NEVADA
HOMEOWNER
ASSISTANCE FUND

NEVADA AFFORDABLE HOUSING ASSISTANCE CORPORATION

Information Security and Safeguards Program

Version 5.0

TABLE OF CONTENTS

TABLE OF CONTENTS

INTRODUCTION

Background

The State of Nevada received $120 million from U.S. Treasury's Homeowner Assistance Fund, established by the American Rescue Plan Act of 2021, to provide relief to homeowners who suffered a financial hardship due to the coronavirus pandemic.

The Nevada Affordable Housing Assistance Corporation (NAHAC) administers the Homeowner Assistance Fund program by offering the following types of assistance to eligible homeowners:

- Unemployment Mortgage Assistance to unemployed homeowners that need help with their monthly mortgage payments.
- Mortgage Reinstatement to catch up on delinquent payments or payments currently in forbearance.

Previously, NAHAC was the "Eligible Entity" pursuant to the HFA Participation Agreement entered into by the United States Department of Treasury ("Treasury"), the Nevada Housing Division (NHD) and NAHAC for the purpose of providing foreclosure prevention services, implementing the Hardest Hit Funds Program® ("Hardest Hit Fund") in the State of Nevada.

The purpose of the Hardest Hit Fund was to prevent and mitigate residential foreclosures and stabilize the housing market by assisting homeowners through several mortgage assistance programs designed to accomplish its goals.

In addition to the above-mentioned retention programs, NHD and NAHAC also administered a Down Payment Assistance (DPA) Program which provided qualifying Nevada home buyers with funds which can be used toward their down payment and closing costs on a home purchase.

This manual sets forth the policies and procedures that apply to all NAHAC full and part-time employees, temporary employees, management, contractors and sub-contractors ("Employees") as said policies and procedures apply to information security of all NAHAC Program data. In addition, this document applies to vendors, suppliers, affiliates, business partners, nonaffiliated third parties and any other parties who have access to NAHAC's data in order to protect information, as defined hereinafter in all its forms including digital, written, spoken, recorded electronically or printed, from accidental or intentional unauthorized modification, destruction or disclosure throughout its life cycle.

Purpose

NAHAC recognizes the importance and fundamental obligation to keep corporate and client communications and information confidential and has adopted safeguards as detailed herein to keep confidential information from unauthorized access and acquisition. This protection includes an appropriate level of security over the facilities, equipment and software used to process, store, and transmit that information.

The Information Security and Safeguards Program ("ISSP") is intended to provide a framework for the

security of corporate information assets by making confidential information available to authorized individuals as necessary for work purposes and protecting confidential information from unauthorized disclosure, alteration, misuse, and destruction. The ISSP uses a risk-based approach to accomplish these objectives. This means information assets are:

- Identified, Classified, and Labeled
- Protected
- Managed
- Appropriately Accessed and Used
- Monitored for Vulnerabilities
- Properly Utilized through User Education

Information Security Policies

The processes above are embodied in the Policies listed below, which form the framework for the ISSP risk-based program.

- Information Classification and Labeling
- Asset Protection
- Network Security
- Asset Management
- Acceptable Use
- Vulnerabilities Assessment and Management
- Threat Assessment and Management
- Security Awareness and Education

Document Scope

This document applies to all NAHAC full and part-time employees, temporary employees, management, contractors and sub-contractors ("Employees"). In addition, this document applies to vendors, suppliers, affiliates, business partners, nonaffiliated third parties and any other parties who have access to NAHAC's data.

Program Hierarchy

The ISSP is organized as follows:

Policies – Provide the broad, high-level security principles that form the risk-based asset protection framework that anchors and maps the supporting Standards.

Standards – Define the minimum acceptable requirements needed to comply with each of the Policies.

Procedures – Provide step-by-step directions on how to implement a Standard or Technical Standard. A Subject Matter Expert (SME) usually writes, or causes to be written, and maintains procedures.

Information Security Standards

Each of the eight Policies is put into practice through a set of Standards representing NAHAC-wide minimum requirements for complying with each Policy. This document presents this set of Standards and is the official reference for them. Failure to meet the minimum requirements outlined in the Standards is non-compliance with ISSP and requires resolution. (See Risk Acceptance Process under Policy and Standards Management.)

Policies and Standards Management

A joint Executive Team comprised of representatives from NAHAC Information Technology, NAHAC Compliance, and NAHAC Management are responsible for:

- Developing Information Security Policies
- Developing Information Security Standards
- Interpreting Policies and Standards
- Reviewing and Updating Policies and Standards not less than annually

NAHAC IT management and NAHAC Compliance are responsible for administering this program. For any questions about this document, or to report misuse of NAHAC data, persons should contact NAHAC IT management at [redacted] or via email at [redacted].

Risk Acceptance Process

When a system, application, or process does not comply with ISSP Standards for any reason, that system, application, or process is out of compliance and requires the Risk Acceptance Process for resolution. This process allows for agreement to be reached on a plan for achieving compliance or acceptable mitigating controls. The risk acceptance process is also used when additional risk factors are present that are not directly related to compliance with ISSP Policies, Standards, or Technical Standards. If appropriate, they will be integrated into the Policies, Standards, and/or Technical Standards.

How to Use These Standards

The Standards covered in this document are grouped under their associated Policies. The applicable policy is stated for reference at the beginning of each section.

Responsibilities, Compliance and Enforcement

All Standards in this document define Minimum Acceptable Requirements. Any system, process, application (including products and services acquired from vendors), and/or users not meeting these Standards, regardless of reason, is out of compliance. The Standards do not prevent systems and/or users from exceeding these minimum requirements. The Standards apply to all employees, contractors, part time and temporary workers, and those employed by others to perform work on NAHAC premises or who have been granted access to NAHAC information or systems.

Any entity or individual, who is not able to comply with the defined Standards and believes a process and/or action should be allowed to continue, must contact NAHAC IT Management and follow the Risk Acceptance Process.

Persons or entities not complying with these Standards and Policies may be subject to civil and criminal penalties. Employees found to be in violation of these Standards and Policies may also be subject to disciplinary action, up to and including termination, in accordance with NAHAC policies. All employees are responsible for adhering to these Standards and Policies and reporting to management any activities that do not comply with these requirements.

NAHAC Management is responsible for ensuring that employees understand the scope and implications of these Standards Policies. NAHAC IT Management will be responsible for monitoring data for unauthorized activity and is responsible for updating access requirements as needed.
Any system, process, application (including products and services acquired from vendors) and/or users having access to NAHAC systems, processes and/or applications prior to the date of publication of the ISSP must be brought into compliance with the ISSP as soon as is reasonably possible.

Assumptions

The following assumptions apply to the Information Security Standards contained herein, unless specifically stated otherwise:

Internal Consistency – All Standards are consistent and compliant with each other and compliant with Information Security Policies.

Technical Standards – All Technical Standards comply with applicable Standards and the Policies.

Compliance Exemption – Compliance with these Standards does not preclude compliance with or exemption from any other applicable policies, standards, technical standards, procedures, legislative, legal, and/or regulatory requirements.

Exceeding Standards – A unit (platform, application, process, and system) may set internal requirements above the minimum requirements.

Conflict Priority – If any of these Standards conflict with an applicable legal or regulatory requirement, then the legal or regulatory requirement takes precedent. If these Standards conflict with another standard, technical standard, procedure and/or process, the highest security posture or requirements takes precedent, as determined by ISSP through the Risk Acceptance Process.

IS Policies and Standards Relationship

The Standards are arranged under their relevant Policies, as described in the chart below.

Policy	Standards	Explanations
Data Classification & Labeling	Classification	The classification of information to establish its risk level—High, Medium, or Low based on "sensitivity", "criticality", and "integrity"
	Labeling	The process for labeling data in this classification system
Information Asset Protection	Access Control	Standards for access control technologies—access rights, passwords, tokens, digital certificates, etc.
	Remote Access	Standards governing the use of remote access channels into NAHAC Network
	Encryption	Standards governing encryption
	BYOD	Standards covering Bring Your Own Device information security
	Physical Access	Standards covering physical and facilities security directly affecting information security
	Availability Protection	Standards for disaster recovery, technology recovery, and business continuity
	Integrity Protection	Standards governing the control measures taken to protect the integrity level of low, medium, or high risk data
	Endpoint Protection	Standards governing the required use of Endpoint protection
	Information Handling	Standards on the physical management and destruction of information media, including: paper, magnetic media, etc.
	Audit/Logging	Standards for the keeping of logs sufficient to reconstruct, review, and examine events and activities leading up to an event
	Network	Standards for network and communications hardware, software, and related resources, including services and operations
Network Security	Network Requirements	Standards for network isolation, communications, and security
	Extranets	Standards for communication with NAHAC business partners
	Internet	Methods for the scanning of inbound internet communications
	Wireless	Standards for wireless data encryption
	Service Organization Networks	SOC Report submittals by Service Organization having Systems that are utilized to store or process NAHAC data

Table 1a

Policy	Standards	Explanations
Information Asset Management	Life Cycle Management	Standards for tracking all the phases of a project
	Configuration Management	Standards dealing with the tracking and control of project development
	Change Management	Standards concerned with the process of making a modification or deviation that affects the normal operating state in both operating and test environments
	System Development Life Cycle	Standards to provide for the implementation of appropriate security controls within system development life cycles
		Standards to provide for the implementation of appropriate security controls within system development life cycles
Acceptable Use	Internet Use	Standards governing Internet usage
	Intranet Use	Standards governing using NAHAC internal network
	E-mail	Standards for employee use of e-mail and instant messaging
	Mobile Device Security	Standards for employee use of mobile and Bring Your Own Devices
	Telecommunications	Standards for appropriate use of equipment such as modems, laptops, personally owned PCs, and mobile devices
	Incident Reporting	Standards for reporting misuse or potential misuse
Vulnerability Assessment & Management	Vulnerability Assessment	Standards for determining if NAHAC systems are secure at network, operating system, and application levels
	Vulnerability Management	Standards covering setting priorities on known vulnerabilities, mitigating risks, and tracking projects
Threat Assessment and Protection	Threat Assessment	Standards for monitoring, assessing, and setting priorities on information security threats
	Threat Management	Standards for intrusion detection and monitoring
	Incident Response	Standards governing problem notification, containment, and recovery services
Education & Awareness	New Hire Education/Awareness	Standards applicable to educating new hires on ISSP
	Ongoing Education/Awareness	Standards on keeping employees aware of ISSP Policies and Standards

Table 1b

Information Security Standards

Standards are grouped under the associated Policy. Each section first states the Policy for reference, then lists Standards supporting that Policy.

Note: All Standards in this document define ***MINIMUM ACCEPTABLE REQUIREMENTS***. Any system, process, application (including products and services acquired from vendors) and/or users not meeting these Standards, regardless of reason, is out of compliance. The Standards apply to all employees, contractors, part-time and temporary workers, and those employed by others to perform work on NAHAC premises or who have been granted access to NAHAC information or systems. Business and system owners may choose to go beyond these minimum Standards at their discretion.

1. Information Classification and Labeling

Policy: NAHAC defines, identifies, classifies, and labels information assets based on criticality, sensitivity, and integrity. All sensitive or confidential NAHAC generated and/or managed data must be so labeled.

1.1. Definition of information to safeguard

Confidential information shall mean any information, including, but not limited to, trade secrets, business processes, business plans, client files, client information, client documentation, data of any kind, pictures, customer lists, financial statements, financial data, proprietary business information, research or development projects or results, test, and/or any non-public information which concerns the business, clients, operations, ideas or plans conveyed by any format or means including, but not limited to, written, typed, facsimile, email, or orally transmitted.

1.2. Information Classification

All NAHAC information must be classified by Data Sensitivity levels as specified below. These Data Sensitivity levels are as follows:

NAHAC-Owned Data - that relates to such areas as NAHAC financials, employment records, and payroll.

Personally Identifiable Information (PII) – is any information that can be used to distinguish or trace an individual's identity, such as name, social security number, mother's maiden name, and any other information that is linked or linkable to an individual, such as medical, educational, financial and employment information.

This policy is intended to help employees determine what information can be disclosed to non-employees, as well as the relative sensitivity of information that should not be disclosed outside of NAHAC without proper authorization (See Table 2). The information covered in the sections below includes, but are not limited to, information that is either stored or shared via any means. This includes: electronic information, information on paper, and information shared orally or visually (such as telephone and video conferencing).

SSN	Address	Date of Birth	Employment Info	Medical Info
Drivers License	Home or Cell Phone Number	Homeowner ID	Education	Mother's Maiden Name
First and Last Name	Email Address	Account Numbers	Credit and/or Financial Info	Photographic Images

Table 2

All employees should familiarize themselves with the information labeling and handling guidelines as set forth below. It should be noted that the sensitivity level definitions were created as guidelines and to emphasize common sense steps that should be taken to protect NAHAC and its Clients.

1.2.1. Data Sensitivity

NAHAC information is categorized into three data sensitivity levels. All NAHAC information must be classified under one of the following data sensitivity levels:

1.2.1.1. Public: Information that is generally available to anyone within or outside of NAHAC. Access to this data is unrestricted, may already be available and can be distributed as needed. Public/unclassified data includes, but is not limited to, marketing materials, internet materials, public filings, etc.

1.2.1.2. Sensitive: Personal or NAHAC information that may be considered potentially damaging if released and is only accessible to specific groups. Sensitive data includes, but is not limited to, certain HR information, accounting data, policies and procedures, sales information, non-personally identifiable data about customers and employees.

1.2.1.3. Private: Personal or NAHAC information that is considered damaging if released and is only accessible to specific groups. Private data includes all customer and employee personally identifiable information (PII), trade secrets and marketing, operational, personnel, financial, source code, and technical information integral to the success of NAHAC.

1.2.2. Data Classification Rating Process

The above data classifications represent a continuum, in that it is understood that some information is more sensitive than other information and should be protected in a more secure manner. Information that should be protected very closely is as follows: PII, other client information, client lists, property information, development programs, and other information integral to the success of NAHAC and/or the security of NAHAC clients and employees. Information that is less critical, such as telephone directories, production reports and other general corporate information is still considered to be confidential but does not require as stringent a degree of protection.

1.2.2.1. Employees are encouraged to use common sense judgment and training instruction in securing confidential information to the proper extent. If an employee is uncertain of the sensitivity of a particular piece of information, the employee should contact their manager immediately for instructions.

1.3. Information Labeling

All NAHAC information must be labeled in a way that identifies its classification. This Standard pertains only to new data applications that have processes in place to handle such labeling. Unless otherwise specified, the information owner has the responsibility for information labeling.

1.3.1. The default label for any piece of information not otherwise labeled is: "Private." This label is implied when no other label is present. Any employee who authors or generates corporate or client data must classify that data according to the criteria outlined above.

1.3.1.1. When information of mixed classification is stored, transported, and/or processed together, the collective entity must be labeled with the highest classified individual information element.

1.4. Information Exchanged between Third Parties

Confidentiality of client information (PII) and NAHAC information is critical. NAHAC recognizes the importance of protecting the confidential information that it holds with respect to clients, employees and others.

NAHAC may utilize the services of third-party vendors during the course of a client related matter. Any and all information transmitted to any third-party vendor shall be done in the following manner:

1) All third-party vendors shall execute a confidentiality agreement prior to receiving any confidential information.

2) All third-party vendors shall adhere to the Information Security and Safeguards Program.

3) Any employee who communicates with a third-party vendor shall provide only such confidential information as is necessary for the third party to carry out the agreed upon services, duties, and/or tasks.

4) All communications of any kind between employees and third parties shall be considered confidential communications and must be held in strict confidence.

5) Upon request third-part vendors shall return any and/or all NAHAC owned information in their possession. NAHAC information that remains in the possession of the third-party vendor shall be maintained in accordance with NAHAC document retention policies [redacted]

6) All questions relating to whether or not information should be provided to a third-party should be immediately referred to the NAHAC Compliance Manager or to the employee's manager.

1.5. Prohibited Distribution of Information

At no time shall any employee share any information of any kind with a third party that has not been approved by management. Such communication may require the execution of an approved confidentiality agreement.

2. Asset Protection

The Policy: NAHAC protects the confidentiality, integrity, and availability of all information assets under its care. Access controls (including remote access, remote control, cloud systems access and/or physical access) are granted on a "need-to-know" basis and are required for all protected Client and NAHAC confidential information.

2.1. Access Control

All non-public NAHAC systems require users to identify themselves and provide a means to authenticate their claimed identities appropriately for the risk level of the system and/or transaction.

2.1.1. Credential Authority: Access to Information

Only credentials (the means by which to be authenticated) obtained from approved sources and by approved processes will be accepted. Data access privileges, which will be updated as required when an employee joins or leaves NAHAC or whose duties are changed to a degree requiring modified access are initiated through the submission of a System Authorization Access Request (SAAR) by appropriate NAHAC Management. Additional accesses to information that is required as a result of increased work responsibilities can be initiated by appropriate NAHAC Management by emailing [redacted]

NAHAC Management shall determine which employees have access to sensitive and personal information. Upon hiring, an employee will be advised of their access to sensitive information and shall strictly and diligently follow Standards and Policies herein that relate to public, sensitive, or private information. Not all employees are entitled to or given access to all available information. NAHAC limits access to sensitive and/or confidential information to employees who need the information to carry out their duties and responsibilities. The limit of access to information shall be accomplished through locked cabinets and doors, passwords on computer workstations, systems passwords, file level permissions and prohibitions against leaving sensitive and personal information unattended.

2.1.2. Logon Standards

All logon procedures will adhere to the appropriate Standard(s) below.

2.1.2.1. Logon Banners. [redacted]

2.1.2.2. Session Time-outs. [redacted]

2.1.2.2.1. Standard Desktop Functions. [redacted]

2.1.2.2.2. Customer Servicing/Administrative Functions. [redacted]

2.1.2.2.3. System and/or Application Session Timeouts. [redacted]

2.1.2.2.4. Unattended Systems. [redacted]

2.1.2.2.5. Successive Logon Attempt Controls. [redacted]

2.1.3. Authorization

Authorization to access any NAHAC resource must meet the appropriate Standard(s) below.

2.1.3.1. All information assets must be assigned an owner responsible for authorizing access to that data or resource. Authorization for access to NAHAC information assets must be granted on a need-to-know basis at the appropriate responsibility level for the minimum amount of time necessary and not compromise segregation of duties (defined as no single person having responsibility for an entire process or operation).

2.1.4. All requests for system access must be submitted on the appropriate SAAR form and approved by the employee's manager. In the case of a file system, requests for access to the root folders should be included on the SAAR form.

2.1.4.1. User IDs and User Names. [redacted]

2.1.4.2. Proper Use. [redacted].

2.1.4.3. Account Deactivation. NAHAC network and computing control environments must have:

2.1.4.3.1. Terminated and/or Closed Accounts. [redacted]

2.1.4.4. Using Trusted IDs. IT must approve Trusted IDs for system administration purposes. The following Standards for using Trusted IDs must be followed:

2.1.4.4.1. To Supplement System Access. [redacted]

2.1.4.4.2. For Approved Purpose. [redacted]

2.1.4.4.3. For Production and Test Quality Assurance (QA). [redacted]

2.1.4.5. Default IDs must be disabled. [redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]

[redacted]

[redacted]

[redacted]

2.1.5. Access Credentials. [redacted]

2.1.5.1. Passwords. [redacted]

2.1.5.1.1. Baseline Controls. [redacted]

2.1.5.1.2. Baseline Password Syntax Controls Grid

Length [1]	Login Attempts Before Lockout	* History [2]	* Change frequency [3]	* Password Reuse Schedule [4]	Numeric or special character check
[redacted]					

Table 3

Note: Password change recommendations:

For systems that handle password history based on number of previous passwords, do not allow users to select a password selected in the past [redacted] password changes, and do not allow users to change passwords more than [redacted]. For systems that handle password history based on time, do not allow users to select a password previously selected within the past [redacted].

2.1.5.1.3. Clear Text. [redacted]

2.1.5.1.4. Password Encryption. [redacted]

2.1.5.1.5. Password Sharing. [redacted]

2.1.5.1.6. Password Resets. [redacted]

2.1.5.1.7. Password Privacy. [redacted]

2.1.5.1.8. Initial Passwords. [redacted]

2.1.5.1.9. Change of Initial or Reset Passwords. [redacted]

2.1.5.1.10. Password Screen Entry. [redacted]

2.1.5.1.11. **Paper.** [redacted]

2.2. Remote Access

All remote access users (i.e., employee, vendor, contractor, etc.) must adhere to the following Standards:

2.2.1. Authentication. All remote access to NAHAC systems/applications must include user authentication. Remote connections must use data encryption and be approved by IT.

2.2.2. Passwords. Secure remote access must be strictly controlled. Control will be enforced via [redacted]. Anonymous access is not allowed.

2.2.3. Email Accounts. NAHAC employees and contractors with remote access privileges to NAHAC corporate network must not use non-NAHAC email accounts (i.e., Hotmail, Yahoo, AOL), or other external resources to conduct NAHAC business, thereby ensuring that official business is never confused with personal business.

2.2.4. Antivirus/Endpoint Security. All hosts that connect to NAHAC's internal networks via remote access technologies must use the most up-to-date antivirus and/or endpoint security software.

2.2.5. Firewall. All hosts that are connected to NAHAC's internal network must use a software firewall on the host computer.

2.2.1. Individual Accounts. Remote access accounts must be assigned to individuals only and not shared.

2.2.2. Enrollment. Users shall be provided with direct access only to the services that they have been specifically authorized to use. Access to information shall be based on the need for the information, or the need to maintain and administer the information resource.

2.2.3. Third Parties. To obtain access to NAHAC networks, all third parties (i.e., contractors, vendors, business partners) must have contracts that include a confidentiality clause.

2.2.4. **Professionalism.** It is the responsibility of NAHAC employees, contractors, vendors and agents with remote access privileges to corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to NAHAC's network.

2.2.5. **Remote Control.** "Remote control" software allows a desktop and/or server to be accessed and controlled remotely by another user or system. All remote control software tools and their use in any particular setting must be approved by IT. The following specific Standard also apply:

2.2.5.1. **Internal System Use Only.** Remote control tools can be used only to offer desktop support to employees (including contractors, vendors, and/or consultants) using NAHAC desktop equipment and/or to maintain unattended NAHAC servers.

2.2.5.2. **User Permission Required.** Attended desktop devices and/or servers must be accessed by only authorized individuals and/or systems via remote control after the desktop owner grants real-time, online permission, in a manner appropriate to the remote-control tool and environment.

2.3. Encryption

All encryption technologies, products, and tools used in production environments for storing, transporting, and/or processing NAHAC information assets must be approved by IT prior to use.

2.3.1. [redacted]

2.3.2. [redacted]

2.4. Bring Your Own Device (BYOD)

"Bring Your Own Device" (BYOD) refers to organizations permitting their device owners to utilize personally owned mobile devices (e.g. tablets and smart phones) in and outside of their workplace, to access privileged organizational information and applications.

NAHAC management recognizes that device owners wish to use their own mobile devices to access NAHAC data and use NAHAC applications as part of flexible working arrangements. This policy outlines the responsibilities of both the device owner and NAHAC.

Section 2.4 of the ISSP provides standards and guidance for the acceptable use of personal devices, such as smart phones and tablets, by NAHAC device owners to access network resources.

[redacted] The use of a personally owned device in connection with NAHAC business is a privilege granted to device owners through approval of Information Technology management. NAHAC reserves the right to revoke these privileges in the event that device owners do not abide by the policies and procedures set forth in this document.

2.4.1. Who does this apply to? [redacted]

2.4.2. Device Coverage. Current devices approved for BYOD along with the minimum system requirements use are as follows:

- [redacted]

2.4.3. Approved Apps. [redacted]

- [redacted]

These are the only approved applications for BYOD.

2.4.4. Device Owner Responsibilities. Users that are authorized to participate in the BYOD program have the following specific responsibilities:

- [redacted]

[redacted]

- [redacted]

- [redacted]

- [redacted]

- [redacted]

- [redacted]

- [redacted]

- [redacted]

- [redacted]

- [redacted]

- [redacted]

- [redacted]

- [redacted]

- [redacted]

- [redacted]

[redacted]

2.5. Physical Access

The physical security of all communications, network, and related operational sites (any area housing communications and network equipment and/or operating/administering/monitoring such equipment) must meet NAHAC physical security requirements.

2.5.1. General Requirements

2.5.1.1. [redacted]

2.5.2. Hardware and Software Maintenance

2.5.2.1. Whenever computers or peripherals are relocated or removed from operation (e.g., maintenance, salvage, sold, or storage), the following standards must apply:

- All removable media must be removed.
- Internal drives must be overwritten, re-formatted, removed, or destroyed according to current industry best practices.
- All paper should be removed from printers.
- All data must be cleared. Clearing is the process of removing the data on media or devices before permitting access by personnel without the proper clearance, need-to-know or formal access approvals. All internal memory, buffer, or other reusable memory shall be cleared to effectively deny access to previously stored information using methods approved in corporate security policy.
- Media must be sanitized. Sanitization is the process of removing information from media or equipment such that data recovery using any known technique or analysis is prevented, as well as the removal of all confidential labels and markings. Normally sanitization is performed when the equipment is to be released for repair, upgrade, use by another user, or when no longer required for confidential processing.

2.5.3. Audit and Logging (See Standard *2.10 Auditing and Logging.*)

2.5.4. Input/Output Control. Procedures should be implemented to verify the secure storage or distribution of all outputs/reports, in accordance with procedures defined by the owners for each system.

2.5.4.1. Media Management (See Standard *2.8.1.2 Electronic Media)* Responsibilities for media library management and protection must be defined and assigned.

2.6. Availability Protection

NAHAC information assets must be available to authorized users when needed. All known threats to availability, including natural disasters, accidents, malicious destruction, failures, and denial of service, must be addressed. The following Standards specifically address availability protection.

2.6.1. Technology Recovery. NAHAC requires appropriate planning and testing processes to be in place to ensure that, in the event of significant business interruptions, production environments can be recovered and sustained to meet customer business requirements. To facilitate effective technology recovery, collaboration is required among trusted vendors, technology areas, and business departments.

The Standards described in this section apply to all production processing environments, whether operated across NAHAC or operated independently within a business unit. They include mainframe, midrange, cloud, and distributed environments whether managed internally by or managed by external service providers, and apply specifically to the following assets:

All platforms, including hardware, operating systems, supporting tools, and utilities.

Applications, including network infrastructure

2.6.1.1. Technology Recovery Planning The following technology recovery Standards must be met:

2.6.1.1.1. Technology recovery plans (IT/DR) must be developed prior to implementation as part of the development life cycle for technology development or deployment by the line of business to address all production processing environments and assets listed in Standard 2.6.1.

The line of business must review and update the plan(s) at least annually, or whenever a significant change impacts the plan(s) and/or a significant change affects the technology recovery strategy of the plan. All technology recovery plans require approval by IT annually. The technology recovery plan includes application, infrastructure, and site recovery components and should minimally cover the following:

- Application identification and description, including if applicable: Application ID, Application Name, Description of Application Functionality/Business Use.
- Contact information, including if applicable: Primary Application Support/Subject Matter Expert, DBA, Vendor Name/Contact information.
- Hardware configuration, including if applicable: Production Platform/Server Type, Production Server Location(s), Production System/Server Name, DR Platform/Server Type, DR Server Location(s), DR System/Server Name, Configuration Requirements.
- Software configuration and interfaces, including if

applicable: Programming Language, Critical Software/Tools/Utilities, Application Interdependencies/Interfaces and Type, External Service Providers.

- Network configuration, including if applicable: Protocols, External Connections, Backup processes, including if applicable: Backup Utility/Tools Used, Backup Schedule/Frequency/Retention, Offsite Rotation/Location, Retrieval Process, Critical File Listing, Area Responsible for Backup/Media Management.
- Recovery strategy & procedures, including if applicable: Recovery Strategy, Recovery Steps, Synchronization Steps with Interfacing Applications, External Service Providers.
- Batch processing information, including if applicable: Critical Batch Jobs/Schedules, Batch Scheduling Software/Tools, Critical Reports.
- Recovery objectives and capabilities, including if applicable: Recovery Time Objectives, Recovery Point Objectives, Last DR Exercise Date, Demonstrated Recovery Time and Point Capabilities from Past Test.

2.6.1.2. Disaster Recovery Testing. To protect the integrity of NAHAC's business continuity philosophy, routine, periodic testing of all technology recovery plans is required. Table 4 shows a list of possible testing types.

The Following Table Describes Possible Test Types	
Test Type	**Description**
Walk-Through	A participatory session featuring an oral walk-through of the technology recovery plan and of the specific tasks documented within the plan. This exercise should confirm the plan's design and identify role and responsibility gaps or other weaknesses in the plan. This type of exercise can be used for applications with RTOs of 2 or 1 every other year. On the alternate year, these applications must be included in a more robust test.
Stand-Alone	Tests one or more specific components of a technology recovery plan in isolation from other components. Focuses on data restoration with network connectivity and is usually limited to a single platform or system. It may or may not include testing application interdependencies.
Partial Integration	Tests one or more specific components of a technology recovery plan. Includes testing data restoration with network connectivity and testing some interdependencies with applications and/or platforms.
Full End-to-End	Where it is feasible in the Disaster Recovery testing environment without risk to the production environment, tests all components of the technology recovery plan and all functionality of an application. Includes testing transactions and testing all interdependencies with other applications and/or platforms.

Table 4

2.6.1.2.1. Disaster recovery exercises must be designed to measure the recovery readiness of hardware and of software and data backup processes, as well as to test the ability to execute related business processes.

2.6.1.2.2. Each line of business participating in a disaster recovery exercise must perform a verification of recovery activities.

2.6.1.2.3. Exercise participants must provide the documented exercise results (required for each test type) to IT for inclusion in management reports. Each area must track action items resulting from problems revealed during testing until the problems are resolved.

2.7. Integrity Protection

Information integrity refers to the necessity for an application's information to be protected from errors as well as deliberate, fraudulent manipulation or alteration. Management must establish and maintain controls to verify that NAHAC information is free from a significant risk of undetected alteration. The Standards below specifically address integrity protection controls. [redacted])

2.7.1. Segregation of Duties. Segregation of duties, close supervision, and/or other compensating controls must be established throughout NAHAC's infrastructure to limit the potential that a single person is responsible for an entire process or operation. User access to application and system specific features should be controlled by the appropriate access control groups and settings available in applications and systems.

2.7.2. Accuracy Assurance. Application, system, and process errors must be minimized through processes such as edit checks, hashes, electronic signatures, program testing, application controls, and change control processes. Accuracy and completeness are a corporate expectation of all employees.

2.7.3. Change Management. Networks, systems, applications, and processes that store, transport, and/or process NAHAC information assets must adhere to currently approved Change Management Policies and Standards.

2.8. Endpoint Security

Management must establish and maintain controls to verify that NAHAC information is being protected from viruses, malware, zero-day threats and other security risks. Comprehensive protection from these threats is required where appropriate and available on all:

- NAHAC owned and/or operated servers, cloud environments, desktops, or laptop workstations with Microsoft Windows operating systems.
- NAHAC owned and/or operated file servers in production, QA, or test environments and mail servers.
- Contractor owned systems that are authorized to access NAHAC internal and/or external managed systems
- All mobile devices that are NAHAC or user owned that will access NAHAC app data.

2.8.1. Required Scanning. NAHAC requires scanning by approved endpoint protection software and/or systems for the following:

2.8.1.1. Software. All new externally obtained software, whether downloaded or loaded via data storage media, prior to use, including purchased, freeware, and shareware.

2.8.1.2. Electronic Media. All externally supplied electronic media (i.e., Flash Drives, CD-ROM, tape, etc.)

2.8.1.3. Computer-readable Media. All externally supplied computer-readable media (i.e., software programs, databases, word processing documents, spreadsheets, etc.)

2.8.1.4. Distributed Software and Media. All software, electronic media, and computer-readable media prior to distribution to external or third parties.

2.8.2. Installation Responsibilities. The following applicable virus protection Standards must be met for all NAHAC system installations:

2.8.2.1. Designated IT personnel must include NAHAC approved endpoint protection software in system builds and/or Common Operating Environment (COE) images.

2.8.2.2. NAHAC IT is responsible for verifying that NAHAC approved endpoint protection software is installed and operational on all microcomputer systems and/or networks under their control.

2.8.2.3. IT administrators monitor endpoint protection for all information assets, including:

2.8.2.3.1. Monitoring internal and selected external sources for malware activity.

2.8.2.3.2. Issuing virus alerts and remedial actions (containment and eradication)

2.8.2.3.3. Utilizing virus response procedures during a virus alert and or breach.

2.8.2.3.4. Providing virus signature updates to IT administrators for immediate distribution.

2.8.3. Antivirus Guidelines.

2.8.3.1. Employees are never to open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Such attachments are to be deleted immediately, then "double deleted" by emptying the “Trash” file.

2.8.3.2. Spam, chain, and other junk email are to be deleted without opening or forwarding.

2.8.3.3. Files from unknown or suspicious sources are never to be downloaded.

2.8.3.4. The act of direct disk sharing with read/write access is prohibited unless there is a business requirement to do so. Such activity requires prior management approval

2.8.3.5. Storage media such as CDs, DVDs, Flash Drives and Memory Cards are to be scanned for viruses before use.

2.8.3.6. Anti-virus software is to be continually updated to ensure security levels are current.

2.8.3.7. Corporate standard software must include an automatic update mechanism to update new virus signatures to client [redacted].

2.9. Information Handling

All information transmitted, stored, and handled in any other way must meet data classification requirements and all applicable Standards contained in this section.

2.9.1. External Transport. All NAHAC confidential information must be encrypted when transported or forwarded outside of NAHAC network. This includes information that is transported manually via physical electronic media storage devices such as CDs, DVDs, Flash Drives and Memory Cards) or electronically and in any format (i.e., e-mail, e-mail attachment, file transfer). ([redacted].) Distribution of information outside of NAHAC shall be via U.S. mail and other public or private carriers or through approved encrypted electronic mail and secure electronic file transmission methods.

2.9.2. Off-site Storage of Backup Media. When backup media is stored off-site, contractual obligations must include a process for secure transport of the media, tracking of shipments, and verification of receipt.

2.9.3. Data Destruction. Information and equipment being removed or reassigned is to be destroyed in the following manner:

2.9.3.1. When NAHAC Confidential information is to be purposely destroyed, it must be carried out by qualified NAHAC personnel, or a certified service provider and be in compliance with current data destruction standards.

Media Type	Destruction Method(s)
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

Table 5

2.9.3.2. Whenever computers or peripherals are reassigned or removed from operation (i.e., transfer to different user/department, maintenance, salvage, sold, or storage), the following Standards apply:

2.9.3.2.1. All removable media must be removed and be overwritten, reformatted, or destroyed in compliance with current data destruction industry standards.

2.9.3.2.2. Internal drives must be overwritten, reformatted, removed, or destroyed in compliance with current data destruction industry standards.

2.9.3.2.3. If applicable, ribbons, toner cartridges, and paper should be removed from printers.

2.9.3.3. Erasing. Whether erasing storage media for internal reuse or resale, NAHAC requires adherence to the following Standards:

2.9.3.3.1. Generally accepted industry practices must be used when erasing any electronic storage media for internal reuse.

2.9.3.3.2. Resale or surrender of used storage media to third parties, even if sanitization standards are met, requires prior approval.

2.9.4. Transmitting. When transmitting public, sensitive, or private information, NAHAC requires the adherence to the following standards:

2.9.4.1. Email. Electronic mail is approved only via the electronic email account provided to each employee by NAHAC. This mail system is supported by designated IT personnel. Employees are prohibited from utilizing any other electronic mail system. Data that is allowed to be transmitted via NAHAC email accounts include:

2.9.4.1.1. **Public Data:** Allowed

2.9.4.1.2. **Sensitive Data:** May be allowed with management approval

2.9.4.1.3. **Private Data:** Prohibited

2.9.4.2. Encrypted Email. Encrypted electronic mail is approved only via the encrypted electronic email account provided to each employee by NAHAC. This mail system is supported by designated IT personnel. Employees are prohibited from utilizing any other encrypted electronic mail system. Data that is allowed to be transmitted via encrypted email includes:

2.9.4.2.1. **Public Data:** Not required

2.9.4.2.2. **Sensitive Data:** May be required, depending on management approval

2.9.4.2.3. **Private Data:** Required

2.9.4.3. Via Paper Fax. Faxing information is approved only via NAHAC owned fax machines. Employees are prohibited from utilizing any other fax machine without management approval.

2.9.4.3.1. Public Data: Approved

2.9.4.3.2. Sensitive Data: [redacted]

2.9.4.3.3. Private Data: [redacted]

2.9.4.4. Via eFax Software Application. Faxing information is approved only via NAHAC IT approved secure encrypted fax application. Employees are prohibited from utilizing any other fax application to send or receive fax data.

2.9.4.5. Electronic File Transfer (FTP): Employees may only utilize NAHAC IT approved FTP (not encrypted) and SFTP (encrypted) systems.

2.9.4.5.1. Public Data: Both FTP and SFTP transmissions technologies are approved.

2.9.4.5.2. Sensitive Data: SFTP is required, FTP is prohibited.

2.9.4.5.3. Private Data: SFTP is required, FTP is prohibited.

2.9.4.6. External Network Connections. Employees may only utilize NAHAC approved external network connections. All external network connections must utilize NAHAC approved encryption technologies.

2.9.4.7. Forwarding of E-mail. Automatically forwarding e-mail is prohibited. However, forwarding e-mail to administrative personnel working directly with managers on internal corporate e-mail systems is permitted.

2.9.4.8. Disposal of Printed Data. All papers, documents and hard copies of information no longer in use shall be disposed of in accordance with NAHAC information destruction standards.

2.9.4.9. Document Retention. Document retention shall be determined by applicable law, regulation and NAHAC policy. in the absence of clear mandates for document retention, the following shall apply:

Record Type	Retention Period
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

Table 6

2.10. Auditing and Logging

A tracking system must be maintained for management to reconstruct, review, and examine events and activities leading up to an event. It is recommended that all audit logs capture sufficient data to establish Who, What, When, and Where for each event logged.

2.10.1. Logging. Activity audit logs, including failed login attempts, and/or database backups must be maintained.

2.10.1.1. Non-Database. Activity audit logs must be kept on all production systems processing transactions and/or sensitive NAHAC confidential information like customer information, negotiations, quotes, internal business matters, personnel information, marketing strategies, etc.

2.10.1.2. Database. If certain database platforms use a daily back-up process in lieu of logs when log size would be prohibitive, then using back-ups instead of audit logs must be approved by IT.

2.10.1.3. Log Content. The following log content Standards must be met:

2.10.1.3.1. Minimum Content. Activity audit logs must record at least the minimum data fields and actions, including failed login attempts, as required by IT and/or the Technical Standards to trace activity for audit and/or adjustment purposes.

2.10.1.3.2. Production Systems. All production application systems that handle Sensitive NAHAC Confidential information must generate logs that show additions, modifications, and deletions to such sensitive information.

2.10.1.3.1. Prohibited Content. Logs must not include access credentials, such as PINs, passwords, etc.

2.10.2. Traceability. Traceability methods must be incorporated.

2.10.2.1. Non-trusted User IDs. Log entries must be traceable to an individual user.

2.10.2.2. Trusted User IDs. Trusted User IDs do not allow traceability to the individual level; therefore, they must be traceable to the Trusted User ID owner. Use of Trusted User IDs requires IT approval.

2.10.3. Log Retention. Log retention must be based on a stated retention schedule, compliant with regulatory requirements, and archived in a secure manner with appropriate back-up and access controls. Where possible, system audit logs should be stored on an alternate system.

2.10.3.1. System audit logs must have adequate access controls (e.g., file protection) to protect against unauthorized modification or deletion.

2.10.3.2. Any removable media containing audit logs must be stored off-site in a secure, protected location.

2.10.4. Systematic Review. Designated IT personnel must periodically review logs.

3. Network Security

The Policy: All networks must comply with applicable NAHAC network security requirements. Network and communication security involve the management of network and communication hardware, software, and related resources including services and operations. The requirements in this section cover all NAHAC networks. When requirements apply to only a subset of network types identified in the previous sentence, those distinctions are noted.

Definitions. A network is an arrangement of nodes and the equipment connecting these nodes. The following categories of network connections are supported by these Standards:

Internet Connections - Network connections that provide access to or from the Internet; a TCP/IP-based global network of public and private organizations, generally provisioned by specialized telecommunications carriers known as Internet Service Providers (ISPs).

Extranet Connections - Network connections that provide non-public, controlled third-party access to NAHAC systems.

For purposes of these Standards, a host is any network-connected device with intelligence, ranging from a personal computer to a server. Network devices such as routers, gateways, network monitors/managers, and concentrators are also considered hosts and need to be secured in accordance with all of the access control, monitoring, integrity, and backup provisions of these Standards.

3.1. General Network Requirements

Note: It is recommended that unused ports on switches, routers, and hubs supporting production environments be disabled or have access limited.

3.1.1. Perimeter. All NAHAC sponsored or managed networks including third party hosted subscription software must provide adequate physical and logical isolation from the Internet, extranets, and any other public networks. Such isolation must be achieved by corporate approved controls, which must include firewalls, and may also include, but not be limited to, packet filtering and application proxy technologies. Firewall configuration must comply with NAHAC firewall requirements.

3.1.2. Network Communication. Network communication systems must comply with the following standards:

3.1.2.1. Any connections from production environments to non-NAHAC hosts or networks must be approved through a documented process, which must include a security review and risk assessment prior to the connection.

3.1.2.2. Connections from other companies will be appropriately isolated by extranet security. This security must include firewalls, and may also include, but not be limited to, VPNs and filtering routers.

3.1.2.3. Connections to third party hosted subscription software must be approved through a documented process, which must include submittal and review of System and Organization Controls (SOC1, SOC2 and/or SOC3) Reports by the Service Organization.

3.1.3. Highest Security Level

3.1.3.1. Networks that operate at varying security levels will be isolated from each other by appropriate firewalls.

3.1.3.2. If connectivity is required between two hosts that reside on networks of different security levels, the lower level host must meet the security requirements of the higher-level network.

3.1.4. Encryption. [redacted]

Note: Network encryption should be employed to protect sensitive and proprietary data that would otherwise travel over insecure unsecured public or private lines/links. As contrasted with application or system level encryption and digital signature systems, network encryption occurs at a LAN or WAN level, and requires either hardware encryption devices or sufficient processor performance and memory capacity in a router to support software-based devices at the link or network layer of the OSI protocol stack. End-to-end application encryption [redacted] is preferred.

3.1.5. Data Dumps. Network data dumps, traces, and other related diagnostic data files must be protected against unauthorized access.

3.1.5.1. Any network data dumps, traces, and other related diagnostic data files transported to vendor sites for evaluation and analysis must be sanitized and encrypted before such transmission is permitted.

3.1.5.2. Non-Disclosure Agreement (NDA) must be in effect with any vendors who will be used for evaluation and analysis of network data dumps, traces, and other related diagnostic data files.

3.1.6. Logon Banner. [redacted]

3.1.7. Network and Communication Log Review. Timely review of network and communication equipment logs should be established. Appropriate review procedures should be put in place, and follow-up of any unusual activities or patterns of access must be investigated promptly by responsible personnel.

3.1.8. **Vulnerability Assessments.** Vulnerability assessment tools are restricted to those with a legitimate need for access. Only selected parties having specific, documented permission from NAHAC may use these tools. Generally, these tools should be made available only for the duration of testing. Rules of Engagement (RoE) should be established by NAHAC IT management prior to the commencement of testing. Consideration should be taken to ensure that tests do not adversely affect the operation of the system under test or the integrity, confidentiality, or availability of data unless the test is specifically designed to show denial of service, or data integrity/confidentiality vulnerabilities and is reviewed in advance. Vulnerability assessment attempts may trigger intrusion detection mechanisms. Therefore, prior to the initiation of testing, the appropriate Testing Authority must be notified about the conditions and intent of the tests.

3.1.9. Information about a deficiency should be restricted to those directly responsible for determining and implementing the corrective action.

3.1.10. Appropriate change control must be followed with IT named as a stakeholder.

3.1.11. **Software.** All software running on the network must be authorized and legally licensed. This includes interfaces and interactions with the Internet.

3.1.12. **Firewalls.** All firewalls will be subject to a thorough test for vulnerability prior to being put into production use and at least every [redacted] thereafter.

[redacted]

3.2. **Extranets.**

Extranets are defined by the communications requirements to establish direct communication with a NAHAC business partner. The endpoints of the communications are well known and independent of the communications technology used to provide the connection.

3.2.1. Any communication facility that connects NAHAC with its business partners using direct, point-to-point communications must be installed in an extranet area of a network security perimeter.

3.2.2. If the communications path traverses a publicly accessible medium ([redacted]), suitable authentication and encryption procedures ([redacted]) are mandatory.

3.2.3. If the communications path does not traverse a publicly accessible medium, then the authentication and encryption methods are determined by the sensitivity and integrity of the data being transmitted.

3.2.4. The communication endpoints of an extranet connection must be established at well-known, secure locations (locations inside the network security perimeter) and use a fixed network address.

3.2.5. Security design and configuration changes to an existing extranet connection must be reviewed and approved by IT. This also includes any changes made by the business partner or NAHAC that would affect the security posture of the remote network and the associated risk.

3.2.6. Extranet connections involving the use of a partner-managed server must locate the server outside of NAHAC's network security perimeter, i.e., firewall boundary.

3.2.7. Extranet connections to different partners or customers must not provide connectivity between partners or customers without both request and liability waivers received from all partners or customers involved and permission granted.

3.3. The Internet.

3.3.1. NAHAC reserves the right to use scanning and filtering technology to automatically scan inbound communications, whether e-mail, attachments to e-mail, web-page content, or other forms of communications, for viruses and inappropriate content.

3.3.2. Internet service channels must incorporate an IP routing boundary (i.e., proxies) such that Internet routes are not advertised on NAHAC internal network, and routes on NAHAC internal network are not advertised on the Internet.

3.4. Wireless:

[redacted] encryption shall be used for all traffic that will be facing the internal networks. Authentication must be in place using Domain account integration before access is granted to the network. The use of passwords for each user, in addition to a shared key is required. Only access points approved by the IT Department shall be allowed to operate.

3.5. Service Organization Networks.

All Service Organization Systems that are utilized to store or process NAHAC data, require the submittal of System and Organization Controls (SOC1, SOC2, and/or SOC3) Reports by the Service Organization. NAHAC IT management must review these reports to ensure that acceptable user controls and Standards as outlined in this document are available for implementation as a part of the NAHAC systems processing.

4. Asset Management

The Policy: NAHAC requires prudent management of its technology infrastructure, including networks, systems, applications, and processes throughout their respective life cycles. This management approach ensures a securely designed, implemented, and maintained asset protection environment.

4.1. Supporting Standards

4.1.1. Life Cycle Management

All networks, systems, applications, and/or processes that store, transport, and/or act on NAHAC information assets must have a documented life cycle. The management of that life cycle must include at least the following:

4.1.1.1. Acquisition Process. Purchases of network, system, and/or application resources, including hardware, software, repair parts, supplies, and consulting and support services must be made according to approved and documented process for acquisition of equipment, software, and related resources.

4.1.1.2. Requests for Proposals (RFPs) For Software and Hardware. RFPs and solicitations for the acquisition of software and hardware must contain a section on Information Security requirements.

4.1.1.3. Third-Party Security and Controls. Access to NAHAC computer systems by other organizations and their employees must comply with the following Information Security Standards.

4.1.1.3.1. Before an external provider is engaged, the provider must sign an NDA or a contract with the appropriate NAHAC entity that addresses this access. To the extent that the external provider will be involved with the Nevada HAF program, its clients, programs or data, approval by NAHAC is required prior to engagement.

4.1.1.3.2. The external service or facility provider must provide an equivalent level of security controls as required by these Information Security Standards. To the extent that the external provider will be involved with the Nevada HAF program, its clients, programs or data, approval by NAHAC is required prior to engagement.

4.1.1.4. Acceptable Life Cycle Management Processes. The use of a life cycle management process/system must meet generally accepted best practices for the involved network, system, application, and/or process.

4.1.1.4.1. **Review.** The process owner and/or an entity other than those directly responsible for its design, implementation, and/or operation must perform periodic review of the network, system, application, and/or process.

4.1.1.5. **Risk Assessment.** The process owner must perform an annual risk assessment. The assessment must include the reconciliation and verification of both physical and logical access to local and remote facilities and systems.

4.1.1.5.1. **Additional Risk Assessments.** A risk assessment must be performed prior to the completion of the following:

- Connections to foreign hosts and networks
- Software acquisition
- Outsourcing of IT operations
- Vendor or third-party access to NAHAC networks or systems.

4.1.1.5.2. **A risk assessment must be performed when:**

- A system, application, or process fails to comply with these Information Security Standards
- When requesting a deviation from Standards.

4.1.1.6. All computer and communications systems used for production processing must employ a formal change control procedure used to verify that only authorized changes are made.

4.2. Configuration Management

All networks and/or systems (collectively referred to as the "system") that store, transport, monitor, control, and/or process NAHAC information assets, or authenticate access, or authorize access level must meet generally acceptable configuration best practices for that system. Additionally:

4.2.1. General Configuration Management Standards

4.2.1.1. System configurations must be tested periodically by designated IT personnel for compliance.

4.2.1.2. Results of periodic compliance testing must be available to audit when requested.

4.2.1.3. Designated IT personnel must take prompt action to resolve compliance issues.

4.2.2. **Windows Standards.** These standards provide minimum information security requirements for securing current corporate-approved Windows server operating systems (OS), including production, test, disaster recovery, and development environments.

4.2.2.1. **Approved Windows Server Operating System Builds.** Windows servers must use an approved server build.

4.2.2.2. **Security Configuration Settings.** Windows servers must apply the Windows Information Security Configuration Settings for approved builds. The settings may be applied either manually (for existing systems) or through automated tools (for new builds).

4.2.2.2.1. **Minimum Information Security Configuration Standards.** Windows Information Security Configuration Settings must support the following minimum information security standards:

4.2.2.2.1.1. The operating system must log and audit attempts to gain access.

4.2.2.2.1.2. User Rights must be configured to minimize inappropriate use or access.

4.2.2.2.1.3. Security Options must be configured to minimize inappropriate use or access.

4.2.2.2.1.4. System Services must be configured to minimize inappropriate use or access.

4.2.2.2.1.5. Password Management must comply with NAHAC password standards.

4.2.2.2.1.6. File and Directory Permissions must be set to minimize inappropriate use or access.

4.2.2.2.1.7. General System Configuration Requirements must be appropriately implemented for each server.

4.2.2.3. **Compliance Monitoring.** Windows servers must be periodically monitored for continued compliance to information security requirements, with out-of-compliance conditions reported and resolved.

4.2.2.4. **OS Build Configuration Monitoring.** Periodically, IT administrators should spot-check a sample of production Windows servers for compliance to the approved server build.

4.3. Change Management

The appropriate Change Management process must be employed when making a deletion,

addition, or modification to, or any activity that may impact the availability or performance of an application or non-application component. This specifically includes all production and test environments.

4.3.1. NAHAC Compliant. Approved change management solutions must be compliant with NAHAC Policies and Standards.

4.3.2. Change Control. All changes to production applications, systems, or networks must utilize the appropriate Change Control/Management solution for the technology(ies) or platform(s) impacted by the change.

4.3.3. Validation of System Status. Before attempting any change (including maintenance) to any component of a system, the individual attempting such change must validate the status ("production," "test," or "other") of the system component. The change process must then proceed based on the change management/change control Standards for that status.

4.3.4. Production Data in Test Environments. Whenever possible, data used in testing application or system changes should not be production data (i.e., should be test data). Test data may be created to meet the application's test requirements or may be the result of sanitizing production data.

4.4. System Development Life Cycle Management

Any internal application development and/or system development efforts that include third-party software must utilize an approved system development life cycle management tool.

4.4.1. System development life cycle management tools must be compliant with NAHAC Policies and Standards.

4.4.2. Adequate procedures should be established to provide separation of duties in the origination and approval of source documents.

4.4.3. Any overrides or changes to confirmed transactions should be appropriately authorized, documented, and reviewed.

4.5. Electronic Data Disposal

Data confidentiality is an issue of legal and ethical concern. The purpose of this policy is to provide for proper cleaning or destruction of sensitive/confidential data and licensed software on all computer systems, electronic devices and electronic media being disposed, recycled or transferred either as surplus property or to another user.

Before any computer system, electronic device or electronic media is disposed, recycled or transferred either as surplus property or to another user, the system, media or device must be either:

- properly sanitized of sensitive/confidential data and software

- properly destroyed

Any confidential data must be appropriately retained / disposed of based on NAHAC records retention policy prior to erasure or destruction of the system, device or media.

[redacted]

5. Acceptable Use

The Policy: NAHAC requires the appropriate business use of all information assets under its care. This includes, but is not limited to, the proper use of information systems, telecommunications systems, the Internet/intranets/extranets connections, electronic mail, voice mail, telephones, cell phones, and faxes. NAHAC maintains the right to monitor, record, and audit the use of such systems and/or equipment, and report potential misuse to appropriate authorities. This policy contains guidelines for Electronic Communications created, sent, received, used, transmitted, or stored using NAHAC communication systems or equipment and employee provided systems or equipment used either in the workplace, during working time or to accomplish work tasks. "Electronic Communications" include, among other things, messages, images, data or any other information used in e-mail, instant messages, voice mail, fax machines, computers, personal digital assistants (including Blackberry, iPhone or similar devices), text messages, pagers, telephones, cellular and mobile phones including those with cameras, Intranet, Internet, back-up storage, information on a memory or flash key or card, jump or zip drive or any other type of internal or external removable storage drives. In the remainder of this policy, all of these communication devices are collectively referred to as "Systems."

Supporting Standards

5.1. Corporate Policies

In addition to the Corporate Information Security and Safeguards Program, employees must also adhere to the Standards and Policies outlined in the NAHAC Employee Handbook and the NAHAC Anti-Fraud Policy.

5.2. Audit Log Controls

Tampering with hardware and software controls that nullify their ability to log activity will be grounds for disciplinary action up to and including termination.

5.3. Authorized Access

Employees may use NAHAC systems to communicate internally with co-workers or externally with clients, suppliers, vendors, advisors, and other business acquaintances for business purposes.

Employees and trusted third parties charged with the monitoring and/or access of information transmitted or contained in NAHAC communication facilities must monitor and/or access such information only on a need-to-know basis related to appropriate business purposes. Such purposes include, but are not limited to:

- Finding lost information
- Performing job duties of an employee who is absent from work or unavailable
- Evaluating the effectiveness of information systems or equipment
- Investigating suspected criminal acts or breaches of security
- Investigating violations of corporate policies

- Repairing or recovering from failures of information systems or equipment.

All Electronic Communications contained on NAHAC systems are NAHAC's records and/or property. Although an employee may have an individual password to access these Systems, the Systems and Electronic Communications belong to NAHAC. Systems and Electronic Communications are accessible to NAHAC at all times including periodic unannounced inspections. Systems and Electronic Communications are subject to use, access, monitoring, review, recording and disclosure without advanced notice. Systems and Electronic Communications are not confidential or private. NAHAC's right to use, access, monitor, record and disclose Electronic Communications without advanced notice applies equally to employee-provided systems or equipment used in the workplace, during working time, or to accomplish work tasks.

Although incidental and occasional personal use of NAHAC Systems that does not interfere or conflict with productivity, NAHAC's business, or violate NAHAC policy is permitted. Personal communications located in NAHAC Systems are treated the same as all other Electronic Communications and will be used, accessed, recorded, monitored, and disclosed by NAHAC at any time without further notice. Since all Electronic Communications and Systems can be accessed without advanced notice, employees should not use NAHAC Systems for communication or information that employees would not want revealed to third parties.

5.4. Prohibited Use

Employees may not use NAHAC Systems in a manner that violates NAHAC policies including but not limited to Non-Harassment, Sexual Harassment, Equal Employment Opportunity, Confidentiality of Client Matters, Protecting NAHAC Information, Conflict of Interest and Solicitation and Distribution. Employees may not use NAHAC Systems in any way that may be seen as insulting, disruptive, obscene, offensive, or harmful to morale. Examples of prohibited uses include, but are not limited to, sexually explicit drawings, messages, images, cartoons, or jokes; propositions or love letters; ethnic or racial slurs, threats, or derogatory comments; or any other message or image that may be in violation of NAHAC policies.

An employee may not misrepresent, disguise, or conceal his or her identity or another's identity in any way while using Electronic Communications; make changes to Electronic Communications without clearly indicating such changes; or use another person's account, mail box, password, etc.

In addition, employees may not use NAHAC Systems:

- To download, save, send or access any defamatory, discriminatory or obscene material;
- To download, save, send or access any music, audio or video file;
- To download anything from the internet (including shareware or free software) without the advance written permission of a NAHAC IT;
- To download, save, send or access any site or content that NAHAC might deem "adult entertainment;"
- To access any "blog" or otherwise post a personal opinion on the intranet;

- To solicit employees or others;
- To attempt or to gain unauthorized or unlawful access to computers, equipment, networks, or systems of NAHAC or any other person or entity;
- In connection with any infringement of intellectual property rights, including but not limited to copyrights and trademarks; and
- In connection with the violation or attempted violation of any law.

5.5. Desktop Access Management

All employees, when leaving their desktop work area, must either log off the desktop computer or disable both the keyboard and screen via an approved desktop access control tool.

5.6. Clean Work Area

All employees must clear their work areas of documents and materials containing sensitive NAHAC confidential information and store such documents and materials appropriately before leaving the area.

5.7. Software Use

All employees must use the Common Operating Environment (COE) where available for desktop use and meet the following requirements when using any additional software on the desktop.

5.7.1. Non-COE Applications. Designated IT Personnel must review any desktop application outside NAHAC's COE that accesses customer sensitive data.

5.7.2. Freeware, Shareware. Only approved freeware or shareware can be downloaded to a NAHAC desktop by authorized personnel; all such software must be for appropriate business use.

5.7.3. Mobile Device Security. The following Standards are required of users of NAHAC-provided laptop personal computers, tablets, smartphones, e-Readers and other mobile devices capable of capturing and storing data ("Mobile Devices"):

5.7.3.1. For all Mobile Devices operating on the Desktop Services, all sensitive NAHAC confidential data stored on the Mobile Device's hard drive must be encrypted.

5.7.3.2. Users of NAHAC-owned Mobile Devices that may contain sensitive NAHAC confidential information are responsible for protecting that information from loss, theft, and damage.

5.7.3.3. Mobile Device Security; Storing Customer Confidential Information. The following Standards are required of users of NAHAC-provided Mobile Devices that may carry Customer Confidential Information.

5.7.3.3.1. For all Mobile Devices carrying Customer Confidential information (for example, information protected by law, regulation or which is covered under Confidentiality Agreements), such Mobile Devices must utilize full disk encryption ([redacted]).

6. Vulnerability Assessment and Management

The Policy: NAHAC continually identifies and prioritizes technical, organizational, procedural, and/or physical security weaknesses, manages the mitigation of identified risks, and maintains metrics on progress.

Supporting Standards

6.1. Vulnerability Assessment

The first step in vulnerability assessment and management must be to identify and assess vulnerabilities. A designated third-party security Organization must test for vulnerabilities at the network level, the operating systems level, and the application level.

6.1.1. Vulnerability Testing. Vulnerability testing must be performed to verify that existing security controls are functioning on all high risk and externally assessable solutions. It is strongly recommended that testing be conducted on all remaining solutions (i.e., medium and low risk).

6.1.1.1. Approval. To minimize disruption and/or damage to production networks, systems, and/or applications, only tests authorized by the IT management are permitted.

6.1.2. IT Security Assessments. IT shall authorize periodic security assessments.

6.2. Vulnerability Management

The second step in vulnerability assessment must be the management functions, including prioritizing known vulnerabilities, managing the mitigation of these risks, and tracking progress.

6.2.1. System Configuration Monitoring. Designated personnel must periodically review the configuration and operating environment of production operating systems, networks, and applications.

6.2.1.1. Monitoring/Compliance Tools. Where security configuration monitoring and/or reporting tools are in place, they must be utilized and the results forwarded to IT audit upon request.

6.2.1.2. Vulnerabilities. High Risk vulnerabilities discovered through configuration monitoring must be brought to the attention of the system owner and IT management must be included in the next risk assessment, if not mitigated.

6.2.2. Disclosure. Specific information about information system vulnerabilities is confidential and must NOT be distributed to internal or external parties who do not have a demonstrated need-to-know.

6.2.3. System vulnerability analysis software should be run periodically ([redacted]) on all network server systems, mid-range systems, and perimeter systems. Results should be shared only with audit and designated IT personnel responsible for fixing the vulnerabilities.

7. Threat Assessment, Monitoring and Response

The Policy: NAHAC identifies and prioritizes categories of threats and seeks to deter them. NAHAC employs threat detection monitoring tools to provide timely response and recovery. In addition, NAHAC has defined response protocols which it is bound, by law and regulation, to follow in the event of a data security breach.

Supporting Standards

7.1. Threat Assessment

Natural threats (storms, floods, disasters), human threats (malicious and/or careless behavior), and technical threats (intrusion, interception, alteration, denial, and/or system failure) all could jeopardize NAHAC information assets and/or reputation. All employees must be aware of these threats and report observed threats to management.

7.1.1. Designated IT personnel will monitor, assess, and prioritize information security threats, using available tools, knowledge bases, and/or third-party services.

7.1.2. Designated IT personnel will inform management, of known high risk threats immediately upon becoming aware of such threats.

7.2. Disclosure

Any potential information about the individuals, organizations, or specific systems that have been damaged by computer crimes and computer abuses, as well as the specific methods used to exploit such vulnerabilities, are confidential and must NOT be disclosed to parties who do not have a demonstrated need to know.

7.2.1. Log Access. Access to data captured and/or logged by intrusion detection activity must be restricted to only those who have a demonstrated need to know.

7.3. Reporting Information Security Incidents and Computer-Related Crimes

The Reporting Information Security Incidents and Computer-Related Crimes policy applies to all staff and contractors of Nevada Affordable Housing Assistance Corporation (NAHAC), working on the Nevada HAF and HHF Programs. This policy does not apply to Vendor or other Subcontractors or to NAHAC resources that do not perform services for the Nevada HAF and HHF Programs.

Vendor and Subcontractors must have their own similar policy which is at least as protective of NAHAC's and client's sensitive information as this policy and be compatible with applicable laws, rules, regulations, and best business practices. It is the responsibility of NAHAC Compliance Manager to ensure such policies are in force.

Purpose

The purpose of this policy is to ensure that immediate and appropriate action is taken to protect the security, integrity, availability, and confidentiality of NAHAC information assets, deter further

loss of, or damage to, those assets and remediate issues discovered as a result of any incident in order to strengthen the security of NAHAC information and the Information Security and Safeguards Program ("ISSP"). Any incident (e.g., any event, suspected event, or vulnerability that could pose a threat to NAHAC information assets) must be reported to the appropriate NAHAC staff, and external entities, as appropriate, and mitigated immediately.

It is the responsibility of all employees to protect NAHAC's data. Both intentional and unintentional misuse of NAHAC-owned, sensitive and private data subject NAHAC staff to disciplinary action in accordance with the extent and frequency of the misuse and may include criminal charges.

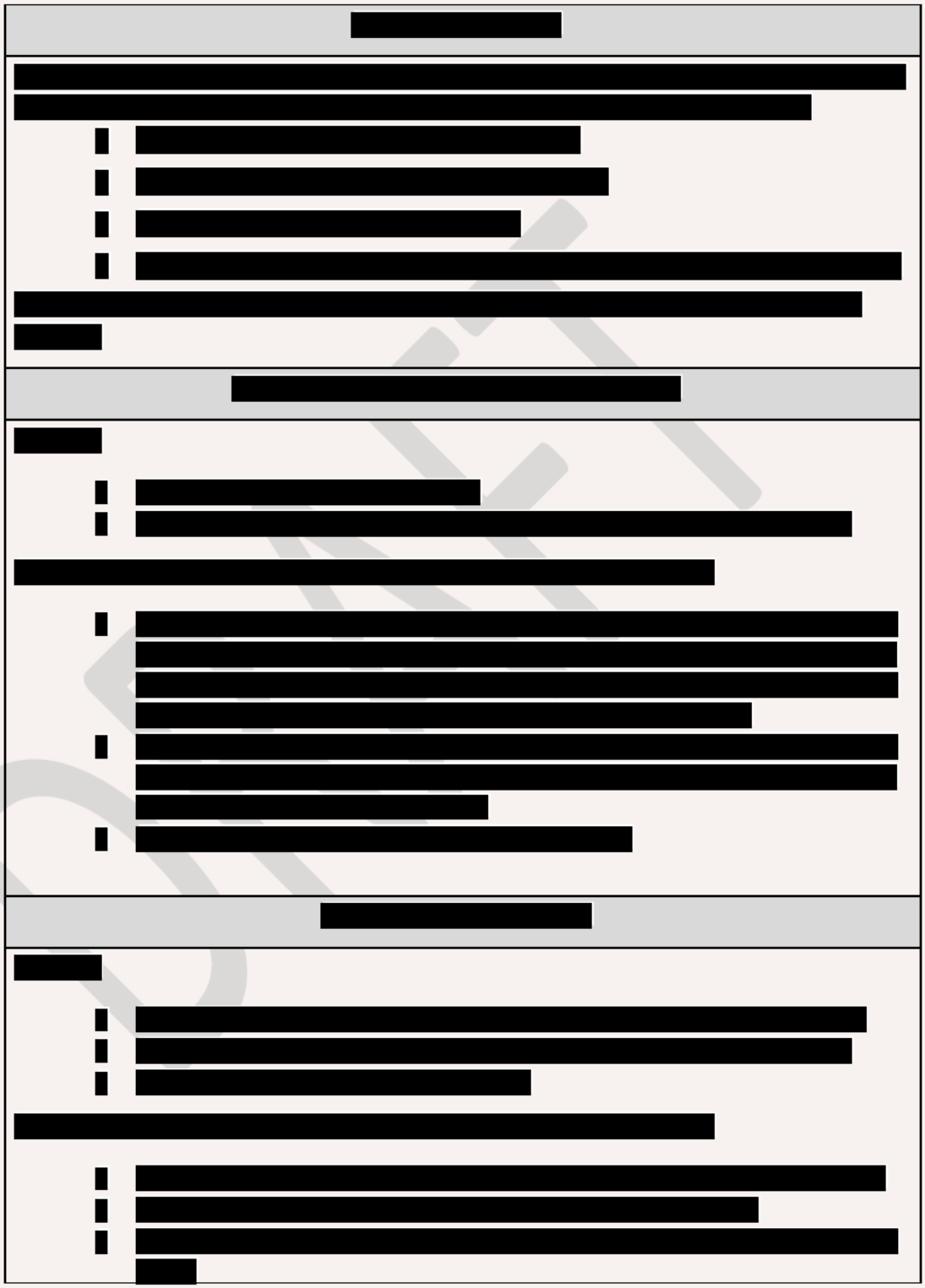
Management is responsible for ensuring that their direct reports understand the scope and implications of this policy.

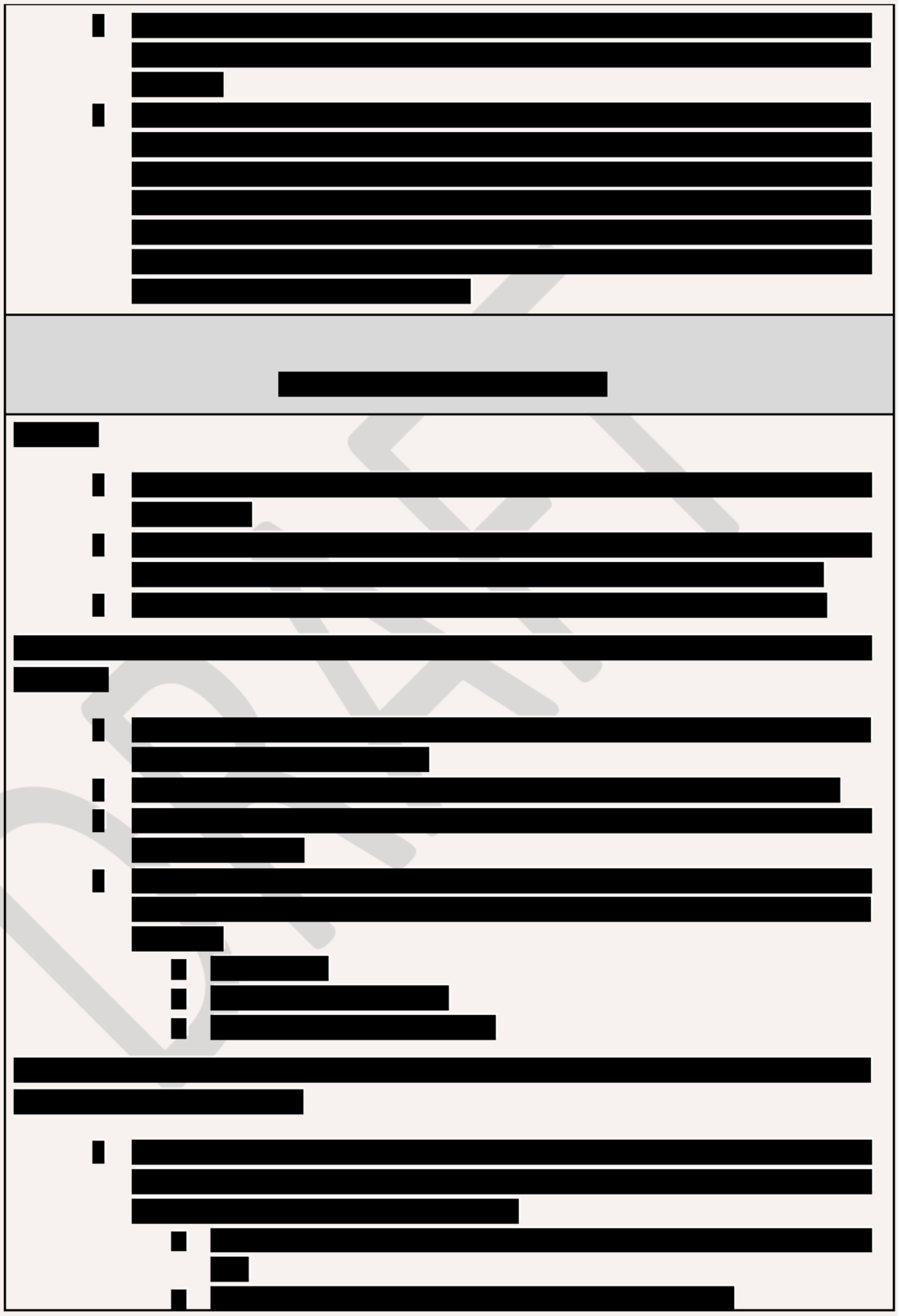
Types of Incidents

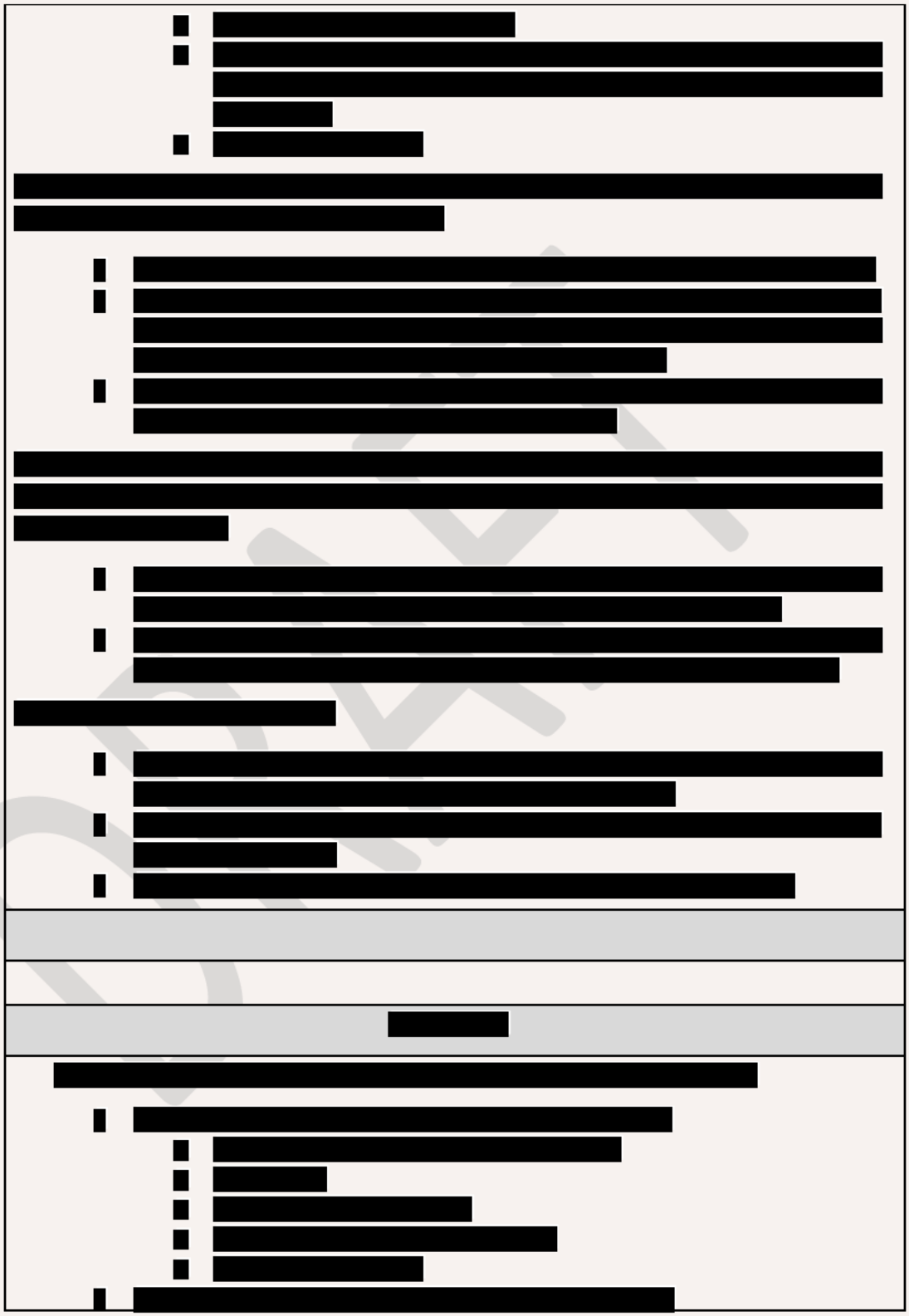
Some examples of information security incidents that must be reported are listed below. Any event, suspected event, or vulnerability that could pose a threat to NAHAC information assets should be reported.

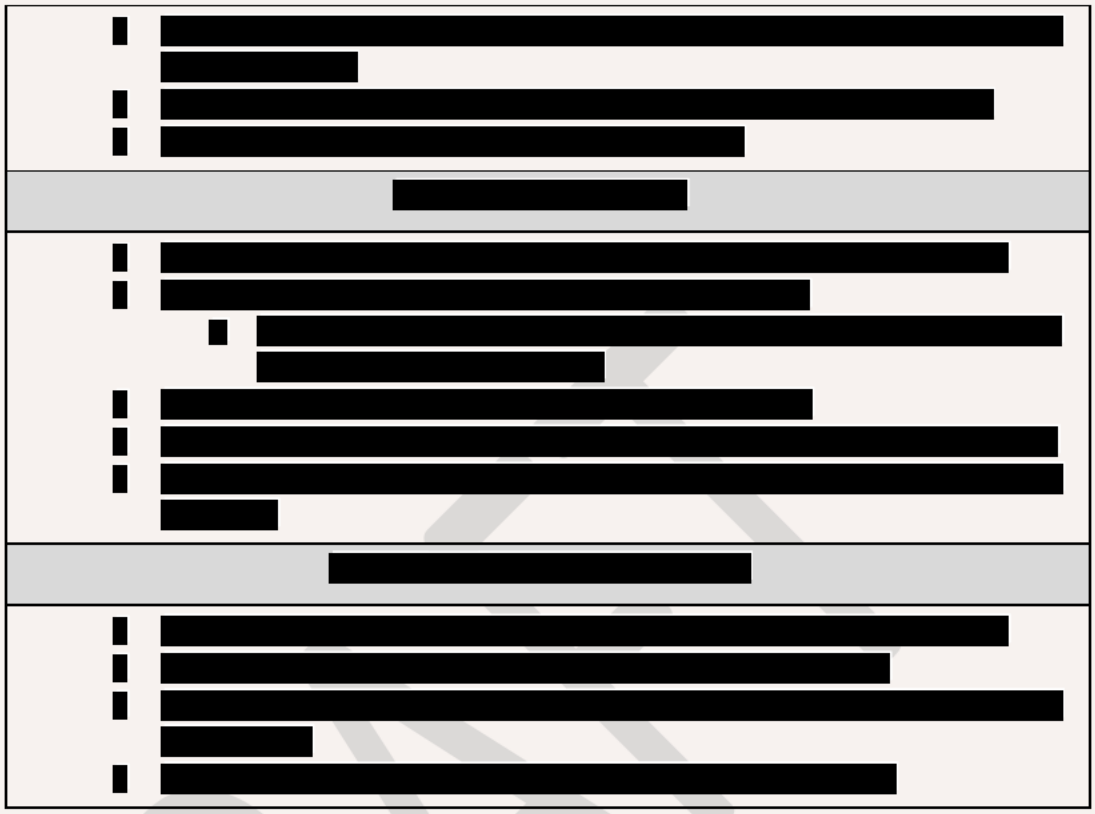
1. Unauthorized parties accessed one or more NAHAC computers, computer systems, computer networks or hardcopy documentation potentially containing NAHAC-owned, sensitive or private information.
2. NAHAC subcontractor experiences a security breach, or suspects they have experienced a security breach, of Nevada HAF and HHF Programs information for which they are contractually responsible.
3. Personally Identifiable Information (PII) was transmitted via means that would be reasonably considered not adequately secured and may have been intercepted by unauthorized persons.
4. Without prior written approval, NAHAC-owned data or PII was damaged, destroyed, deleted, shared, altered, copied, or used for purposes other than those which support the Nevada HHF program.
5. Someone has accessed and without permission added, altered, damaged, deleted, or destroyed any computer software or computer programs that reside in an NAHAC computer, computer system, or computer network.
6. Physical intrusions into NAHAC facilities that may have resulted in compromise of NAHAC sensitive information or PII.
7. A contaminant is introduced into any NAHAC computer, computer system, or computer network that may make NAHAC information vulnerable to unauthorized access (e.g., viruses, malware, Trojans, worms, bots, exploit, back door, and other types of malicious attacks).

Roles and Procedures









8. Security Awareness and Education

The Policy: The Organization requires policy framework elements and standards content be properly communicated and accessible to new hires, employees, and third parties through the provision of appropriate education and training.

Supporting Standards

8.1. Security Awareness and Education for New Hires

The following applicable Standards apply to all new employees:

8.1.1. New employees shall be trained in all aspects of confidentiality, privacy, and the protection of sensitive information. All employees will be retrained not less than once each year.

8.2. Ongoing Security Awareness and Education

An on-going employee (including contractors, consultants, and vendors with access to Organization information assets) awareness program must be established to create and maintain security awareness of applicable Policies, Standards, and responsibilities at all staff levels.

8.3. Contracts

Contracts define the relationships between NAHAC and its business partners, suppliers, customers, and other business associates. Each entity must be made aware of their information security responsibilities through the use of specific language used in contracts.

8.4. Security Awareness Availability

Information security media, such as video, pamphlets, web sites, personal and/or on-site training will be available and accessible to all employees in an effort to make employees aware of information security.