10-409 Confidential/Sensitive Electronic Data Handling

Previous Revision:	April 13, 2018
First Issued:	February 1, 2005

Effective Date: July 11, 2024

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	Employees with access to restricted records or information will use such access only for legitimate and appropriate business purposes. Employees are prohibited from improperly accessing, using or divulging SBA information for personal gain, private advantage or meddlesome/impertinent/ casual viewing. Based on the classification of electronic data and information, appropriate processing procedures and priorities will be applied.
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 Senior Information Technology Officer (SITO) 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, CD/DVD 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 Director of Network Services 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

The Senior Information Technology Officer is the primary owner of this policy. 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 & Chief Ethics Officer.

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