

Invitation to Negotiate for Asset Guidance Services

State Board of Administration Responses to Requests for Clarification August 7, 2023

According to the ITN Section 5.1, "Requests for clarification regarding the specifications and/or requirements of this solicitation should be sent..." Only the questions meeting this criteria are answered below. Any requests for data or documents will be forwarded to the SBA's General Counsel's office for processing.

1. If a more granular list is available than provided in Appendix A, please list the key features of the participant website and of any reporting or other tools required by FRS.

Response:

Additional information on the current services provided by GuidedChoice are available at <https://www.myfrs.com/GuidedChoiceAdvisorService.htm>. Monthly usage, uptime, and data aggregation usage are to be provided monthly with the monthly invoice.

2. Describe the extent of integration of this service with Alight and the extent to which participants access the service directly and/or through Alight (or other entry points). How many DC and DB systems will the service provider need to integrate with?

Response:

Members access the Advisor Service by logging into MyFRS.com, then clicking an Advisor Service button that takes them directly to the online advice service. Members do not currently access the service directly and/or through Alight.

As indicated in Exhibit 2, the connectivity capabilities with Alight currently/preferred are as follows:

- *Currently, Investment Plan members who accept the current AGS investment recommendation guidance (fund changes), have this information flow electronically from AGS to Alight Solutions via an Application Programming Interface (API). Beginning in July 2024, Alight Solutions will no longer support such APIs.*
- *The SBA prefers an AGS who has an existing, integrated relationship with Alight Solutions and can provide fund change transactions seamlessly. If such a relationship does not exist, the AGS is required, at the AGS' expense, to establish such a connection.*

The service will need to integrate only with the FRS Pension Plan (DB) and FRS Investment Plan (DC).

3. A publicly available online brochure for the current service (<https://www.myfrs.com/pdf/GuidedChoiceAboutUs.pdf>) appears to describe the extent of accounts covered by the asset guidance more broadly than described in Appendix A. To what extent do the asset guidance services provide advice/guidance on participant assets outside of the covered DC plans- e.g. other retirement or non-retirement accounts (including self-directed brokerage assets) or are those taken as a "given" which may influence the asset guidance for covered plans? How are spousal assets and advice/guidance addressed?

Response:

The current tool takes into account the following when making recommendations:

- *Member's taxable assets*
- *Member's other tax-deferred assets*
- *Spouse's tax-deferred and taxable assets*
- *Member's and spouse's projected social security income*
- *Member's and spouse's other sources of retirement income, including annuities*

The current tool gives investment advice on employer sponsored retirement plans and IRAs. It does not give investment advice on taxable accounts.

The SBA is open to providers who can provide investment advice on the Investment Plan, 457, 403(b), IRA's, etc., on both taxable and non-taxable accounts.

4. What steps are involved in a participant choosing to implement the point in time advice online? Does this apply to both investment changes and savings rate changes? When a participant engages with the service, what if any agreement or acknowledgement do they enter into, and/or what disclaimers or disclosures are presented to them? Does the service provider have any contractual relationship with the participants today?

Response:

The SBA prefers an AGS who has an existing, integrated relationship with Alight Solutions and can provide Investment Plan fund change transactions seamlessly.

FRS employee contributions are fixed at 3% and employees cannot make additional contributions beyond the 3%. The tool should recommend additional savings for any non-FRS accounts.

Members who utilize the advisor service for the first time must acknowledge specific privacy and security items. In addition, MyFRS.com first time users must acknowledge that they have reviewed the following privacy, security, and terms of use: <https://www.myfrs.com/Privacy.htm>

The current service provider only has a contractual relationship with the SBA (not individual members).

5. Does the current service provider need to do anything differently based on underlying participating employers (e.g. various state, county and municipal employers), such as tracking specific plan offerings or providing participant assessments/reporting with the name of the underlying participating employer?

Response:

No. The Division of Retirement of the Department of Management Services is the central repository for all FRS member data that it receives from FRS employers (city, state, county, etc.). Data feeds are provided by the Division of Retirement to the provider.

If a member wants to take into account a 457 account he has with his employer, he is responsible for entering the applicable data.

6. What entity pays the fees for the covered services today and are you anticipating any changes to the way fees are paid? Also, we understand that participants do not pay the fees for the current services;

are there any add-on or premium services directly associated with this offering for which participants do pay a fee directly?

Response:

The SBA pays all the fees for the service provider. Active members or terminated/retired members with a balance in the Investment Plan do not currently pay the service provider for any services.

We do not anticipate any changes to the above fee model but are open to reviewing any add on services you may want to propose.

7. What type of access does E&Y have to the services/technology and to what extent do they receive participant-specific information through the technology? Are there any contractual relationships, intellectual property protections or other formal arrangements in place between the current provider and E&Y whom we understand is expected to continue to serve in a similar capacity going forward?

Response:

EY can access the service as a superuser and run the advisor service on behalf of a member.

The current service provider does not have a contractual arrangement with EY. The previous service provider did have a contractual arrangement with EY and the SBA. We are open to such a triparty agreement, if needed.

8. Please describe how participant and E&Y end user web authentication is managed / federated between SBA and other vendors today; is/could SAML be used?

Response:

Participants access the service by logging into MyFRS.com via normal security measures (password, username, MFA). EY accesses the service by logging into its customer service application then selecting the service. The current service provider established the secure connection for EY.

When members login to MyFRS.com it is considered single sign on and the member can access the service provider, the 2nd Choice tool, and Alight (if an Investment Plan member) without having to login separately for each service.

Use of SAML could be utilized.

Data transferred between partners and from the Division of Retirement are all provided via secure connections.

9. We understand that while E&Y handles participant calls; Appendix A notes that the respondent “may be responsible for operating a limited technical support telephone service for other partner vendors”. Please confirm that the respondent is not expected to handle calls directly from participants and please confirm which party handles participants requests for technological assistance (e.g. password resets, navigation questions, etc.). If technological assistance calls are handled by the current provider please provide estimated call volume similar to that provided in the ITN for other providers.

Response:

EY fields all questions from FRS members regarding the service, including any technological assistance. The service provider must provide technical support telephone service only to EY, Alight, TekStream, or the SBA, if needed. Only a handful of technical support telephone calls are anticipated yearly.

10. What is the role of web portal provider TekStream with respect to the services and do they have any involvement in the current participant user experience?

Response:

TekStream is the web portal provider and acts as the gatekeeper for MyFRS.com. TekStream will be responsible for assisting with connections between MyFRS.com and the service provider.

TekStream has no role in the participant user experience.

11. Please describe any feature/functionality differences SBA expects for participants at different life stages; a basic example being accumulator vs. near retiree vs. already retired participants. Do retirees have access to the guidance system or receive the annual Personal Forecast Statement?

Response:

We are open to any life stage services you want to offer.

Pension Plan terminated members or retirees (except for DROP members) do not have access to the service. Terminated or retired Investment Plan who maintain a minimum balance of at least \$1,000 in their account have access to the service.

The Personal Forecast Statement is not currently produced. If produced, it would most likely be sent only to active Investment Plan and Pension Plan members.

12. Section 4.5 of Appendix A states "This statement is not currently produced; however it may be reinstated in the future. See sample in Appendix D". Is the fulfillment of printing and mailing either on demand and/or periodically scheduled Employee Personal Forecast Statements by the AGS a hard requirement respondents must include in our responses, and/or could it be fulfilled by a third-party (eg. Alight Communications)?

Response:

Printing and mailing via a third party would be permitted as long as appropriate security was utilized.

13. Per Section 1.3 of Exhibit 5, please define "Transition Services Plan" : "Detail your Transition Services Plan including all operational and organizational components, and specifically the method of data transfers, supported data file formats and related data dictionaries."

Response:

If a new service provider is chosen, a transition process would be required. We are requesting a detailed explanation of how you would conduct this transition (project plan, data connections required, etc.).

14. Per Section 9.1 of Exhibit 5, please clarify the intended uses and users of these: "What API's, web service, or other integration points are provided for your application?"

Response:

*Uses: Setting up connections with other partners to exchange data and communicate in a secure way.
Users: Other partners and state agencies (Alight, TekStream, EY, SBA and Division of Retirement).*

15. Can you provide more details on the current DB integration, the data/projection provided to the advice provider, the range of scenario analysis required and assumptions that are made. How often there are

updates to consider and should participants be notified to refresh advice as DB benefit changes? And does current service assist participants in making decisions around DB benefits or with the decision between DB and DC that can be made at time of hire and again once during employment?

Response:

Pension Plan (DB) members can utilize the service for projections on their future Pension Plan benefit, Social Security, outside assets, etc. The current tool gives investment advice on outside assets (457, 403(b), etc.).

Each time a member logs into the service, current data is pulled from the Division of Retirement thereby updating the service.

Members who have not logged into the service for over a year are sent an email encouraging them to login and check their progress.

The service does not assist members in choosing between the Investment Plan or Pension Plan, and should not be considered for this ITN. The choice service is provided by a separate vendor.

16. How often do participants consolidate assets, and does that happen manually or via an account aggregation service? Does it happen primarily through discussions with E&Y reps, or Participant-led?

Response:

The frequency with which members consolidate assets is unknown. If members choose to consolidate assets within the Investment Plan they would most likely discuss the rollover process with EY or Alight.

17. Does the Participant and/or E&Y rep set up distributions based on the income forecast?

Response:

Members who receive an income forecast may discuss various distribution options with EY. However, the ultimate distribution decision would be the members who would set the distribution up either online or by contacting Alight.

18. How often are there fund line up changes?

Response:

Line up changes are infrequent. The most recent change was effective July 1, 2023 when the 2065 Retirement Date Fund was added.

19. Is there an expected document exchange approach to host the annual Personal Forecast Statement on the MyFRS website?

Response:

The Personal Forecast Statement could be placed in an Investment Plan member's online mailbox hosted by Alight. Pension Plan members do not have such a mailbox on MyFRS.com.

20. What is the data exchange format and frequency for employee data flowing between the Division of Retirement and the current guidance service? What is the comprehensive set of data points being exchanged between the Division of Retirement and the current guidance service?

Response:

A new service provider would receive an initial data dump for all FRS members. Subsequently, each time a member logs into the service, current data would be pulled from the Division of Retirement thereby updating the service.

All applicable data needed to calculate projections would be provided. Detailed data points will be provided later in the ITN process to finalists, if requested.

21. What is the shared unique participant identifier to link data between Alight, Division of Retirement, and/or TekStream? SSN? Employee ID?

Response:

Social Security number.

22. Are there any SLAs or service model requirements for the guidance provider to confirm that a participant's DC plan guidance was properly implemented? In the event a participant's guidance implementation fails due to a pending transaction, who is responsible for following up with the participant or Alight to notify them of the issue and/or ensure the guidance transaction is implemented after the account hold is removed?

Response:

SLA's will be decided upon during the contract phase.

If implementation of the guidance did not process, the service provider would contact the SBA and Alight. Alight would contact the member.

23. How many participants have implemented an updated DC plan asset allocation within the current guidance service over the last 3 years?

Response:

The requested information is not readily available and may not be available prior to the submission date.

24. To better understand the likelihood & potential timeline for needing to integrate with another recordkeeper for the continued provision of these services, what is the remaining duration of the State of Florida's existing contract with Alight Solutions for recordkeeping services?

Response:

Alight's contract is in effect through June 30, 2025, with a two year extension possible.

25. Please provide the full list of DB and DC plans that the current service provider includes through automatic feed or calculation (as opposed to by participant entry).

Response:

Not applicable. The FRS Pension Plan (DB) and FRS Investment Plan (DC) are the only two plans.

26. Per Section 3.10 of Appendix B, please provide copies of SBA Data Security Standards: "User 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,..."

Response:

See the policies attached.

27. Appendix A – 3 Deliverables – second paragraph states that Alight Solutions, Division and Tekstream are responsible for giving the AGS electronic access to member data. Do any of these data providers require separate agreements or fees with the AGS for these connections and/or services or are all of it covered via this agreement with the SBA?

Response:

Separate agreements are not currently required between the service provider and Alight, the Division of Retirement, or TekStream. Fees may be possible depending on the connections or services required.

28. Appendix A – 3.2 Specific Software Requirements 3.2.6 – Can you clarify which fees need to be covered? Is this referring to the fees charged for the Advice Service or typical fees imbedded in funds like 12b-1 fees?

Response:

The fees referred to in this section are typical fees charged by investment funds.

29. Appendix A – 3.2 Specific Software Requirements 3.2.9 – Is this referring to the market in general over time or specific to the investments available within the Florida Retirement Plan?

Response:

Both. Historic investment returns in general and for specific Investment Plan funds or 457, 403(b), IRA funds being evaluated.

30. Appendix A – 3.5 Employee Personal Forecast Statement

- a. How will the data be provided to generate the statements, considering there are multiple sources?
- b. How will the statements be transferred to the SBA for distribution and who will be responsible for lading it into the member account on the MyFRS site?
- c. Are you open to the option of providing the statement via the web-based financial education services application via single sign on?

Response:

- a. *Data for Pension Plan members will be provided by the Division of Retirement. Data for Investment Plan members will be provided by both the Division of Retirement and Alight.*
- b. *The Statements will either be mailed to members home address or an electronic copy will be placed in their online mailbox (Investment Plan only).*
- c. *We are open to providing the Statement in such a manner.*

31. Can you describe the data available to support the supplemental plans that FRS members have access to for voluntary contributions (403(b), 457, 401(k), etc.)? This includes plan rules, investment lineups, and employee data.

Response:

The current service provider does not have any data links with outside supplemental plans. Members voluntarily enter the specifics of the plan into the service (type of plan, member or spouse's plan, total assets, funds invested in, etc.).

32. Does the current provider offer, or does the scope of the RFP include providing fund level investment advice on these supplemental plans (403(b), 457, 401(k), etc.)?

Response:

Offering fund level investment advice on supplemental plans is preferred. However, we are open to evaluating other investment advice (for example, advice on asset categories members should consider investing in).

33. For those who elect the Pension Plan, what kind of data will we receive?

Response:

Salary, service credit, Pension Plan projected benefits, etc.

34. Will the Employee Website (www.MyFRS.com) need any prepopulated data from our database in a widget to direct traffic to us?

Response:

The current design requires the member to login to MyFRS.com, then access the service provider via a link on the landing page. This single sign on allows the member to access the service provider, the 2nd Choice tool, and Alight (if an Investment Plan member) without having to login separately for each service.

35. One of the specific software requirements (3.2.6) refers to fees and how they impact long-term returns. Is this more of a general explanation of fees or the specific fees related to the investment products available in the FRS system?

Response:

Both. Historic investment returns in general and for specific Investment Plan funds or 457, 403(b), IRA funds being evaluated.

36. If EY is the primary contact for members utilizing our software, will EY or FRS be the one to assess our performance and utilization?

Response:

The SBA will assess the service provider's performance and utilization.

37. Is Financial Well-Being an important piece of the deliverables?

Response:

Preparation for retirement is paramount to the SBA. The service provider tool is a key component of this preparation. Financial Well-Being, as it relates to the preparation for retirement, should be considered an important deliverable.

38. Is telephone support all that is necessary, or do we need additional channels for operational technical support as well?

Response:

EY fields all questions from FRS members regarding the service, including any technological assistance. The service provider must provide technical support telephone service only to EY, Alight, TekStream, or the SBA, if needed. Only a handful of technical support telephone calls are anticipated yearly.

39. On what section/area of the SBAFLA.com site will clarifications be posted?

Response:

Responses to requests for clarification, and all other announcements pertaining to this ITN, will be posted to Doing Business with the SBA > Vendors page, <https://www.sbafla.com/fsb/DoingBusinesswiththeSBA/Vendors.aspx>.

40. Would FRS be amenable to advisory services that are borne by the member, by FRS, or both FRS and the member?

Response:

We are open to reviewing such arrangements. Please provide cost estimates based on each of the above scenarios, if applicable.

41. Appendix A, Section 3 mentions data furnished by the Division. Are phone numbers part of the data? What percentage of members have a phone number on file? Would we be able to offer to take calls directly from members if we didn't charge FRS? What if we did?

Response:

Telephone numbers are not currently included in the data provide to the service provider. Telephone numbers are collected from members; however, the exact percentage is unknown.

We are open to reviewing how you would contemplate taking calls from members at no cost and at cost.

42. Employee Personal Forecast Statements: Section 3.5 of Exhibit A states that statements may be printed and mailed or stored electronically on MyFRS.com with password protection. As an alternative form of delivery can the AGS (Asset Guidance Specialists) email the statement to members? What percentage of members have email addresses linked with their employer or the SBA? Could an email-only delivery be considered, with other options available upon request? Can you provide a copy of the current statement as well as the requirements for the content?

Response:

We do not believe emailing the Statement would be acceptable because it would contain secure member information. The exact percentage of emails on file is unknown. However, approximately 85% of new hires have an email address on file. The last statement produced was included in Appendix D.

43. Normal retirement age: What is the Normal Retirement Age for Pension Plan and Investment Plan members?

Response:

Pension Plan Normal Retirement

| Special Risk Class | All Other Membership Classes |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><u>Hired after July 1, 2011</u></p> <p>Age 55 or older and eight or more years of FRS-covered service</p> <p>Age 52 or older and 25 or more years of Special Risk and military service</p> <p>Any age and 25 or more years of Special Risk service</p> <p><u>Hired prior to July 1, 2011</u></p> <p>Age 55 or older and six or more years of FRS-covered service</p> <p>Age 52 or older and 25 or more years of Special Risk and military service</p> <p>Any age and 25 or more years of Special Risk service</p> | <p><u>Hired after July 1, 2011</u></p> <p>Age 65 or older and eight or more years of FRS-covered service</p> <p>Any age and 33 or more years of FRS-covered service</p> <p><u>Hired prior to July 1, 2011</u></p> <p>Age 62 or older and six or more years of FRS-covered service</p> <p>Any age and 30 or more years of FRS-covered service</p> |

Investment Plan Normal Retirement

| Special Risk Class | All Other Membership Classes |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Age 55 or older and one or more years of FRS-covered service</p> <p>Age 52 or older and 25 or more years of Special Risk and military service</p> <p>Any age and 25 or more years of Special Risk service</p> | <p><u>Hired after July 1, 2011</u></p> <p>Age 65 or older and one or more years of FRS-covered service</p> <p>Any age and 33 or more years of FRS-covered service</p> <p><u>Hired prior to July 1, 2011</u></p> <p>Age 62 or older and one or more years of FRS-covered service</p> <p>Any age and 30 or more years of FRS-covered service</p> |

44. Are the MyFRS.com Visits listed in the ITN unique visits? For instance, Personal Online Advisor Service users are listed as 73,272 for the period May 2022-April 2023. Are those unique users? Or do some users use the Service multiple times during the same period (i.e., Jane Smith used the service three times, so she counts as three users or one user)? Do you get requests for additional forms or help

and/or guidance? Are you interested in making available additional services to help participants manage their financial picture, in plan, out of plan, or both?

Response:

Total logins for this period were 73,272 (not unique logins). Users do use the service multiple times.

We occasionally get requests for specifics on how the tool operates and those are responded to by EY with input from the service provider. We are open to reviewing any additional services that may help members manage their financial future.

45. EY is listed as “appropriately credentialed.” What are the qualifications (licenses or certifications held) by EY? Does EY serve as a fiduciary for the services they provide? Does EY “screen share” when providing asset guidance (i.e., are the member and EY representative able to see the same screens)? Please list specific services that EY performs on the member’s behalf.

Response:

All EY planners have a minimum of an advanced educational degree and/or a professional designation such as a CPA, CFP, etc. In addition, all planners have received training on the FRS Investment Plan and FRS Pension Plan.

EY planners and workshop presenters are fiduciaries under Federal securities law and need to act in the best interests of their clients. But they are not fiduciaries under the Department of Labor’s (“DOL”) Fiduciary Rule and provide only education, and not advice, as defined by the DOL.

EY does not “screen share” when providing asset guidance services for members.

EY provides the following services for FRS members:

- *Telephone counseling through the MyFRS Financial Guidance Line (both Pension Plan and Investment Plan members), including:*
 - *New hire counseling (choice between Pension Plan and Investment Plan)*
 - *2nd election counseling (should a member switch retirement plans)*
 - *Financial counseling (debt management, taxes, retirement planning)*
 - *Assistance with MyFRS.com*
- *Employee workshops held throughout the state for both Pension Plan and Investment Plan members.*

46. Does EY provide any services for members who have separated from service or retired? (I.e., financial plans, separation of service guidance, etc.)

Response:

Pension Plan retirees who have retired or terminated are provided general information on the FRS.

Investment Plan retirees with a balance remaining in the FRS are provided individual retirement planning information.

47. Is there a link to a demonstration site to determine what they experience is for FRS members?

Response:

Not available.

48. Does Guided Choice or EY currently provide any guidance around the decumulation/draw down period for retiring members? What level of support does each provide members when they request/require guaranteed income?

Response:

GuidedChoice provides a service that assists members in the spend down phase of retirement.

EY can provide members with a complete financial plan including estimates of income during retirement.

The SBA has a contract with MetLife to provide immediate and deferred annuities to Investment Plan members. Members can run an online quoting tool or have EY run it for them.

49. What type of plan reporting do you get today? What are your reporting requirements?


Response:

Monthly usage, uptime, and data aggregation usage are provided monthly with the monthly invoice. Annually, a summary of the prior year's activity is provided.

Our reporting requirements going forward anticipate continuing to receive monthly and annual reports.

20-404 Remote Access



| | | |
|---------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Previous Revision: First Issued: | October 5, 2020 February 1, 2005 | <div style="text-align: center;"> Sampson Nancy May 24 2022 10:58 AM DocuSign </div> <div style="display: flex; justify-content: space-between; align-items: flex-end;"> <div style="text-align: center;"> Nancy Sampson Acting Senior Operating Officer </div> <div style="text-align: center;">  Lamar Taylor Interim Executive Director & CIO </div> </div> <div style="text-align: right; margin-top: 10px;"> <u>5-24-22</u> Date </div> |
| 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 | <p>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.</p> <p>SBA also supports remote access via Citrix connections using either SBA managed devices or non-SBA managed devices for the following scenarios:</p> <ul style="list-style-type: none"> • 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 <p>VPN connections are not allowed from devices that are not owned and managed by the SBA.</p> <p>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.</p> | |
| 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 | <p>Employee – All SBA, Florida Prepaid and Division of Bond Finance employees, including OPS and Interns.</p> <p>Users – All SBA employees, including OPS and Interns, and approved third parties that use SBA IT resource(s).</p> <p>Approved third parties – Non-SBA employees that have a contractual or regulatory relationship with the SBA, such as vendors, state auditors, etc.</p> <p>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.</p> <p>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.</p> <p>Third-Party Sponsor – The SBA, Florida Prepaid or Division of Bond Finance employee overseeing a third party's contractual, regulatory or audit activities.</p> |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

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 breach 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

X 
Lamar Taylor
Chief Operating/Financial Officer

X 
Nancy Sampson
Director of Information Technology

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.

10-409 Confidential/Sensitive Electronic Data Handling



Current Revision: April 13, 2018
Previous Revision: December 20, 2011
First Issued: February 1, 2005

X 
Ash Williams
Executive Director & CIO

| | |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Applies to | All State Board of Administration (SBA), Bond Finance, and Florida Prepaid employees, including OPS and Interns. |
| Purpose | To set forth the standards of processing confidential/sensitive electronic data and information, including guidance for the legal, appropriate, and reliable storage, accessing, handling, transmission, backup/recovery, and disposal of all confidential/sensitive data and information. |
| Policy | <p>Employees with access to restricted records or information will use such access only for legitimate and appropriate business purposes.</p> <p>Employees are prohibited from improperly accessing, using or divulging SBA information for personal gain, private advantage or meddlesome/impertinent/casual viewing.</p> <p>Based on the classification of electronic data and information, appropriate processing procedures and priorities will be applied.</p> |
| Governing Law | N/A |
| Related Policies | 10-040 Ethics 10-043 Confidentiality 20-407 Backup and Replication 20-412 Acceptable Encryption |

Guidelines/Implementation

Electronic Data Classification

The following two distinctions in data may affect how data and information is processed:

1. Confidential/Sensitive Data: Electronic data or information that is considered confidential by law under the Florida Public Records Act, or other statutes or by agreement. Some examples of this type of data are:
 - security procedures
 - data and information technology threat risk and analysis information
 - certain specifically delineated investment records and strategies
 - internal audits of information security resource programs
 - licensed products
 - select agency personnel information
 - personal identifying information
 - certain personal or family health or medical protected information

If issues exist as to whether certain data/information is classified in this category, supervisors are required to ask the General Counsel's Office for a determination.

2. Standard Data: Electronic data or information that does not require special access, handling, transmission, or disposal, as may be the case with confidential/sensitive electronic data.

The classification of electronic data as confidential or sensitive is the responsibility of the data owner, typically a business unit manager or higher.

Guidelines

- Confidential/sensitive electronic data will be accessible only to personnel who are authorized by the data owner or the Director of Information Technology (DIT) on the basis of strict "need to know" in the performance of their duties.
- Confidential/sensitive electronic data will be physically and/or electronically secured in such a manner to prevent unauthorized access.
- When confidential/sensitive electronic data is received from a third person (including another agency), confidentiality of the information will be maintained in accordance with conditions imposed by this policy.
- Magnetic media and hard copy documents that contain confidential/sensitive electronic data will be disposed of in accordance with IT procedures that are designed to ensure that such information has been destroyed and cannot be recovered.
- Owners of confidential/sensitive electronic data must review such data against established retention schedules. Owners will authorize the deletion or destruction of any such data determined to be past its retention schedule.
- Audit trails will be maintained to provide accountability for access to confidential/sensitive data and information, all transfer of and changes to records which control movement of funds or fixed assets, and all changes to security or access rules.
- Violations of access controls will be documented and reported to the Network Services Manager and the data owner.
- Removable storage devices containing electronic data and information must be clearly labeled to indicate their contents.
- All data being 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.
- All e-mail messages being sent outside the organization by SBA personnel will automatically carry an official disclaimer. An example of such is shown below:

"This communication may contain confidential, proprietary, and/or privileged information. It is intended solely for the use of the addressee. If you are not the intended recipient, you are strictly prohibited from disclosing, copying, distributing or using any of this information. If you received this communication in error, please contact the sender immediately and destroy the material in its entirety, whether electronic or hard copy."

Additionally, please note that Florida has a very broad public records law. This communication (including your email address, any attachments and other email contents) may be subject to disclosure to the public and media."

- All data will be backed up according to Policy 20-407, Backups and Replication.
- Test environments will be kept either physically or virtually separate from production environments. Copies of production information will not be used for testing unless all personnel involved in testing are authorized to access the information.

Compliance

All SBA, Bond Finance, and Florida Prepaid employees are responsible for compliance with this Policy. Employees are urged to seek guidance if any uncertainty exists with respect to confidentiality issues. Any person who believes this policy to be ambiguous in a particular situation is responsible for requesting a determination from the General Counsel.

The DIT is responsible for compliance with standards of processing confidential/sensitive electronic data and information as set forth in this policy. The DIT may develop additional procedures to implement this policy and will maintain sufficient documentation to demonstrate compliance with such standards.