities. Such activities shall include:

(a) Incorporating lessons learned in recovery plans (RC.IM-1).

(b) Updating recovery strategies (RC.IM-2).

(3) Communications. Each agency shall coordinate restoration activities with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors. Such activities shall include:

(a) Managing public relations (RC.CO-1).

(b) Attempts to repair reputation after an event, if applicable (RC.CO-2).

(c) Communicating recovery activities to stakeholders, internal and external where appropriate (RC.CO-3).

Rulemaking Authority 282.318(11) FS. Law Implemented 282.318(3) FS. History–New 3-10-16, Amended 1-2-19, Formerly 74-2.006.

SCHEDULE F – DISASTER RECOVERY PLAN

[*Contractor’s Disaster Recovery Plan is to be included as an attachment*]

SCHEDULE G – TRANSITION PLAN

Contractor shall be responsible for end-of-Contract activities to ensure that the transition from Contractor operations to the successor contractor, or CSC Leon, occurs smoothly and without disruption to CSC Leon. Contractor must designate a person with the appropriate training to act as the transition coordinator. The transition coordinator must interact closely with CSC Leon and/or staff of the successor contractor to ensure an orderly transition.

Contractor shall within 180 days before the end of the Contract, at the rates published in Schedule B, develop a Transition Plan and submit it to CSC Leon for review and approval. The Transition Plan must include the following activities and requirements:

1. Transfer all completed or partially completed Deliverables to CSC Leon;

2. Transfer ownership and title to all completed or partially completed Deliverables to CSC Leon;

3. Return to CSC Leon all CSC Leon Data and CSC Leon Materials in a mutually acceptable format and manner. Contractor may retain one copy of any non-Confidential data as required to comply with applicable Work Product documentation standards or as are automatically retained in the course of Contractor's routine back up procedures;

4. Reasonably cooperate (at no expense to Contractor) with any successor in the assumption of any Contract obligations. Transition activities will include planning and timely transfer of data and documentation. Contractor shall provide technical and professional support to CSC Leon and/or a successor Contractor in support of the turnover as mutually agreed between CSC Leon and Contractor;

5. Reasonably cooperate (at no expense to Contractor) with any successor Contactor, person or entity with the transfer of information or data related to Contract. Contractor must submit, for approval by CSC Leon, a detailed plan for the transition of services to a successor system that includes the schedule for key activities and milestones; and

6. Return or vacate any CSC Leon owned real or personal property.

Nothing in this Schedule should be construed to require Contractor to surrender intellectual property, real or personal property, or information or data owned by Contractor for which CSC Leon has no legal claim, or to incur any non-reimbursed expense in connection with any of the foregoing transition services.

This Schedule does not limit CSC Leon's ability to terminate the Contract as provided in Contract Section 16.