ACAM Data Security Policy

6/11/19 Revised 3/27/23, 1/27/25

The purpose of this policy is to cover the Data Security Policy: Employee/Contractors Requirements and Data Security Policy: System Safeguards and Emergency Storage/Recovery.

<u>Data security policy: Employee/Contractor requirements</u>

This policy outlines behaviors expected of employees when dealing with data and provides a classification of the types of data with which they should be concerned. This policy provides users with guidance on the required behaviors.

<u>Purpose</u>
ACAM must protect restricted, confidential, or sensitive data from loss to avoid reputation damage and to avoid adversely impacting our partnering organizations and clients. The protection of data is a critical business requirement, yet flexibility to access data and work effectively is also critical.

It is not anticipated that this technology control can effectively deal with a malicious theft scenario, or that it will reliably protect all data. The primary objective of this policy is user awareness and to avoid accidental loss scenarios. This policy outlines the requirements for data leakage prevention, a focus for the policy and a rationale.

<u>Scope</u>

1. Any employee, contractor, or individual with access to ACAM systems or data.
2. Definition of data to be protected:
   - Personal identifying data of employees, ACAM's partnering organizations and clients served, and
   - Restricted/Sensitive or confidential information.
3. State requirements for technology-enabled devices

<u>Policy – Employee and contractor requirements</u>

1. ACAM's employees shall uphold the acceptable use policy as well as related policies outlined in the (i) Employees Handbook, (ii) Homeless Management Information (HMIS) user agreement, (iii) ACAM Privacy Policy and Homelessness Prevention and Intervention Business Rules, (iv) Case Management procedures, and (v) Record Retention Policy, as applicable.
2. Contractors and Sub-contractors are formally held responsible and accountable for all contractual agreements and requirements. Contractual agreements shall accommodate ACAM's requirements/restrictions concerning the physical storage location of ACAM data and/or physical routing of sensitive information.
3. If an employee and/or contractor identifies an unknown, un-escorted or otherwise unauthorized individual in ACAM's offices, employees and contractors must immediately notify the CEO and IT Consultant.
4. Visitors to ACAM must be escorted by an authorized employee at all times. If employees and contractors are responsible for escorting visitors, such employees and contractors must restrict the visitors from secured areas.
5. Employees and contractors are required not to reference the subject or content of sensitive or confidential data publicly, or via systems or communication channels not

controlled by ACAM. For example, the use of external e-mail systems not hosted by ACAM to distribute data is not allowed.

6. Please keep a clean desk. To maintain information security, employees and contractors need to ensure that all printed sensitive data is not left unattended at employee or contractor workstations.
7. Employees and contractors need to use a secure password on all ACAM systems. The system is set to require a reset of network passwords every 90 days. These credentials must be unique and must not be used on any other external systems or services. The minimum password length is 7, and it must meet the Windows Active Directory complexity requirements, information on the requirements can be found here.
8. Terminated employees will be required, immediately upon termination, to return all records, in any format, containing personal information as well as all ACAM proprietary information and records.
9. Employees and contractors must immediately notify the CEO if a device containing protected or confidential data is lost (e.g., mobiles, laptops etc.).
10. If employees and contractors find a system or process that employees and contractors suspect is not compliant with this policy, or the objective of information security, employees and contractors have a duty to inform the CEO so that the CEO can take appropriate action.
11. Authorization to work remotely will be determined on a case-by-case basis by the CEO. Remote access to ACAM systems is provided by the Microsoft Remote Desktop Protocol, which is encrypted. This access is restricted by the IT consultant via Active Directory security policies. Furthermore, even with remote access, only those data folders that are necessary will be visible to the user.
12. Remote employees and contractors must follow industry best practices to ensure that data is appropriately protected from loss/theft. Some examples of industry best practices are running a supported operating system (e.g., Windows 10 instead of Windows 7), and antivirus software that is supported with up-to-date definitions. Furthermore, remote access to ACAM's network from public or shared* computers is strictly prohibited. Employees and contractors should seek guidance from the CEO if unsure as to employees and contractor responsibilities and/or for clarification regarding current industry best practices. * An example of a shared computer would be a family PC that is used by more than one individual.
13. All documents and data on ACAM's network are the property of ACAM and are not to be taken off-premises electronically or physically without prior authorization from the CEO or a supervisor.
14. ACAM's Data Security Policy is in place to protect all ACAM data, facilitate ease of access by authorized individuals to shared data, and enable back-up procedures that are in place for the U: drive that would not be available for other storage methods. Documents, emails, or any other files, including drafts, must not be stored, even temporarily, on personal property. Personal property includes desktops, personal One Drives, thumb drives, personal Drop Box accounts or any other location that is not on an ACAM approved network (U: drive) and/or ACAM owned and administered document sharing platform (e.g., ACAM owned Teams account). When storing files on the U: drive, files should be properly labeled to prevent issues of version control (e.g. Working File DRAFT V2).
15. Please ensure that equipment holding data within the scope of this policy are not left unduly exposed, for example visible in the back seat of an employee's or contractor's car. Desktops that display sensitive information are to be positioned to prevent unauthorized viewing.

16. Access to secure areas are controlled by key distribution management and a receptionist is always present when the doors are open.
17. Some files in the ACAM network contain "ACAM Confidential" and/or personally identifiable data of clients or employees as defined by HIPAA/PCI (sensitive data). If these files must be transmitted outside of ACAM's secured network, industry best practices for protection of that data must be followed. One example of industry best practices can be found here.
18. Sensitive data that must be moved within ACAM is to be transferred only via business-provided secure transfer mechanisms (e.g., encrypted USB keys, secure file shares etc.). ACAM will provide employees and contractors with systems or devices that fit this purpose. Employees and contractors must not use other mechanisms to handle sensitive or confidential data. If an employee or contractor has a query regarding use of a transfer mechanism, or the designated transfer mechanism does not meet an employee's or contractor's business purpose, employees and contractors must raise this with their supervisor or the CEO.
19. If sensitive data is suspected to have been transmitted insecurely, the employee or consultant must report it to their supervisor or the CEO immediately. The IT Consultant will conduct the first review, identifying data that may be sensitive and situations where its transfer was or was not authorized and whether or not there is a concern of inappropriate use. These findings will be escalated to ACAM's management to protect the individual or individuals affected by the breach.
20. State-Owned Devices: On December 7, 2022, Governor Greg Abbott required (https://gov.texas.gov/uploads/files/press/State_Agencies_Letter_1.pdf) all state agencies to ban the video-sharing application TikTok from all state-owned and state-issued devices and networks. Governor Abbott also directed the Texas Department of Public Safety (DPS) and the Texas Department of Information Resources (DIR) to develop a plan providing state agencies guidance on managing personal devices used to conduct state business. ACAM will implement the removal and prohibition of any listed applications and technology. ACAM may prohibit technology threats in addition to those identified by DIR and DPS.

    In addition to TikTok, ACAM may add other software and hardware products with security concerns to this prohibition policy and will be required to remove prohibited technologies that are on the DIR prohibited technology list. "Prohibited Technologies" shall refer to TikTok and any additional hardware or software products added to this Policy.

    When applicable, employees will have use of a Workforce Solutions (state-owned) device(s) (e.g., mobile phone and/or laptop) purchased with funding through the Workforce Solutions/Texas Workforce Commission for the sole purpose of conducting business. Workforce Solutions employees are prohibited from conducting state business on technology-enabled personal devices. A list of prohibited software and hardware can be found at https://dir.texas.gov/information-security/prohibited-technologies. Except where approved exceptions apply, the use or download of prohibited applications or websites is prohibited on all Workforce Solutions/Texas Workforce Commission (state-owned) devices, including cell phones, tablets, desktop and laptop computers, and other internet capable devices.

    - For devices purchased with state funding (such as Texas Workforce Commission dollars), ACAM will identify, track, and control state-owned devices to prohibit the installation of or access to all prohibited applications. This includes the various prohibited applications for mobile, desktop, or other internet capable devices.

- ACAM will manage all state-issued mobile devices by acquiring services of one or more third-party Mobile Device Management (MDM) companies, such as Hexnode and/or Addigy, to comply with new requirements and have the ability to lock down state-owned devices used by ACAM staff running a state-funded program. The security controls managed by the MDM will include the ability to:
    - Restrict access to "app stores" or non-authorized software repositories to prevent the installation of unauthorized applications.
    - Maintain the ability to remotely "wipe" or erase non-compliant or compromised mobile devices.
    - Maintain the ability to remotely uninstall un-authorized software from mobile devices.
    - Deploy secure baseline configurations, for mobile devices, as determined by Texas Workforce Commission.

Sensitive locations must be identified, cataloged, and labeled by the agency. A sensitive location is any location, physical, or technological (such as video conferencing, or electronic meeting rooms) that is used to discuss confidential or sensitive information, including information technology configurations, criminal justice information, financial data, personally identifiable data, sensitive personal information, or any data protected by federal or state law.

Unauthorized devices such as personal cell phones, tablets, or laptops may not enter sensitive locations, which includes any electronic meeting labeled as a sensitive location.
Visitors granted access to secure locations are subject to the same limitations as contractors and employees on unauthorized personal devices when entering secure locations.

21. For ACAM staff who are part of the NextGen program with Workforce Solutions, Information Resources are to be used for official Workforce Solutions-approved business and are not for personal use; by signing this form you agree to the following statements:
    - I will not perform any work, review, update, or otherwise act to obtain information about my own, or any relative's, friend's, or business associate's case, claim or account, even if it is closed.
    - There may be specific limited use exceptions outlined in other policies and procedures of Workforce Solutions.
    - Workforce Solutions has a duty to protect its Information Resources.
    - Workforce Solutions has the right to control or filter access to specific Information Resources.
    - Workforce Solutions has the right to monitor the use of Information Resources under its authority.
    - Workforce Solutions retains the right to terminate, restrict or limit access to or use of any Information Resources by any individual(s).
    - Use of personal devices to conduct Workforce Solutions business, including accessing any Workforce Solutions owned data, applications, email accounts, or non-public facing communications, is prohibited under the Information Security Standards and Guidelines.
    - Users of Workforce Solutions Information Resources have no right to privacy in their use of Information Resources or in the content of their communications sent or stored in Workforce Solutions owned or operated.

System Safeguards and Emergency Storage/Recovery

This section documents emergency procedures, responsibilities, and how copies of these items are stored securely at multiple sites.

1. Daily backups of customer data are stored securely in the cloud in a Microsoft SharePoint folder that also replicates automatically to an accessible secured offsite location. In the event of a disaster, the CEO can access the documents via either the cloud or the secured offsite location. In the event that the network is down, and the CEO is unavailable, the IT Consultant has a copy of the SharePoint password in their password management system to ensure ACAM business continuity.
2. ACAM does not currently utilize backup media.
3. Antivirus and firewall. ACAM uses Kaseya Antivirus as a part of the endpoint security suite software. ACAM's current hardware firewall is a Sonicwall TZ 370W.
4. All vendor-supplied default passwords or similar "published" access codes for all installed operating systems, database management systems, network devices, application packages, and any other commercially produced IT products have been changed or disabled.
5. Access is immediately removed or modified when personnel terminate, transfer, or change job functions.
6. Appropriate environmental controls have been implemented where possible to manage the equipment risks such as: alarms, fire safety, cooling, heating, smoke detector, battery backup, etc.

Other related Policies and Procedures:

1) ACAM Employee Handbook
2) ACAM ESG Business Rules
3) ACAM Disaster Response Plan
4) Coalition for the Homeless' HMIS Privacy Policy
5) ACAM Privacy Policy
6) ACAM Record Retention Policy

All employees and contractors shall sign a document confirming their understanding of this policy.

____

Name & Date

____

Title

____

Organization