AHFC Information Security Policy and Procedure

Febuary 2021

Information Systems

4300 Boniface Parkway • Anchorage, Alaska 99504 • P.O. Box 101020 • Anchorage, Alaska 99510
907-338-6100 (Anchorage) or (Toll-Free) 1-800-478-AHFC (2432) • www.ahfc.us

AHFC Information Security Policy & Procedures

CONTENTS

SECTION 1 – PURPOSE

As an independent state agency, Alaska Housing Finance Corporation employees and its agents produce, collect, and use many different types of data. AHFC's data assets are highly valuable. Laws, industry standards and institutional procedures have varying requirements obligating the privacy and protection of these assets. Establishing common standards for the classification and handling of data reduces risks to the AHFC, its stakeholders, and the public.

This policy is intended to guide AHFC employees in the classification of data for the purposes of defining its need for protection and determine applicable handling.

DRIVERS

Many factors govern the need for data loss prevention standards, policies, and procedures. Most importantly, they protect AHFC, its customers and business partners from harm.

- Regulatory

AHFC operationally strives to meet or exceed the best practices outlined within the standards listed below. By doing so, AHFC is well prepared to match the needs its business partners and customers, and is positioned to address prescribed regulatory requirements when required.

- Alaska Law: Personally Identifiable Information Security (HB 65, July 1, 2009)
- HUD: Notice PIH-2014-10, Privacy Protection Guidance for Third Parties o Payment Card Industry Data Security Standard (PCI_DSS) o HIPPA, FISMA, FERPA (HR), SOX, etc.

- Insurance requirements, claims and premiums (e.g. cyber insurance)
- Preparedness for industry certification on matters of data handling and information security assurance such as a SOC 2 Type II
- Costs of security incident, negligence or inaction: legal or civil liability
- Reputational harm to the corporation
- Contractual agreements such as structured within a non-disclosure agreement

SECTION 2 – SCOPE

This policy and the following procedures apply to all AHFC employees and Departments.

SECTION 3 – DEFINITION

PERSONALLY - IDENTIFIABLE INFORMATION (PII)

Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other PII which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

Information that can be considered PII when combined with other information include, but are not limited to, the following:

- An individual's name, meaning a combination of:
  - First name or first initial, and
  - Last name; and
  - One or more of the following information elements:
    - Individual's social security number
    - Driver's license number or state identification card number
    - Passport number
    - Account number, credit card number, or debit card number
    - Password, personal identification numbers, or other access codes for financial accounts

This definition can be used to classify any data that are stored, processed, transmitted or received by AHFC. The definition applies to all types of data:

- Electronic data
- Data recorded on physical media, including paper

- Information shared orally, visually or by other means

SECTION 4 – AHFC RESPONSIBILITY

AHFC POLICY

AHFC will limit the collection of PII when possible. When it is collected, PII must be relevant to the purposes for which they are to be used and to the extent necessary for those purposes.

AHFC follows industry standards and best practices in the treatment of PII:

- Do not collect information that is not needed, that is not included in the governing request or that is outside of any contract or agreement covering the collection, storage or transmission of the information.
- Personal data should not be disclosed, made available or otherwise used for purposes other than those specified, except with the consent of the data subject or by the authority of law.

AHFC PROCEDURES AND CONTROLS

Department management will ensure AHFC staff are trained to implement the procedures, controls and systems set forth in this policy. Training will take place when a new employee is hired and thereafter on at least an annual basis while the individual is employed by AHFC. This policy/procedure applies to all AHFC departments.

Reviews by Department management and Internal Audit will include computer security compliance as well as physical security at the AHFC offices and facilities.

The Department Director, with guidance from the Executive Director/Designee will monitor, and evaluate as appropriate, this Information Security Policy. At least annually, and more frequently as appropriate, the Department Director will report to the Executive Director/Designee their compliance with this policy.

The following systems, controls and or procedures designed to manage and mitigate risks to the integrity of PII are found to be appropriate and are adhered to by AHFC:

- Access is restricted, controlled and monitored in any area where PII is physically or electronically stored.
- Locked security shred containers are located throughout the office. All PII documents must be placed in these containers after work related to the documents is completed; use of unsecured trash bins for disposal of documents that include PII is not permitted.
- All computer access is controlled by systems using AAA (Authentication, Authorization, and Accounting) in accordance with AHFC login and password policies.
- Software applications containing PII are password protected in accordance with AHFC password policy.
- Access to software applications containing PII is provided to authorized personnel as determined by job function and authorization by management.
- All computers are subject to a 20-minute inactivity lock out.
- Unauthorized attempts to access AHFC's network and computing resources are currently logged and reviewed by I.S. Department staff.
- Segregation of duties and dual control procedures are employed where practical.

- System utilizing encryption and other security mechanisms are provided for use when transmitting PII to and from authorized recipients.
- Corporate file servers should only contain PII if necessary as part of an approved business process. The location of files containing PII must be access controlled and limited to staff that require access as part of their job duties.
- Corporate data is protected from loss by maintaining mirroring datasets to alternate location as described in the I.S. business continuity plan.
- Due diligence is exercised in the selection of service providers that deal with AHFC data. Vendors are selected based on their ability to protect AHFC's data based on adhering to industry standards and best practices.

DEPARTMENT RESPONSIBILITY

It is the responsibility of each Department Director to ensure enforcement with the policies above.

SECTION 5 - EMPLOYEE RESPONSIBILITY

AHFC will provide the following information and guidance for all employees with regard to PII security. Employees are expected to take steps to maintain security, confidentiality and integrity of AHFC's data.

Basic protection of PII include the following:

- All physical PII will remain in AHFC's offices.
- Locking rooms and file cabinets where physical records containing potential personal information is kept.
- Using strong complex passwords in accordance with AHFC password policy.
- Passwords must never be written down and left in a location easily accessible or visible to others. This includes the storing of passwords on non-AHFC systems or devices.
- Do not share passwords or accounts with anyone.
- Referring all calls or other requests for PII to designated individuals who have had safeguards training.
- Not revealing or disclosing conversations overheard regarding confidential or sensitive information.
- Reporting any security incident, including fraudulent attempts to obtain personal information, to the Information Systems director.
- Access to PII will be limited to employees who have a business reason for accessing the information and access to PII will be granted to employees who respond to PII inquiries but only to the extent they need it to do their jobs.
- All physical PII destined for disposal must be placed in the authorized and provided locked security shred containers located through AHFC facilities.
- Electronic data containing PII must be deleted.
- Devices containing PII must be destroyed in accordance with I.S. Data Destruction Policy. This includes but is not limited to USB drives, hard drives, DVDs, CDs or any other data storage media and can be turned into the IT Department for proper disposal.

GOOD PRACTICES INVOLVING PERSONAL INFORMATION

Daily awareness of the importance of securing personal information can significantly reduce the possible exposure of that personal information. Good practices to accomplish this goal include but are not limited to:

- Reducing the volume of conversations involving PII or utilizing a conference room or office and closing the door.
- Locking your computer or logging off when leaving your workspace for short times and minimizing screens containing PII when other staff or visitors are present that should not be able to access the information. This may also include privacy screens in close working spaces to shield wandering eyes.
- Not utilizing the browsers username/password auto-saving features on non-AHFC devices.

CLEAN DESK POLICY

A Clean Desk Policy is an important tool to ensure that all sensitive/confidential materials are removed from an end user workspace and locked away when the items are not in use or when an employee leaves his/her workstation. It is one of the top strategies to utilize when trying to reduce the risk of security breaches in the workplace.

The purpose for this policy is to establish the minimum requirements for maintaining a "clean desk" – where sensitive/critical information about our employees, intellectual property, customers, clients, and vendors is secure in locked areas and out of sight.

Clean Desk refers to keeping printed information, as well as, the displaying of electronic information secure. Sensitive or confidential information should only be printed if required as part of an approved business process.

This Clean Desk Policy applies to all Alaska Housing Finance Corporation employees.

Employees are required to ensure that all sensitive/confidential information in hardcopy or electronic form is secured when they are away from their workstation for an extended period of time and at the end of the day.

- Computer must be locked when workspace is unoccupied.
- Computer must be logged off but powered on at the end of the workday.
- File cabinets containing all sensitive/confidential information must be kept closed and locked when not in use or when not attended.
- Keys and keycards used for access to sensitive/confidential information must not be left unattended.
- Passwords must not be written down or stored in the office.
- Printouts containing sensitive/confidential information should be immediately removed from the printer/fax.
- Upon disposal, all sensitive/confidential documents must be shredded in the official shredder bins or placed in the locked confidential disposal bins.
- Whiteboards containing sensitive/confidential information should be erased.
- Secure portable computing devices such as laptops, tablets and phone.
- Do not copy sensitive/confidential information to any mass storage device such as CD/DVD or USB drives.

Compliance Measurement - Compliance with this policy will be verified through various methods, including but not limited to, periodic walk-throughs, internal audits, feedback to the I.S. Director, and general employee supervision.

If you notice that any of your devices or documents are missing, notify the I.S. Director immediately. If you believe your workspace has been tampered with, notify Risk Management.

Non-Compliance - An employee found to have violated this policy may be subject to disciplinary action, up to and including dismissal.

SECTION 6 - DATA CLASSIFICATIONS AND PROTECTION STANDARDS

Data can be classified either in terms of the required level of protection (e.g. Sensitive Data) or requirement for availability (e.g. Critical Data). There are four data protection categories: public, internal, sensitive, and restricted. The following two tables outline these standards:

TABLE I. DATA PROTECTION CATEGORIES

Type	Characterization	Examples
Public Data	Data that can be disclosed without restriction and or authorization.	• Maps • Handouts • De-identified information • Etc.
Internal Data	Data may be subject to open records disclosure and is often considered confidential.	• Some email correspondence • Budgets • Address lists • Client lists • Etc.
Sensitive Data	Data with confidentiality concerns that are governed or guided by law, policy, or contractual obligation. Characteristics: • *Compliance Risk:* Protection of data is mandated by law or required by private contract. • *Reputation Risk:* Loss of confidentiality or integrity will cause significant damage to AHFC's reputation. • *Other Risks:* Loss of confidentiality that could cause harm to individuals such as AHFC customers, clients, personnel, and partners. Loss of confidentiality or integrity that would cause AHFC to incur significant costs in response. • *Treatment in Records Requests:* Sensitive information is typically redacted from open records disclosures.	• Information protected by non-disclosure agreements (NDAs) • Law enforcement and investigative records • Pending litigation records • Research information • Intellectual Property data • Critical infrastructure information (physical plant, IT systems, IT security plans)
Restricted Data	Restricted data requires privacy and specific security protections. Special authorization is required for use and collection. Data with confidentiality concerns that are governed or guided by law, policy, or contractual obligation. Characteristics: • *Senior Management Approval:* AHFC senior management or their designees must authorize all storing, processing, and transmitting of restricted information. • *Compliance Risk:* Protection of information is mandated by law or required by private contract. • *Reputation Risk:* Loss of confidentiality or integrity will cause significant damage to AHFC's reputation. • *Other Risks:* Loss of the confidentiality or integrity of the information that could cause harm to individuals and cause the Corporation to incur significant costs in response. • *Treatment in Records Requests:* Records with restricted information are typically not open for public inspection unless compelled by law.	• Personally Identifiable Information (PII) • Passwords • Credit card data • Financial accounts • Social Security Numbers (including partials, such as last four digits) • Health record related data • Information systems countermeasure • configuration information etc.

TABLE II. DATA PROTECTION STANDARDS

Refer to the table below for minimum standard protection requirements for each category of data when being used or handled in a specific context. Protection standards are not intended to supersede any regulatory or contractual requirements for handling data. Some classifications of data may have stricter requirements in addition to what is outlined below. In all cases, the storage and transmission of sensitive and restricted data classes should be limited to absolute required minimums as per business case.

	CONTEXT	PUBLIC DATA	INTERNAL DATA	SENSITIVE DATA	RESTRICTED DATA
1	Collection and Use	• No protection requirements	• No protection requirements	• Limited to identified use by management	• Limited to identified use by management • 'Limited Collection' practices apply
2	Granting Access or Sharing	• No protection Requirements	• Reasonable methods will be used to ensure data is shared with authorized individuals with a legitimate need to know.	• Access is limited to and specifically approved for access by authorized individuals with a legitimate need to know. • Granting by external third parties may require contractual agreements per AHFC management	• Access is limited and specifically approved for access by authorized individuals with a legitimate need to know. • Granting by external third parties MUST require contractual agreements per AHFC management • 'Use limitation' practices apply
3	Disclosure, Public Posting, etc.	• No Protection Requirements	• Reasonable methods will be used to ensure data is shared with authorized individuals with a legitimate need to know.	• Cannot be posted publicly. • Cannot be disclosed without consent.	• Not permitted unless required to by law.

	CONTEXT	PUBLIC DATA	INTERNAL DATA	SENSITIVE DATA	RESTRICTED DATA
5	Public Records Requests or Freedom of Information Act (FOIA)	• Data can be provided given the proper coordination with designated AHFC staff.	• Requesting entities must coordinate with designated AHFC staff.	• Access is limited and specifically approved by AHFC for requesting individuals. • Granting by external third parties may require contractual agreements per AHFC management. • Granting may involve legal counsel.	• Access is limited and specifically approved by AHFC for requesting individuals. • Granting by external third parties may require contractual agreements per AHFC management. • Granting may involve legal counsel
6	Exchanging with Third Parties, Service Providers, Cloud Services, etc.	• No protection requirements	• Reasonable methods will be used to ensure data is shared with authorized individuals with a legitimate need to know.	• Access is limited and specifically approved for access by authorized individuals with a legitimate need to know. • Granting by external third parties may require contractual agreements per AHFC management	• Access is limited and specifically approved for access by authorized individuals with a legitimate need to know. • Granting by external third parties MUST require contractual agreements per AHFC management
7	Storing or processing on a server	• Subject to the minimum protection requirements of AHFC's storage & computing environment	• Subject to the protection requirement of AHFC's storage & computing environment • Limited to authorized and authenticated users of a system.	• Subject to the protection requirement of AHFC's storage & computing environment • Limited to authorized and authenticated users of a system.	• Subject to the protection requirement of AHFC's storage & computing environment • Limited to authorized and authenticated users of a system. • Storage of Credit/Debit card data is not permitted. • Storage at rest may be encrypted.

	CONTEXT	PUBLIC DATA	INTERNAL DATA	SENSITIVE DATA	RESTRICTED DATA
8	Storing or processing on an AHFC mobile device	• Subject to the minimum protection requirements of AHFC's mobile computing devices	• Subject to the protection requirement of AHFC's storage & computing environment • Limited to authorized and authenticated users of a system	• Not permitted	• Not permitted
9	Storing or processing on an non-AHFC device	• No protection requirements	• Not recommended	• Not permitted	• Not permitted
10	Storing or processing on *removable* media device. (Thumb drive, hard drive, DVD, etc.)	• No protection requirements	• Not recommended	• Not permitted	• Not permitted
11	Networked transmission (Secure Sockets Layer, File Transfer Protocol, etc.)	• No protection requirements	• No protection requirements	• Data will be transmitted as an encrypted file format or over an encrypted protocol or connection.	• Data will be transmitted as an encrypted file format or over an encrypted protocol or connection.
12	Email, Instant Messaging, blogs, message boards, social media posting and other network message transmissions	• Subject to minimum protection requirements of AHFC's email, messaging and social media policies	• Reasonable methods will be used to ensure internal data is only included in messages to authorized individuals or individuals with a legitimate need to know.	• Not permitted	• Not permitted

	CONTEXT	PUBLIC DATA	INTERNAL DATA	SENSITIVE DATA	RESTRICTED DATA
13	Printing, Mailing, Fax, etc.	• No protection requirements	• Reasonable methods will be used to ensure internal data is only included in messages to authorized individuals or individuals with a legitimate need to know.	• Reasonable methods will be used to ensure internal data is only included in messages to authorized individuals or individuals with a legitimate need to know. • Physical access security where sensitive data are stored should will be limited by they use of controls (e. g. locks, doors, monitoring, etc.) sufficient to prevent unauthorized entry.	• Reasonable methods will be used to ensure internal data is only included in messages to authorized individuals or individuals with a legitimate need to know. • Physical access security where sensitive data are stored should will be limited by they use of controls (e. g. locks, doors, monitoring, etc.) sufficient to prevent unauthorized entry. • Data masking will be used when possible. • Printing of SSNs on mailed material is not permitted unless required by State or Federal agencies.
14	Disposal	• No protection requirements	• Physical media (e.g. paper, CD, tape, etc.) should be destroyed (shredded) or placed in a secure bin where contents are to ultimately be shredded/destroyed	• Data will be deleted and unrecoverable (e.g. eraser, zero-fill, DoD multipass, etc.) • Physical media (e.g. paper, CD, tape, etc.) should be destroyed so that data in the media cannot be recovered of reconstructed.	• Data will be deleted and unrecoverable (e.g. eraser, zero-fill, DoD multipass, etc.) • Physical media (e.g. paper, CD, tape, etc.) should be destroyed so that data in the media cannot be recovered of reconstructed.

Information Security Policy & Procedures

February 2021

I specifically agree to read and comply with the Information Security Policy & Procedures of the Alaska Housing Finance Corporation.

This policy must be read in conjunction with all related policies and procedures of AHFC. By signing below, I acknowledge I have read and understand my responsibilities regarding Personal Identifiable Information.

Employee Signature

Date

Print Employee Name

Ref: AHFC Information Security Policy and Procedure