AGREEMENT FOR CONSULTING SERVICES PERTAINING TO PORTFOLIO OPTIMIZATION ASSESSMENT

This Agreement for Consulting Services ("Agreement") is made and effective as of June 1, 2023, by and between the State Board of Administration of Florida (the "SBA"), located at 1801 Hermitage Boulevard, Tallahassee, Florida 32308, and Luciola Solutions LLC (the "Consultant"), located at 420 Summit Avenue, Suite 316, Saint Paul, MN 55102.

WITNESSETH

For good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the SBA hereby retains and engages the Consultant to act on the terms and conditions hereinafter set forth.

I. SERVICES TO BE PROVIDED

The Consultant shall render those consulting services needed to evaluate the SBA's current practices and assist in developing new tools supporting total portfolio optimization. The Services to be provided are more particularly set forth in Schedule A, attached hereto and by this reference made a part of this Agreement.

In addition, the SBA may ask Consultant to provide additional consulting and other non-retainer services (hereinafter "Additional Services") as the SBA may require during the term of the Agreement. The scope and nature of such Additional Services will be negotiated by the parties as needed.

II. TERMS AND CONDITIONS:

A. Term of Contract:

This Agreement shall have a term commencing as of the date first written above and ending September 15, 2023. The Agreement is renewable upon agreement of both parties for a period, scope and fee to be determined by both parties.

Notwithstanding the foregoing, either party may terminate this Agreement upon written notice under the terms and conditions of the Agreement.

B. Fee Schedule: As compensation for the Services for the Scope of Services project described in Schedule A, the SBA shall pay to the Consultant an all-inclusive fee (professional fees and expenses) in the amount of $75,000. The Consultant shall invoice the SBA for the professional fees in equal monthly installments, and payment of such fees will be due within thirty (30) days of the date of each invoice.

C. Reserved.

D. Confidentiality

1. Consultant, in the course of its duties, may have access to certain non-public information pertaining to the FRS Defined Benefit Plan, the FRS Defined Contribution Plan, other SBA mandates, the SBA and its employees, and/or the State of Florida. All such information may be confidential, pursuant to the provisions Florida law, including, without limitation, Sections 215.44(8), 215.557, and 121.4501(19), Florida Statutes. Consultant agrees that all confidential information shall be received in strict confidence and shall be used only for the purposes of this Agreement. Consultant further agrees that such confidential information shall only be provided to parties, whether internal or external to Consultant, that are directly involved with performing the duties under the Agreement and that further have a need to know the confidential information in order to carry out their duties in support of the Agreement. Consultant agrees to take all reasonable precautions to prevent the disclosure of such information to parties other than those previously specified except as may be necessary by reason of legal (including the provisions of Chapter 119, Florida Statutes), accounting or regulatory requirements, as the case may be. The obligation to treat information as confidential shall not apply to information which:

    a) is in the public domain, other than by any breach of this agreement;
    b) is in the possession of the Consultant on the effective date of this Agreement, and such information was not obtained from the SBA;
    c) was developed by Consultant outside the scope of any agreement with the SBA; or
    d) was obtained rightfully from third parties.

2. Consultant shall treat the confidential information as confidential, using the same standard of care that it uses to protect its own proprietary or confidential information (but not less than a reasonable standard of care), and no information shall be disclosed to third parties by the Consultant, its officers, employees, consultants, or agents without the prior written request of the SBA. Consultant agrees to take all reasonable precautions to prevent the disclosure to third parties of such information, except as may be necessary by reason of legal, accounting or regulatory requirements, as the case may be.

3. Consultant shall not be bound by this Section to the extent that it acts under compulsion of law or in accordance with the requirements of any national or local government instrumentality. If Consultant is required to disclose confidential information pursuant to such requirements of law, the Consultant shall first notify the SBA so that it may seek protective orders or take any other legal action it deems necessary. Any Confidential Information disclosed pursuant to requirements of law shall still be deemed confidential.

4. The SBA and the Consultant acknowledge and agree that a breach of these confidentiality obligations would cause irreparable harm to the SBA and that no adequate remedy is available at law for such breach. Accordingly, it is agreed that the SBA will be entitled to

an injunction or injunctions to prevent breaches of these confidentiality obligations and to enforce specifically the terms and provisions of this Section II(D).

E. Conflict of Interest

1. It is understood by the parties hereto that the Consultant will be performing consulting services for various other clients. In the event it appears that the duties of the Consultant to the SBA and the duties to one or more of the other clients may conflict, the Consultant will notify the SBA of this potential conflict and the parties will discuss how this potential conflict may be resolved, and will agree to take any and all necessary actions to allow resolution of the conflict.

2. Consultant has dissolved Luciola Systematic Fund I, LP and shall ensure no conflict of interest arises between such firm and the Consultant's duties under this Agreement while the business of the fund is being concluded.

3. Consultant shall not directly or indirectly receive any benefit from recommendations made to the SBA and shall disclose to the SBA any actual or potential personal investment or economic interest of the Consultant which may be enhanced by the recommendations made to the SBA.

4. Consultant acknowledges and understands that the SBA is subject to the provisions of Chapter 112, Part III, "Code of Ethics for Public Officers and Employees," Florida Statutes, and all rules adopted thereunder, and Consultant agrees to comply promptly with any requirements that may be applicable to it thereunder. Consultant represents that it and/or its parent organization currently has, and further covenants that it and/or its parent organization will have at all times during the term of this Agreement, a code of ethics, code of professional conduct or other policies and procedures that prohibit all officers, directors or employees thereof from engaging in any activity or conduct that would constitute an actual or perceived conflict of interest between such person and the Consultant's clients without the prior written approval of Consultant.

5. Consultant shall promptly notify the SBA of any pending or threatened action by Consultant's clients regarding the retention of Consultant based on any allegation of an actual or perceived conflict of interest between such client and Consultant (including any divisions, subsidiaries or affiliates).

F. Indemnification

Consultant agrees to protect, indemnify, defend and hold harmless the SBA, its Trustees, officers and employees from and against any and all losses, costs, claims, demands, damages, losses, liabilities and expenses (including reasonable attorneys' fees and expenses, and investigation, collection, settlement and litigation costs), resulting from or arising out of negligence, omissions, fraud, willful misconduct or breach of duty or this contract (including all Addenda); or Consultant's breach of data security; or the violation

of or non-compliance with any law, rule, regulation or other legal requirement (including without limitation, the securities laws) of Consultant or its agents, nominees, appointees or subcontractors.

G. Compliance with Laws.

The Consultant hereby covenants and agrees that at all times during the term of this Agreement, the Consultant shall comply with all applicable laws, rules, regulations, industry/professional standards, or other applicable legal requirements (including, without limitation, all applicable laws, rules, regulations, and industry standards relating to cybersecurity or data collection, storage, security or privacy) to which the Consultant, its Services or any of the activities contemplated by this Agreement are subject.

H. Public Records

1. Notwithstanding any provision in this Agreement between the parties, Consultant acknowledges and agrees that the SBA is bound by the provisions of Chapter 119 (Public Records), Florida Statutes, and in the event of any conflict between Chapter 119, Florida Statutes, and the terms of this Agreement between the parties, the provisions and procedures of Chapter 119, Florida Statutes, shall prevail. To the extent applicable, Consultant shall comply with Chapter 119, Florida Statutes. In particular, Consultant shall:

   (a) Keep and maintain public records required by the SBA in order to perform the Services under this Agreement;

   (b) Upon request from the SBA's custodian of public records, provide the SBA with a copy of the requested public records or allow such records to be inspected or copied within a reasonable time at a cost that does not exceed the cost provided in Chapter 119, Florida Statutes or as otherwise provided by Florida law;

   (c) Ensure that public records that are exempt or confidential and exempt from public records disclosure requirements are not disclosed except as authorized by law for the duration of the contract term and following the completion of the contract if Consultant does not transfer the records to the SBA when the Agreement is completed;

   (d) Upon completion of the Agreement, transfer, at no cost, to the SBA all public records in Consultant's possession or keep and maintain the public records required by the SBA in order to perform the services under this Agreement. If Consultant transfers all public records to the SBA upon completion of the contract, Consultant shall destroy any duplicate public records that are exempt or confidential and exempt from public records disclosure requirements. If Consultant keeps and maintains public records upon completion of the contract, Consultant shall meet all applicable requirements for retaining public records. Consultant shall, upon request from the SBA's custodian of records, provide all records that are stored

electronically to the SBA in a format that is compatible with the information technology systems of the SBA.

(e) **IF CONSULTANT HAS QUESTIONS REGARDING THE APPLICATION OF CHAPTER 119, FLORIDA STATUTES, TO CONSULTANT'S DUTY TO PROVIDE PUBLIC RECORDS RELATING TO THIS CONTRACT, CONTACT THE SBA'S CUSTODIAN OF PUBLIC RECORDS AT: STATE BOARD OF ADMINISTRATION OF FLORIDA, POST OFFICE BOX 13300, TALLAHASSEE, FLORIDA 32317-3300, sbacontracts@sbafla.com, (850) 488-4406.**

(f) Consultant consents and agrees to be sued in, and subject to the exclusive jurisdiction of, Florida state courts located in Leon County, Florida with respect to any civil or criminal litigation required to enforce the provisions of Chapter 119, Florida Statutes, or the provisions of this Section II.(H).

(g) All requests, including telephone requests, for inspection of public records shall be immediately forwarded to the SBA's Office of General Counsel.

I. Right to Audit

(a) During the term of and for a period of six (6) years after the expiration or termination of the Agreement, the SBA shall have the right to have any person or entity designated by the SBA, including an independent public accountant or auditor and/or any federal or state auditor, to inspect, review and/or audit, any books, records and supporting documents relating to the Agreement and/or the subject matter of the Agreement (the "Records"). In the event such right is exercised and upon no less than ten (10) business days' prior written notice by the SBA, Consultant agrees to permit reasonable access to its premises and the Records during Consultant's normal business hours. The SBA shall have the right, in connection with any such inspection, review and/or audit, to have one or more members of its staff present at all times. During the term of and for a period of six (6) years after the expiration or termination of the Agreement (or for any longer period of time that may be required by any applicable law relating to the retention of Records), Consultant shall maintain and retain the Records, at its sole expense. In the event the SBA and/or its designees are in the process of conducting such an inspection, review and/or audit upon the expiration of the six (6)-year access and/or retention periods described herein, then this Section II.(I). shall survive in its entirety until the conclusion of such inspection, review and/or audit, in the SBA's or the SBA designee's reasonable determination. For the avoidance of doubt, the scope of any inspection, review and/or audit under this Section may include, without limitation, Consultant's compliance with the terms of the Agreement compliance with any applicable foreign, federal, state and/or local law, an assessment of risks and controls or the source and application of the SBA's funds.

(b) Consultant shall use best efforts to cooperate with the SBA and any person or entity designated by the SBA in connection with any inspection, review and/or audit under this Section including, without limitation, causing its relevant and knowledgeable employees and/or representatives to be available to assist and to respond to reasonable inquiries and requests of the SBA and/or its designees. Consultant shall respond (including, if relevant and appropriate, with an action plan) within a reasonable time to any reports, findings and/or assessments provided to Consultant by the SBA and/or its designees, and Consultant shall provide a copy of all such responses to the SBA (including the SBA's management contact listed in the Letter of Understanding. Consultant acknowledges and agrees that any such report, finding and/or assessment is intended for the sole use and for the benefit of the SBA.

(c) Except as set forth herein, the SBA shall bear the costs of any inspection, review and/or audit described in this Section II.(I). However, in the event Consultant engaged in or committed (including through acts or omissions) any fraud, misrepresentation and/or non-performance, then Consultant shall be obligated to reimburse the SBA for the total costs of inspection, review and/or audit. Consultant's reimbursement obligation herein shall be in addition to all other rights, remedies and damages available to the SBA at law or in equity, which shall not be deemed waived or relinquished in any way because of Consultant's additional reimbursement obligation hereunder.

J. Termination:

The SBA may terminate the Agreement at any time for any reason whatsoever upon providing thirty (30) days written notice to the Consultant. The Consultant may resign upon sixty (60) days advance written notice. However, certain provisions of the Agreement may survive the termination of the Agreement by the SBA or the resignation of the Consultant under the Agreement. Except as set forth herein or as otherwise required by law, upon expiration or termination hereof, Consultant shall have no further obligations under this Agreement. As long as the SBA is not in material breach of its obligations under this Agreement, Consultant shall continue to serve, at the same fees, at the SBA's request until the appointment of a successor.

K. Assignments

Consultant shall not assign or delegate its rights or responsibilities without the prior written consent of the SBA. No person or organization may succeed to or assume Consultant's rights and obligations under the Agreement by operation of law, whether by merger, consolidation, change in control, reorganization or otherwise without the SBA's prior written consent.

L. Subcontractors/Agents

Consultant shall be responsible and accountable for the acts or omissions of Consultant Representatives (including the Consultant's officers, directors, employees, agents, contractors, subcontractors and consultants, including affiliates thereof) to the same extent

it is responsible and accountable for its own actions or omissions under the Agreement. Consultant agrees to impose the requirements of this Agreement on all Contractor Representatives. Consultant shall execute a written agreement with each Consultant Representative containing equivalent terms to this Agreement.

M. Information to be Provided

Consultant shall assume any information the SBA supplies (or which is supplied on its behalf) is accurate and complete. Consultant's responsibilities (and the associated project fees) do not include extensive independent verification of required information.

N. Consultant Intellectual Capital

Consultant hereby grants to the SBA and its successors and assigns a perpetual license to use, alter and modify for any purpose any and all work, services (including the Services), records, information, methodologies, processes, documentation, deliverables or any other intellectual capital of any kind, including all modifications, derivations and adaptations thereof (the "Intellectual Capital"), performed, prepared, created or developed, in whole or in part, by the Consultant under this Agreement, subject to the understanding that the SBA shall not sell or transmit the Intellectual Capital to third persons for compensation (which shall exclude reimbursement or payment for copying and other ministerial costs) unless otherwise required by law. Except as otherwise set forth above, Consultant shall retain exclusive rights to the Intellectual Capital. Notwithstanding the foregoing, the Consultant, for itself and its past, present and future successors, assigns, representatives, officers, directors, shareholders, employees and agents, does hereby release, permit, acquit, satisfy, and forever discharge the SBA, its successors, assigns, affiliates, trustees, officers, and employees from any and all claims, demands, actions, causes of action, costs, expenses, attorneys' fees, sums of money, lost profits, damages and all liabilities of any kind whatsoever (the "Liabilities"), at law or in equity, whether known or unknown, that Consultant had, now has and may have in the future relating to the SBA's use, transmission and disclosure of the Intellectual Capital, except for the Liabilities directly resulting from the SBA's material breach of this Section II.(N).

O. Governing Law and Jurisdiction

This Agreement shall be governed by, construed under and interpreted in accordance with laws of the State of Florida without regard to conflict of law principles. Any proceedings to resolve disputes regarding or arising out of this Agreement shall be conducted in the state courts located in Leon County, Florida, and the parties hereby consent to the jurisdiction and venue of those courts.

P. E-Verify.

Consultant shall register with and use the E-Verify system to verify employment eligibility of newly hired employees performing services within the United States in accordance with Section 448.095, Florida Statutes. Consultant acknowledges that the SBA is subject to, and

Consultant agrees to comply with, Section 448.095, Florida Statutes, as amended from time to time, to the extent applicable.

Q. Agreement Transparency.

Consistent with the Florida Transparency in Contracting Initiative, the SBA posts certain operational Agreements on its website, and this Agreement will be one of the agreements posted. Consultant hereby agrees that the SBA is authorized to post this Agreement (including any amendments or addenda hereto) and a description of the content of the Agreement (including any amendments or addenda hereto) on the SBA's website.

R. Former SBA Employees

Except upon the prior written approval of the SBA, Consultant shall not assign any former employee of the SBA to perform any of the services in this Agreement.

S. Data Security

Consultant and the SBA agree to the terms set forth in Schedule B, the Data Security Terms and the Systems Use Agreement, which are attached hereto and incorporated into this Agreement by this reference.

T. Counterparts

This Agreement may be executed in one or more counterparts, and when each party has executed at least one counterpart, this Agreement shall be deemed to be one and the same document.

U. Severability

If one or more provisions of this Agreement or the application of any such provisions to any set of circumstances shall be determined to be invalid or ineffective for any reason, such determination shall not affect the validity and enforceability of the remaining provisions or the application of the same provisions or any of the remaining provisions to other circumstances.

V. Remedies

All rights and remedies granted under this Agreement shall be cumulative and not exclusive of any other rights and remedies which the parties may have at law or in equity. The parties may exercise all or any of such rights and remedies at any one or more times without being deemed to have waived any or all other rights or remedies which they may have.

W. Survival

All representations, warranties, covenants and agreements set forth in Section II(F), (G), (H), (I), (J), (N), (O), (P), (R), (S), (V) and (Y) of this Agreement or in any instrument, document, agreement or writing delivered in connection therewith shall survive the completion of any of the Services provided hereunder or the termination of this Agreement.

X. Entire Agreement

The SBA and Consultant acknowledge that they have read this Agreement and that together with all written amendments, exhibits, schedules, and addenda hereto, which shall be incorporated by reference herein, this Agreement constitutes the entire and exclusive agreement between the SBA and Consultant with respect to the subject matter hereof, and no statement, agreement, or understanding not contained herein shall be enforced or recognized. THIS AGREEMENT CANNOT BE MODIFIED OR SUPPLEMENTED BY ORAL STATEMENTS MADE EITHER BEFORE OR AFTER EXECUTION OF THIS AGREEMENT AND ANY SUCH STATEMENTS DO NOT CONSTITUTE WARRANTIES. NO COLLATERAL OR PRIOR STATEMENTS, REPRESENTATIONS, UNDERSTANDINGS, AGREEMENTS, OR WARRANTIES (EXPRESS OR IMPLIED) ARE A PART OF THIS AGREEMENT.

Y. Binding Effect

This Agreement shall be binding upon the parties, their successors, legal representatives, and assignees. Consultant and SBA intend this Agreement to be a valid legal instrument, and no provision of this Agreement which shall be deemed unenforceable shall in any way invalidate any other provision of this Agreement, all of which remain in full force and effect. No waiver, alteration, or modification of any of the provisions of this Agreement shall be effective or binding unless in writing and signed by authorized representatives of both parties.

Z. Relationship of the Parties

The relationship between the parties is that of independent contractors. None of the provisions of this Agreement shall be construed to create a partnership or joint venture relationship between the parties or the partners, officers, members or employees of the other party by virtue of either this Agreement or actions taken pursuant to this Agreement. No employee or representative of Consultant will hold himself or herself out as, nor claim to be, an officer or employee of the State or the SBA by reason of this Agreement, nor will he or she make any claim of right, privilege or benefit which would accrue to an employee of the SBA under Florida law.

aa. SBA Policies

Communication Policy. Consultant acknowledges and agrees that it has received the SBA Communications Policy (#10-004) (the "Communications Policy"). Consultant

covenants and agrees that it shall comply with the Communication Policy, and such modifications to the policy as may be provided to Consultant from time to time, to the fullest extent that the Communications Policy applies to the Consultant. Consultant may not identify the SBA for purposes of business development or press releases without the express prior written consent of the SBA.

Fraud Hotline. The SBA maintains a fraud hotline at (888) 876-7548 to encourage individuals to report suspected SBA-related fraud, theft, or financial misconduct on an anonymous basis. Within 30 days following the effective date of this Agreement, Consultant agrees to communicate this hotline information to those of its employees that are responsible for to those employees providing services under this contract upon the written providing services under this contract. Consultant also agrees to re-communicate this hotline information at the request of the SBA.

bb. Notices

All notices, requests, instructions, other advice, or documents required hereunder shall be in writing and delivered personally or via a recognized overnight delivery service mailed by first-class mail, postage prepaid, to the following:

If to the SBA:

if mailed:	State Board of Administration of Florida Post Office Box 13300 Tallahassee, Florida 32317-3300 Attention: Executive Director
if hand delivered:	State Board of Administration of Florida 1801 Hermitage Boulevard Suite 100 Tallahassee, Florida 32308 Attention: Executive Director
If to the Consultant:	Luciola Solutions LLC 420 Summit Avenue Suite 316 Saint Paul, MN 55105 Attention: Marco Perzichilli Email: marco.perzichilli@luciola-im.com

cc. No Waiver:

A party's failure at any time to enforce any of the provisions of this Agreement or any right with respect thereto shall not be construed to be a waiver of such provision or right, nor to affect the validity of this Agreement. The exercise or non-exercise by a party of any right under the terms or covenants herein shall not preclude or prejudice the exercising thereafter of the same or other rights under this Agreement.

dd. Nondiscrimination:

Consultant agrees not to discriminate against any employee or applicant because of age, race, religion, color, handicap, sex, physical conditions, developmental disability, sexual orientation or national origin.

ee. Headings and Captions.

All headings and captions contained in this Agreement are for convenience of reference only and shall not affect in any way the interpretation or meaning of this Agreement.

ff. Pronouns.

Words used herein, regardless of the number and gender specifically used, shall be deemed and construed to include any other number, singular or plural, and any other gender, masculine, feminine, or neuter, as the context requires.

gg. Data Security.

Consultant and the SBA agree to the terms set forth in Schedule B, the Data Security Addendum, and the Systems Use Agreement that are attached hereto and incorporated into this Agreement by this reference.

IN WITNESS WHEREOF, the parties have caused this Agreement to be executed by their respective duly authorized officers as of the dates set forth below.

[redacted]

[redacted]

SCHEDULE A
SCOPE OF CONSULTING SERVICES

Evaluate current practices and assist in developing new tools supporting total portfolio optimization. Potential examples include tools/data/reports to evaluate:

- Total fund performance, attribution, and risk
- Ability to drill down to evaluate the source of return and risk attribution to better understand the source of risk / return analytics at the portfolio level
- Target risk/return goals in portfolio allocation
- Proper proportions to each asset class for portfolio optimization
- Investment selection that achieves the optimal result from a risk/return perspective
    - Are we getting as much return from the level of risk we are taking on?
    - Can we reduce risk for predetermined level of return?
    - Are we achieving return/volatility objectives that was the basis for the decision?
- Usage of time-weighted and dollar-weighted returns
- Ability to assess if we are accomplishing the original basis for prior investment decisions
- Leveraged vs unleveraged returns
- Ability to identifying risks that may not be successfully diversified risks across asset classes
- Factor generation capabilities supporting "what if" analysis

DELIVERABLES

a. An interim analysis and progress update to be provided approximately monthly. This can be completed in conjunction with Deliverable C below.

b. A detailed, written document setting forth the Consultant's evaluations, observations, suggestions and recommendations concerning the various issues, challenges and opportunities as detailed in this Schedule A, Scope of Consulting Services will be provided on or before September 15, 2023.

c. One or more meetings between Consultant and SBA in which the written report may be discussed and providing SBA Leadership with an opportunity to ask questions and provide challenges to the recommendations and conclusions offered.

SCHEDULE B:

STATE BOARD OF ADMINISTRATION DATA SECURITY ADDENDUM

1 DATA SECURITY STANDARDS

Consultant shall comply with either the provisions of applicable SBA policies (SBA Policy #20-404 Remote Access; SBA Policy #20-411 Anti-Virus; and SBA Policy #10-409 Confidential/Sensitive Electronic Data Handling), as amended from time to time, or NIST SP 800 Series, ISO/IEC 27000 Series, or a comparable similar industry standard. Consultant will provide immediate notice to the SBA of any known or suspected violation of any SBA policy or industry standard.

2 NONDISCLOSURE

SBA Data shall be considered confidential and proprietary information to the extent permitted by Florida or other applicable law. Consultant shall hold SBA Data in confidence and shall not disclose SBA Data to any person or entity, whether internal or external to the Consultant, except those persons that are directly involved with performing the duties under the Agreement and that further have a need to know the SBA Data in order to carry out their duties under the Agreement. Additionally, SBA Data may be disclosed when the disclosure is authorized by the SBA or is specifically required by law. For purposes of this Section 2, Data Security, "SBA Data" means all data accessed, created, maintained, obtained, processed, stored, or transmitted by Consultant in the course of performing the Agreement and all information derived therefrom.

3 LOSS OR BREACH OF DATA

Consultant shall provide immediate notice to the SBA in the event it becomes aware of any security breach or any unauthorized transmission or loss of any SBA Data. In the event of loss or destruction of any SBA Data where such loss or destruction is due to the fault or negligence of Consultant, Consultant shall be responsible for recreating such lost or destroyed data in the manner and on the schedule set by the SBA, at Consultant's sole expense, in addition to any other damages the SBA may be entitled to by law or this Agreement. In the event lost or damaged data is suspected, Consultant will perform due diligence, report findings to the SBA, and take all reasonable measures necessary to recover the data, all at Consultant's sole expense. If such data is unrecoverable, Consultant will pay all costs to remediate and correct the problems caused by or resulting from each loss or destruction of data (including, without limitation, the cost to notify third parties and to provide credit monitoring services to third parties), in addition to any other damages the SBA may be entitled to by law or this Agreement. Consultant acknowledges that failure to maintain security that results in a breach of data may subject this Agreement to the administrative sanctions for failure to comply with Section 501.171, Florida Statutes, together with liability for any costs to the SBA of such breach of security caused by Consultant.

4 SECURITY AUDITS

If SBA Data will reside in Consultant's system, the SBA may conduct, or may request Consultant to conduct at Consultant's expense, an annual network penetration test or security audit of Consultant's system(s) on which SBA Data resides. If the term of the Agreement is less than a year long, the penetration test or security audit of Consultant's system(s) on which SBA Data resides, may be exercised at any time during the term of the Agreement.

5 DATA PROTECTION

No SBA Data will be transmitted or shipped to entities outside of the United States of America, nor will it be stored or processed in systems located outside of the United States of America, regardless of the method or level of encryption employed. Access to SBA Data shall only be available to authorized Consultant Representatives that have a legitimate business need. For purposes of this Addendum, "Consultant Representatives" means Consultant's officers, directors, employees, agents, contractors, subcontractors and consultants (including affiliates thereof). Requests for access to the SBA's information technology resources shall be submitted to the SBA's Support and Office Services ("Help Desk") staff. With the SBA's approval, Consultant Representatives may be granted access to SBA information technology resources as necessary for fulfillment of related responsibilities.

6 ENCRYPTION

Consultant shall encrypt all SBA Data, in transmission and at rest, using an SBA approved encryption technology.

7 BACK-UPS

Consultant shall maintain and secure adequate back-ups of all documentation and programs utilized to process or access SBA Data.

8 DATA SECURITY PROCEDURES

Consultant has established appropriate administrative, technical, and physical safeguards to protect the confidentiality of, and to prevent the unauthorized use or access to, SBA Data. Consultant shall develop data security procedures to ensure only authorized access to data and databases by Consultant Representatives for purposes of performing the Agreement and to ensure no unauthorized access to data or databases by individuals or entities other than those authorized by the Agreement or the SBA. Consultant shall ensure that access to data and databases by Consultant Representatives will be provided on a need to know basis and will adhere to the principle of least privilege. (The principle of least privileged means giving a user account only those privileges which are essential to perform its intended function.)

9 OWNERSHIP OF DATA

Consultant shall provide to the SBA, upon its request, SBA Data in the form and format reasonably requested by the SBA. Consultant will not sell, assign, lease, or otherwise transfer any SBA Data to third parties, or commercially exploit SBA Data, except as authorized by the SBA. Consultant will not possess or assert any lien or other right against or to any SBA Data in any circumstances. SBA Data is and shall remain the exclusive property of the SBA. SBA Data created by Consultant, obtained by Consultant from a source other than the SBA,

or derived from SBA Data will become property of the SBA immediately upon the creation, receipt or derivation of such data, as applicable.

10 BACKGROUND CHECKS

Consultant shall confirm that their representatives (which includes Consultant's officers, directors, employees, agents, contractors, subcontractors and consultants, including affiliates thereof) assisting in the performance of the Agreement have passed appropriate, industry standard, background screening (include criminal background checks) and possess the qualifications and training to comply with the terms of the Agreement, before being provided access to SBA Data. Upon the SBA's request, Consultant shall provide to the SBA an attestation that the foregoing background checks have been completed.

11 COMPLIANCE

Consultant represents and warrants that it is in compliance with, and agrees and covenants that it will at all times during the term of the Contract continue to be compliance with, all applicable laws, regulations and industry standards (including, without limitation, all applicable laws, regulations and industry standards relating to cybersecurity or data collection, storage, security or privacy).

12 RETURN/ DESTRUCTION OF SBA DATA

Consultant shall not at any time destroy any SBA Data it holds without the prior written consent of the SBA. If requested by the SBA, within 30 days of the completion, termination or expiration of the Agreement, Consultant will transfer SBA data to the SBA (if so directed by the Agreement), or, unless otherwise required by any applicable law (including, for the avoidance of doubt, Florida's record retention laws), destroy all SBA data possessed by Consultant. Consultant shall provide the SBA documentation affirming the completion of any SBA requested data transfer (including confirmation of receipt by the SBA) and the destruction of any SBA Data possessed by Consultant. Notwithstanding the foregoing, Consultant may, in accordance with applicable legal, disaster recovery and professional requirements, store copies of SBA Data in an archival format which may not be immediately returned or destroyed but which would remain subject to the confidentiality obligations set forth in the Agreement.

13 BUSINESS CONTINUITY PLAN/ DISASTER RECOVERY

Consultant has implemented and will maintain business continuity and disaster recovery plans designed to minimize interruptions of services and ensure recovery of systems and applications used to provide the services under this Agreement. Such plans cover the facilities, systems, data, applications and employees that are critical to the provision of the services, and will be tested at least annually to validate that the recovery strategies, requirements and protocols are viable and sustainable. Consultant shall provide an executive summary of such plans setting forth prioritized threats, time criticality of business functions, resources needed to successfully recover, employee training and communication, and potential costs of recovery, as well as, including an assessment of the plans' most recent test results, to the SBA upon request. In the event of a business disruption that materially impacts (or is reasonably expected to materially impact) Consultant's provision of services under this

Agreement, Consultant will promptly notify the SBA of the disruption and the steps being taken in response.

IN WITNESS WHEREOF, each party has caused this Data Security Addendum to be executed by its respective duly authorized officer, as of June 1, 2023 *(the "**Effective Date**").*

[redacted]

[redacted]

STATE BOARD OF ADMINISTRATION
SYSTEMS USE AGREEMENT

The undersigned ("**User**") enters into this Systems Use Agreement (this "**Agreement**") in consideration of the provision to User of access to information technology resources of the State Board of Administration of Florida (the "**SBA**").

1. The following terms are defined as follows:
    a. "**Chapter 119, Florida Statutes**" means Chapter 119 (Public Records), Florida Statutes, as amended from time to time.
    b. "**SBA Account**" means any set of system access credentials (e.g., a user ID and password) provided by the SBA.
    c. "**SBA Data**" means all information accessed, created, maintained, obtained, processed, stored, or transmitted using any SBA Account or SBA Systems and all information derived therefrom.
    d. "**SBA Systems**" means any of the following:
        i. Any desktop, laptop, server, or other information technology resource (whether physical or virtual) under the administration or ownership of the SBA, wherever located;
        ii. All business applications, including any related data, system services and functions provided by or under the administration or ownership of the SBA.

2. SBA Data is and shall remain the exclusive property of the SBA. User shall use SBA Data solely for authorized purposes. SBA Data created by User, obtained by User from a source other than the SBA, or derived from SBA Data will become property of the SBA immediately upon the creation, receipt or derivation of such data, as applicable.

3. SBA Data shall be considered confidential and proprietary information to the extent permitted by Florida or other applicable law. User shall hold SBA Data in confidence and shall not disclose SBA Data to any person or entity except as authorized by the SBA or as required by law.

4. User does not have a right to privacy regarding any activity conducted using the SBA Systems. The SBA can review, read, access or otherwise monitor all activities on the SBA Systems or on any other systems accessed by use of the SBA Systems, and purge any or all information on the SBA Systems. The use of a password does not create a right to privacy in the SBA Systems.

5. Only persons who are authorized by the SBA may use SBA Systems. User shall not share SBA Account credentials with any other person, including but not limited to sharing of credentials with other authorized users. User shall immediately change User's password should it become known by any other person.

6. User shall not make copies of applications running on SBA Systems for use at home, on laptops, or for any other reason, without SBA authorization. User shall not import, download, copy or store SBA Data (including without limitation, emails) onto non-SBA owned devices without SBA authorization. User shall not import, download, copy, or store copyrighted material without permission from the copyright owner.

7. If User accesses the SBA network remotely, User shall do so only on devices with industry standard, supported anti-virus software installed. This software must be active, be scheduled to perform virus checks at regular intervals, and have its virus definition files kept up to date.

8. User shall not install any applications, programs, applets, or snap-ins on any SBA equipment.

9. User shall not access (or attempt to gain access to) any SBA Account or SBA System other than that to which the User is authorized.

10. User shall not use any SBA Account or SBA System to transmit, distribute, or store content or materials in a manner that violates SBA policies, U.S. state and federal laws, the laws of jurisdictions outside of the U.S., or the terms of this Agreement.

11. User shall comply with the provisions of applicable SBA policies, as amended by the SBA from time to time, including SBA Policy #10-400 Acceptable Use, SBA Policy #10-504 Passwords, SBA Policy #10-422 Email Communications/Internet Access Policy, SBA Policy # 20-404 Remote Access and SBA Policy #20-411 Anti-Virus.

12. If User becomes aware of (or suspects there may have been) any violation of this Agreement, User shall contact the SBA Support and Office Services ("**Help Desk**") at 850-413-1100 to report the situation.

13. User understands the provisions of this Agreement. User understands that violation of this Agreement may lead to penalties imposed by U.S. state and federal laws, and/or the laws of jurisdictions outside of the U.S.

14. User agrees to protect, indemnify, defend and hold harmless the SBA, its trustees, officers and employees from and against any and all costs, claims, demands, damages, losses, liabilities and expenses (including reasonable counsel fees and expenses, and investigation, collection, settlement and litigation costs) resulting or arising from or in any way related to User's breach of data security, negligent acts or omissions, fraud, willful misconduct, violation of law, or breach of this Agreement.

15. User acknowledges that SBA Data will constitute "public records" which will be subject to public access and disclosure under Chapter 119, Florida Statutes unless such records are exempt from disclosure under Chapter 119, Florida Statutes. To the extent applicable, User shall comply with Chapter 119, Florida Statutes. In particular, User shall:

    (a) Keep and maintain public records required by the SBA in order to perform the services under any applicable contract for services with the SBA ("**Contract**");

    (b) Upon request from the SBA's custodian of public records, provide the SBA with a copy of the requested records or allow the records to be inspected or copied within a reasonable time at a cost that does not exceed the cost provided in Chapter 119, Florida Statutes or as otherwise provided by Florida law;

    (c) Ensure that public records that are exempt or confidential and exempt from public records disclosure requirements are not disclosed except as authorized by law for the duration of the term of the Contract and following completion of the Contract if User does not transfer the records to the SBA; and

(d) Upon completion of the Contract, transfer, at no cost, to the SBA all public records in User's possession (if so directed by the SBA) or keep and maintain public records required by the SBA to perform the service. If User transfers all public records to the SBA upon completion of the Contract, User shall destroy any duplicate public records that are exempt or confidential and exempt from public records disclosure requirements. If User keeps and maintains public records upon completion of the Contract, User shall meet all applicable requirements for retaining public records. User shall provide all records that are stored electronically to the SBA, upon request from the SBA's custodian of public records, in a format that is compatible with the information technology systems of the SBA.

IF USER HAS QUESTIONS REGARDING THE APPLICATION OF CHAPTER 119, FLORIDA STATUTES, TO USER'S DUTY TO PROVIDE PUBLIC RECORDS RELATING TO THIS CONTRACT, CONTACT THE CUSTODIAN OF THE PUBLIC RECORDS AT:

STATE BOARD OF ADMINISTRATION OF FLORIDA
POST OFFICE BOX 13300
TALLAHASSEE, FLORIDA 32317-3300
(850) 488-4406
SBAContracts_DL@sbafla.com

16. This Agreement and any and all exhibits, schedules and enclosures attached hereto, which are incorporated into the Agreement by this reference, constitute and embody the entire agreement and understanding of User and the SBA with respect to the subject matter hereof, supersede any prior or contemporaneous agreements or understandings with respect to the subject matter hereof, and, unless otherwise provided herein, cannot be altered, amended, supplemented, or abridged or any provisions waived except by written agreement of User and the SBA.

17. This Agreement shall be construed and enforced in accordance with the laws of the State of Florida without regard to conflict of law principles. Any proceeding to resolve disputes regarding or arising out of this Agreement shall be conducted in the state courts located in Leon County, Florida, and User hereby consents to the jurisdiction and venue of those courts.

(The remainder of this page is intentionally blank.)

STATE BOARD OF ADMINISTRATION
SYSTEMS USE AGREEMENT

IN WITNESS WHEREOF, the undersigned "User" hereby agrees to the provisions of this Agreement, as of the Effective Date set forth below.

Attachments: SBA Policy #10-400 Acceptable Use, SBA Policy #10-504 Passwords, SBA Policy #10-422 Email Communications/Internet Access Policy, SBA Policy # 20-404 Remote Access and SBA Policy #20-411 Anti-Virus

10-400 Acceptable Use

Previous Revision: ***First Issued:***	August 15, 2019 [redacted] February 27, 2023 April 2, 2007 Date
Applies to	This policy applies to all users of State Board of Administration (SBA) systems and network. For the avoidance of doubt, this policy applies to all users regardless of the ownership of the computer or device connected to the network.
Purpose	The purpose of this policy is to outline the acceptable use of information technology resources owned and managed by the SBA and to promote the efficient, ethical, prudent, and lawful use of SBA's information technology resources. This policy addresses the responsibilities and obligations of users once access is granted but does not address the criteria for granting such access. This policy is intended to protect employees, contractors, visitors, customers, and business partners, as well as the SBA and its resources.
Policy	The information technology resources owned and managed by the SBA support the organization's goals and business processes. Usage of these resources is a privilege extended to employees (including OPS employees and interns), contractors, visitors, customers and business partners (collectively 'users'). Users have access to valuable organizational resources, to sensitive and critical data, and to internal and external networks. Consequently, it is important for all users to act in a responsible, ethical and legal manner. In general, acceptable use will be taken to mean respecting the rights of other users, the integrity of physical and digital assets, pertinent license and contractual agreements, and maintaining compliance with legal and regulatory requirements and related SBA policies. This policy establishes specific requirements for the use of all systems and network resources owned and managed by the SBA. While this policy deals specifically with issues involving the use of SBA information technology resources, it does not stand alone. Users are further reminded that state and federal (and possibly foreign) laws apply to the use of SBA's information technology resources, including but not limited to those dealing with: • copyright infringement • defamation • discrimination • fraud • harassment • identity theft • obscene materials • fiduciary principles • privacy • records retention
Governing Law	The unacceptable use of the SBA's information technology resources may be a violation of and/or trigger legal liability under several federal and/or state (and possibly foreign) laws depending on the nature of the unacceptable use. Such laws include, without limitation, criminal laws, intellectual property laws, privacy laws and

	laws relating to personal information, fiduciary laws, employment laws, civil rights laws and defamation and other tortious acts or failure to act.
Related Policies	10-032 Public Records Request 10-401 Personal Computer Security Policy 10-409 Confidential/Sensitive Electronic Data Handling 10-420 Enterprise Access Control 10-422 Email Communications/Internet Access 10-423 Telephony Systems and Equipment Usage 10-425 SBA-Owned Property 20-411 Anti-virus
Definitions	Computer – any electronic device that can be used for accepting, viewing, or processing information, regardless of form (e.g., desktop, laptop, mobile, handheld, etc.). Information Technology Resource – any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, interchange, transmission, or reception of data or information. Examples include computers, wired networks, wireless networks, internet access, printers, scanners, etc. User – any individual that accesses an SBA system or connects to the SBA network. Users include all employees of the SBA, the Division of Bond Finance, the Florida Prepaid College Plan, including OPS employees and interns. Users also include contractors, visitors, customers and business parties that are provided access to the SBA network.

Guidelines/Implementation

Subject to SBA Policies 10-401 Personal Computer Security Policy, 10-422 Email Communications/ Internet Access Policy, 10-423 Telephony Systems and Equipment Usage, and 10-425 SBA-Owned Property, all systems and services available at SBA are to be used for SBA business purposes only. Users will comply with SBA's technical, administrative, and process controls. Users will not engage in disruptive activity that could cause a failure or degradation of systems or services used by others. Users will not subvert a system or service for illegal or inappropriate use. Furthermore:

1. All computers remotely connected to SBA internal networks must use the most up-to-date anti-virus software that meets the requirements set forth in SBA Policy 20-411, Anti-virus.

2. All computers remotely connected to SBA internal networks must use a personal, host-based firewall.

3. Users may obtain access to files or systems only through their authorized logon credentials. The use of other credentials or tools to access files or systems is not permitted, except as authorized by the Senior Information Technology Officer (SITO) and Director of Information Security (DIS) to conduct required duties.

4. Users may not knowingly circumvent or modify any IT controls. Examples of controls include electronic email thresholds, web-filtering tools, proxy configuration, domain naming services, etc.

5. Users must not use any SBA system or service for unethical or illegal activities. Users will respect the privacy of others, use data only as authorized by the data and system owner, and not use SBA technology resources to harass or attack others. The SBA and users are subject to, and must comply with, federal, state, local and (possibly) other laws.

6. Users may not attempt to bypass network security mechanisms. Unauthorized network scanning (e.g., vulnerabilities, post mapping, etc.) of SBA network and computer systems is also prohibited.

7. Data which is confidential and/or exempt from disclosure under the Florida Public Records law, or which meets the criteria set forth in other policies, will not be transmitted over the Internet unless encrypted. Note that all data being transmitted outside the organization via the SBA email system is encrypted by default. Consistent with policy 10-409 Confidential/Sensitive Electronic Data Handling, users that need to transmit large amounts of data will consult with the Network Services Manager to determine the best and most secure mechanism to use. Note: Account credentials, including user IDs and passwords are classified as sensitive information in accordance with SBA policy 10-409, Confidential/Sensitive Electronic Data Handling.

8. Users of information technology resources with access to SBA data are responsible for the continued protection and integrity of such data including:

    a. Ensuring that the SBA's data is accurate, including the prevention of any intentional defacement or misuse;
    b. Ensuring that access to the SBA's data is restricted based on the needs of a job function, and ensuring that proper authorization has been granted for all access consistent with policy 10-420 Enterprise Access Control;
    c. Ensuring that data is available only for appropriate SBA personnel;
    d. Ensuring that confidential data is rigorously protected and used solely for SBA's business; and

9. Confidential data may not be shared with anyone without a legitimate business need, including friends or family members. Employees are required to comply with SBA policy 10-032, Public Records Request, if an employee receives a request to inspect and/or copy SBA data.

10. Viewing, storing or accessing of illegal content is not permitted.

11. Users may not use information technology resources to view, store or access obscene materials, such as pornography.

12. Users may not use information technology resources to support or oppose a candidate for public office or a ballot measure in a manner contrary to Florida and federal laws governing the political activities of public employees.

13. SBA resources are not to be used for non-SBA commercial purposes or for personal financial gain.

14. Users of information technology resources, including the posting of information on the SBA website, must comply with applicable copyright laws. When posting or downloading information to or from the Internet, the user is responsible for ensuring that copyright law is not violated.

15. Users may not falsify or misrepresent their identity, or enable others to falsify an identity, when using SBA information technology resources.

16. The use of Bit Torrent or other similar software is strictly prohibited. In addition, the use of any other software used for circumventing security controls or promoting anonymity is also prohibited.

17. The SBA may monitor and record usage to enforce its policies and may use this information to restrict access or to assist in a disciplinary, civil or criminal proceedings

18. All software installed, stored, or operated on SBA systems must be properly licensed, whether used for educational, professional, or private purposes.

19. Users are not authorized to access, use, copy, modify or delete data, or grant access to others, in a manner inconsistent with SBA policy.

20. Users are required to immediately report computer or network related suspicious activity to the Support Center to minimize damage and risk exposure.

Approved Exceptions

It is the responsibility of the user to ensure that their use of SBA-owned information technology resources is consistent with SBA policies. In cases of doubt, it is the responsibility of the user to review specific scenarios with the user's direct supervisor or manager. If additional clarification is required, the user, at the direction of the user's supervisor or manager, should contact the DIS or SITO.

Exceptions to this policy may be granted on a case-by-case basis by the SITO and DIS after consultation with the Chief Operating/Financial Officer. Exceptions should be requested via the Support Center

If clarification is needed regarding any aspect of this policy, it is the employee's responsibility to request a determination from the SITO.

Compliance

The SITO is responsible for monitoring compliance with this policy and may develop additional procedures to implement this policy. Management will be advised of breaches of this policy and will be responsible for appropriate remedial action which may include disciplinary action, up to and including suspension or termination of employment. Additional civil and/or criminal punishments may be applicable.

10-504 Passwords (Previously 10-410)

Previous Revision:	December 9, 2016	[redacted]	March 24, 2021
First Issued:	February 1, 2005	Ash Williams Executive Director & CIO	Date

Applies to	This policy applies to all user and service accounts on any computer system or application managed by the State Board of Administration (SBA), with the exception of external customer/participant accounts accessing the SBA's externally-facing websites.
Purpose	This policy establishes a standard for creation of strong passwords, the protection of those passwords, guidelines for third party implementation of password systems, and the frequency of required password changes.
Policy	The Director of Information Security (DIS) will establish passwords standards modeled on the guidance established by the National Institute of Standards and Technology (NIST). All users of SBA information systems are responsible for protecting the confidentiality of their user credentials. Where possible, user and system level passwords must be checked against an SBA approved list of known compromised and weak passwords at the time of creation and rejected if found to match any entry in the list. All privileged and service accounts must be managed by a privileged account management (PAM) system, where possible. All vendor supplied default passwords must be changed prior to any system implementation on the SBA network. SBA owned applications developed by SBA employees or contracted vendors must meet the password security requirements established in this policy. Legacy systems that do not support these requirements must be configured to SBA requirements as closely as allowed by the system. All users are responsible for immediately reporting any known or suspected compromise of SBA account credentials.
Governing Law	N/A
Related Policies	10-400 Acceptable Use 10-420 Enterprise Access Control 10-416 System Development 10-503 Data Classification
Definitions	**Privileged Access Management (PAM)** – a class of solutions that help secure, control, manage and monitor privileged access to critical information assets. **Passphrase** – a sequence of words or other text used to control access to a computer system, program or data. A passphrase is similar to a password in usage, but is generally longer for added security. **Password Blacklist** – a list of words or character strings disallowed as user passwords due to their commonplace use or inclusion in data breaches involving the compromise of user account credentials. **Salt** – random data that is used as an additional input to a one-way function that hashes data, a password or passphrase.

User – any individual that accesses an SBA system or connects to the SBA network. Users include all employees of the SBA, the Division of Bond Finance, the Florida Prepaid College Plan, including OPS employees and interns. Users also include contractors, visitors, customers, and business parties that are provided access to the SBA network.

Guidelines/Implementation

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of the SBA network and data systems. As such, all personnel who have or are responsible for a user account are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

User Account Password Standards (non-privileged accounts)

Passwords for all non-privileged end user accounts must meet the following minimum standards:

- Must be at least sixteen (16) characters in length.
- Users must use a separate, unique password for each of their work-related accounts.
- Passwords must be immediately changed upon suspicion or confirmation of compromise, but no other time-based change requirement applies.
- Users may not use any work-related passwords for any personal accounts.
- Users are encouraged, but not required, to include multiple character types (e.g. upper and lower case characters, numbers, and symbols).
- Users are encouraged to use passphrases in lieu of traditional passwords. Passphrases are easier to remember but generally harder to crack.
- Users should avoid creating passwords with multiple sequential or repeating characters (e.g. 1234567, aaabbbccc).

Privileged (Administrator) and Service Account Password Standards

Passwords for all privileged and service accounts must be created and managed by an SBA approved privileged account management (PAM) system, where possible, and meet the following minimum standards:

- Minimum length of twenty-four (24) characters.
- Include at least 3 of the following character types:
    - Uppercase letters
    - Lowercase letters
    - Numbers
    - Special Characters
- Must use a separate, unique password for each account.
- Passwords must be immediately changed upon suspicion or confirmation of compromise, but no other time-based change requirement applies.
- Administrators may not use any work-related passwords for any personal accounts.
- For passwords not managed by an SBA approved PAM solution, administrators are encouraged to use passphrases in lieu of traditional passwords and should avoid creating passwords with multiple sequential or repeating characters (e.g. 1234567, aaabbbccc).

Password Protection Requirements

Each user is responsible for protecting their assigned work-related user credentials. Passwords must not be shared with anyone, including supervisors, coworkers or IT employees.

- All passwords are to be treated as confidential information.
- Passwords must be protected by an SBA approved encryption algorithm when in storage or sent electronically.
- Passwords may be stored only in SBA approved password managers.
- Passwords must not be saved in web browsers or applications, unless approved in writing by the Director of Information Security.
- Employees must immediately report any compromise or suspected compromise of account credentials to their supervisor and the Information Security Office.
- Any compromised or suspected compromised password must be changed immediately upon identification. If the password cannot be updated immediately, the account must be disabled to prevent unauthorized access until the password can be changed.
- Requests to reset a locked or forgotten password must be made by the user, the user's supervisor, or a member of management and recorded in the SBA service ticket system.

System and Application Development Password Requirements

In addition to the previously defined requirements for user and service account passwords, SBA-owned systems and applications developed by SBA staff or by contracted vendor must meet the following requirements regarding passwords:

- Never hard-code passwords in software.
- All vendor-supplied default passwords must be changed prior to any system accessing the SBA network.
- Applications must support authentication of individual users, not groups.
- Application password length must be set to no less than 64 characters, where possible.
- Passwords should not be configured to require additional complexity beyond the requirements outlined in this policy but must allow the use of all standard character types allowed by the system (e.g. letters, numbers, and symbols).
- Passwords must be stored using an SBA approved salt and encryption algorithm.
- Applications must not transmit passwords in clear text over the network.
- Applications must provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.
- Support X.509 with LDAP security retrieval, wherever possible.

Compliance

The DIS is responsible for monitoring compliance with this policy and may develop additional procedures to implement the policy. The DIS will maintain sufficient documentation to demonstrate compliance with this policy.

10-422 Email Communications/Internet Access

Previous Revision:	December 9, 2016
First Issued:	February 8, 1994

[redacted]

12/16/19
Date

Applies to	This policy applies to all users of the State Board of Administration (SBA) email and Internet systems. This policy is also applicable to all employees of the Division of Bond Finance and the Florida Prepaid College Program. However, in those areas of the policy where SBA leadership is specified as the decision making authority, the authority for decision making related to Division of Bond Finance and Florida Prepaid College Program employees will rest with the Director and Executive Director of the respective entities.
Purpose	This policy establishes appropriate use by SBA personnel of the SBA email, computer networking, and Internet access systems. All electronic communications by SBA personnel are subject to these policies and guidelines. This includes communications sent electronically via SBA email or approved instant messaging technologies, and all computer networks used for downloading data and accessing remote computer databases, web sites, discussion groups, or the computer networks of SBA business associates.
Policy	The SBA email system and Internet access are available to all SBA employees subject to the guidelines and procedures established and implemented by the Director of Information Technology (DIT). Employees are encouraged to use email and the Internet for business communications and research related to SBA official business, which may include both internal and external matters. Personal use of the SBA email system and Internet access is discouraged. Personal use of the email system and Internet access must be brief and infrequent and not constitute inappropriate use as described further in this policy and guidelines. Although it is intended that the Internet be used for business purposes, limited access to other sites is permitted before or after approved working hours and during approved breaks. Examples of acceptable Internet sites for personal usage are those pertaining to health matters, weather, news, business topics, community activities, and career advancement. Under certain circumstances, such as emergency weather conditions, access to sites such as weather and news services may be appropriate during approved working hours.
Governing Law	Chapter 119, Florida Statutes (Public Records Law)
Related Policies	10-400 Acceptable Use Policy 10-409 Confidential and Sensitive Electronic Data Handling 10-417 Instant Messaging 10-131 Records Management

Guidelines/Implementation

Oversight and Administration of the Email System and Internet Access

The DIT will govern the email system and Internet access. The DIT will designate a "Systems Administrator," who is responsible for providing secure access to the email and Internet system. The DIT is responsible for developing procedures outlining appropriate use of the email and Internet systems and compliance monitoring, to include primarily automated monitoring and retention of related activity logs. Requests for access to email communications and Internet usage records must be approved by one of the following: Executive Director & CIO, Deputy Executive Director, Inspector General, General Counsel, or Chief Operating/Financial Officer. The Systems Administrator may perform necessary administrative activities in managing the email system and Internet access, which may involve access of the email files or Internet records of employees. In this regard, it is expected that the Systems Administrator will manage the email and Internet system under the highest standards of ethics and business practices, and in a manner that facilitates SBA communications yet safeguards the security of communications. Communications security activities must comply with relevant policies governing communications of a sensitive business nature between employees.

Prohibited Usage of Email and Internet Systems

The email system and Internet access are SBA resources. It is prohibited to use SBA technology resources or work time for political campaigns or messaging, job-seeking, solicitations, operating a personal business, fund raising for any causes or any other activity that is inconsistent with SBA policies. No employee will send email or other communications, files, or programs containing offensive or harassing statements, including comments on race, national origin, sex, sexual orientation, age, disability, religion, any other protected class or political beliefs. Managers should report suspected violations of this policy to the Inspector General to ensure that the SBA email system and Internet are used for appropriate purposes.

Email Guidelines

Email as Official Records

Many documents produced on email systems are records of business transactions or serve as documentation of official business activities. Email messages transmitted through the SBA's email system are considered SBA property. Emails that are more than ninety days old are automatically archived and retained for ten years in an electronic archiving system. Due to the fact that email records can be many different types of official records, there is no single retention period that covers all email records. For emails with a retention schedule of longer than ten years, the email recipient is responsible for transferring the message to a format or file location that may be retained in accordance with the applicable retention period referenced in policy 10-131 Records Management. Finally, email records regarding the SBA's official business are considered public records under the laws of the State of Florida and subject to inspection and/or copying pursuant to a public records request.

Email communications produced on computer equipment and networks supported and funded by the SBA must be truthful and accurate, and the same care must be used in drafting email and other electronic documents as for any forms of communication. Email records are often required to be produced during litigation and discovery proceedings, and they are subject to copyright restrictions and libel laws. Material that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory, or otherwise unlawful or inappropriate should not be sent by email or instant messaging, routed among workgroups, posted to discussion groups, or placed on electronic bulletin boards. Unless expressly permitted by policy or otherwise (e.g. SBA Fraud Hotline), SBA employees must identify themselves as the sender in all communications, as anonymous communications are prohibited, and it is prohibited to modify any email or other communications parameters in an effort to prevent identification of the sender.

Privacy of Email Communications

Email messages or other communications sent or received via SBA computer systems are open for inspection and/or copying by the SBA, subject to Florida law. All email messages and other communications using SBA computer systems and networks are subject to monitoring and review for inappropriate use, system maintenance, legal and administrative reasons, and security purposes and may be subject to disclosure and release under Florida's Public Records Law, a court order or, in the SBA's discretion, if permitted by law. The email system is a technology resource licensed, funded, operated, and owned by the SBA, and as a result, the SBA has free and unrestricted access to all email messages produced, received, transmitted, or retained on SBA computer systems and networks, subject to Florida law. As such, the SBA reserves the right to access and disclose all messages sent over its electronic mail system for any lawful purpose.

Internet Usage Guidelines

Background

The Internet is an informational resource available to SBA personnel for the conduct of business activities. Access to information, documents, and data available on the Internet is critical to SBA personnel for general business reference purposes. The SBA and many of its business associates use Internet-based web sites for posting information, documents, data, and reference resources. However, access to Internet resources by SBA personnel is granted based on the clear understanding that they will be personally and professionally responsible for how they access and transmit Internet based information. When using the Internet to conduct business, employees represent not just themselves, but the SBA. In addition, employees should be cautioned that many Internet sites contain potentially offensive, sexually explicit, or other inappropriate material for reading or using while working at the SBA. Accessing such sites on SBA equipment is strictly prohibited.

Internet Security

The SBA and its employees must protect against computer system intrusion and any possible resulting business risk or damages. Business sensitive or confidential data must not be accessible to external organizations or individuals without proper computer security controls and adherence to personnel authentication procedures. No business sensitive or confidential data may be transmitted across the Internet without proper security precautions implemented in advance through data encryption in transit and at rest, digital signatures, or other data protection measures consistent with SBA standards. Any employee that is uncertain whether such controls are employed by a third party has an obligation to request a review by the Director of Information Security (DIS) or DIT prior to uploading sensitive or confidential data. No computer software or executable files may be downloaded to SBA computers without a prior request made to the Support Center and upon authorization from the DIS or DIT. To maintain data security and avoid the spread of computer viruses, users must not attempt to circumvent SBA established security controls for any reason, including to access unauthorized content, and should avoid going to questionable or non-business related web sites that may harbor malicious code. The SBA employs virus detection software to scan all email, email attachments, and other files downloaded from the Internet. However, no technology is perfect and employees should proceed with caution before opening attachments or downloading files from unknown sources. All suspicious emails should be reported by using the automated Phish Alert mechanism within the email system. When in doubt about the safety of downloading files from the internet, contact the Support Center for guidance.

The SBA uses software to identify inappropriate or sexually explicit Internet sites, which will be blocked from access by SBA employees. In the event that an inappropriate or sexually explicit site is encountered while using the Internet, employees are required to disconnect immediately from the site. The SBA has the right to monitor all aspects of Internet usage including, but not limited to, monitoring sites visited by employees, including chat groups and social media, and reviewing material downloaded or uploaded by users to the Internet.

Privacy of Internet Communication

All communications by SBA employees across the Internet should occur with trusted sources when possible. Business-sensitive or confidential information should only be transmitted over the Internet when necessary for the SBA to fulfill its responsibilities and only after ensuring that proper security controls, including encryption, are applied. Note that all data transmitted outside the organization via the SBA email system is encrypted by default. Employees that need to transmit large amounts of data will consult with the Network Services Manager to determine the best and most secure mechanism to use.

Compliance

The DIT is responsible for monitoring compliance with this policy and is responsible for administering and ensuring the security of the SBA's email and internet system. The DIT may develop additional procedures to implement this policy and will maintain sufficient documentation to demonstrate compliance with this policy. Management will be advised of breaches of this policy and will be responsible for appropriate remedial action, which may include disciplinary action, up to and including suspension or termination of employment. Additional civil and/or criminal punishments may be applicable.

20-404 Remote Access

Previous Revision: ***First Issued:***	October 5, 2020 February 1, 2005	[redacted] [redacted] 5-24-22 Date
Applies to	This policy applies to all State Board of Administration (SBA), Florida Prepaid, and Division of Bond Finance employees, including OPS and Interns, and authorized third parties (vendors, auditors, etc.).	
Purpose	The purpose of this policy is to set forth the requirements for remote access to the SBA's computer network and to ensure such access is carried out in a secure and responsible manner.	
Policy	Employees may utilize remote connections from SBA managed devices using the SBA's VPN capabilities. SBA managed devices must adhere to the SBA's 10-401 Personal Computer Security Policy. SBA also supports remote access via Citrix connections using either SBA managed devices or non-SBA managed devices for the following scenarios: • An employee who has a business need and proper approval from their supervisor • An approved third party with proper approval from their SBA Third-Party Sponsor per the SBA policy 20-420 Enterprise Access Control VPN connections are not allowed from devices that are not owned and managed by the SBA. All remote (VPN and Citrix) connections require Multi-Factor Authentication. All (VPN and Citrix) connections will be automatically disconnected from the SBA Network(s) once an approved time-base period of inactivity is detected or the maximum session length of time is reached, whichever occurs first.	
Governing Law	N/A	
Related Policies	10-401 Personal Computer Security Policy 10-420 Enterprise Access Control 10-502 Security Configuration Management 10-504 Passwords 20-411 Anti-Virus	

Definitions	Employee – All SBA, Florida Prepaid and Division of Bond Finance employees, including OPS and Interns. Users – All SBA employees, including OPS and Interns, and approved third parties that use SBA IT resource(s). Approved third parties – Non-SBA employees that have a contractual or regulatory relationship with the SBA, such as vendors, state auditors, etc. Virtual Private Network (VPN) – Remote access technology that extends a private network across a public network, enabling users to send and receive data as if their computer devices were directly connected to the private network, while maintaining security and privacy. Citrix – A technology that provides remote access to SBA applications that provides security controls to protect user and corporate information even when accessed from personally owned devices not managed by the SBA. Third-Party Sponsor – The SBA, Florida Prepaid or Division of Bond Finance employee overseeing a third party's contractual, regulatory or audit activities.

Guidelines/Implementation

In today's workplace, there is an ever-increasing demand that access to internal resources be provided to individuals that are not physically located at the SBA.

1. Remote access requests for approved third parties will be granted by the Director of Information Technology (DIT) or designee, contingent upon the following criteria having been met:

    a. The Third-Party Sponsor of the individual requiring remote access must follow all aspects of SBA Policy 10-420 Enterprise Access Control to secure the access. This includes submitting the request and the business justification for the access in writing to the Support Center.

    b. The individual requesting remote access is determined by the DIT or designee not to present a security risk and furnishes any requested information required in making this determination.

    c. If the approved third party is covered by an executed contract with the SBA, the contract must include protective provisions such as those detailed in the SBA Data Security Addendum and the Systems Use Agreement

    d. If the approved third party is not covered by an executed contract with the SBA or if the executed contract does not include the Systems Use Agreement terms, the individual requesting remote access must sign the SBA Systems Use Agreement.

2. Access to specific SBA internal network resources through remote connections will be administered via separate guidelines. Different and distinguishable access restrictions will be applied to SBA employees and to approved third parties granted remote access.

3. It is the responsibility of all individuals with remote privileges to ensure that their connections do not allow unauthorized users access to SBA internal networks.

4. It is the responsibility of all individuals with remote privileges to contact the SBA Support Center regarding any suspected breech of security that may have allowed unauthorized access to the SBA network.

Dual (split) tunneling is permitted. All traffic to and from the SBA network and all traffic that must be sourced from an IP within the SBA's ARIN registered networks per third-party requirements must be routed through the SBA VPN tunnel. All other web-based traffic may be routed through the user's internet service provider (ISP) via an SBA approved secure web gateway technology capable of implementing access restrictions similar to those applied to users operating from the SBA network.

Compliance

All SBA staff is responsible for compliance with this Policy. The DIT is responsible for monitoring compliance with this policy. The DIT may develop additional procedures to implement this policy and will maintain sufficient documentation to demonstrate compliance with this policy.

20-411 Anti-virus

Current Revision:	January 26, 2018
Previous Revision:	February 1, 2005
First Issued:	February 1, 2005

[redacted]

Applies to	All computers and mobile devices directly or indirectly connected to the State Board of Administration (SBA) network, including employee owned computers and mobile devices.
Purpose	This Policy establishes requirements that must be met by all computers connected to the SBA network, either directly or indirectly (VPN or other remote access), to ensure effective virus detection and prevention.
Policy	• All SBA computers will have a default standard licensed copy of anti-virus software installed and active. The most current available version of the anti-virus software package will be taken as the default standard. • All computers attached to the SBA network must have standard, supported anti-virus software installed. This software must be active, be scheduled to perform virus checks at regular intervals, and have its virus definition files kept up to date. NOTE: Some anti-virus vendors allow their products to also be installed on employee owned devices but it is the personal and financial responsibility of the employee to ensure their devices have default standard anti-virus installed and active prior to connecting to an SBA Network. • Any activities with the intention to create and/or distribute malicious programs onto the SBA network (e.g. viruses, worms, Trojan horses, e-mail bombs, etc.) are strictly prohibited. • If an employee receives what he/she believes to be a virus or suspects that a computer is infected with a virus, it must be reported to the IT department immediately via SBA Support & Office Services. The following information should be reported (if known): virus name, virus symptoms, extent of infection, source of virus, and potential recipients of infected material. • No employee should attempt to destroy or remove a virus, or any evidence of that virus, without direction from the IT department. • Any virus-infected computer will be removed from the network until it is verified as virus-free.
Governing Law	N/A

Policy References N/A

Guidelines/Implementation

Containment of Virus Incidents

IT will take appropriate action to contain, remove and recover from virus infections affecting the SBA's network. In order to prevent the spread of a virus, or to contain damage being caused by a virus, IT will remove a suspect computer from the network.

IT will assist with recovery from viruses. This includes advice on containment to stop the spread, help with removing viruses, taking note of information about the incident and advice on how to prevent a recurrence.

Compliance

The DIT is responsible for compliance with this Policy and may develop additional procedures to implement this policy. The DIT will maintain sufficient documentation to demonstrate compliance with this policy.