Workforce Solutions Information Security Standards and Guidelines

Revised: October 15, 2024

1. STANDARD

All Workforce Solutions contractors will use information system hardware, software, and computer data in accordance with these rules and procedures to provide high quality service for our customers while maintaining the integrity and security of all individual and service data. These Information Security Standards and Guidelines apply to any person, staff, or volunteer, who has access to a customer's Sensitive Personal Information whether in electronic or paper format.

2. ACCEPTABLE USE

Workforce Solutions computer data, hardware, and software are state/federal property. All information passing through Workforce Solutions network, which has not been specifically identified as the property of other parties, will be treated as a Workforce Solutions asset. Unauthorized access, disclosure, duplication, modification, diversion, destruction, loss, misuse, or theft of this information is prohibited. All equipment must have approved virus protection software.

Every information system privilege that has not been explicitly authorized is prohibited. Information entrusted to Workforce Solutions will be protected in a manner consistent with its confidentiality and in accordance with all applicable standards, agreements, and laws.

All Workforce Solutions employees, Gulf Coast Workforce Board staff, volunteers, private providers of services, contractors, vendors, representatives of other agencies of local, state or federal government, and any other person or entity granted access to Workforce Solutions information resources must comply with the following standards set forth below and elsewhere in these Information Security Standards and Guidelines as they are updated:

1. All User activity on Workforce Solutions information resources is subject to logging and review.

2. Software installed or executed within Workforce Solutions systems and/or networks must be approved.

3. Users in public access facilities must not leave their computers unattended. Users must either lock access to their workstations or logoff. Users with computers behind a permanent physical and visual structural barrier, away from the public, should, as a good practice, also lock access to their workstations or logoff.

4. Users must not share their passwords, Personal Identification Numbers (PIN), Security Tokens (e.g., Smartcard), or similar information or devices used for identification and authentication purposes.

5. Users must not operate an unauthorized public peer-to-peer file sharing system to transfer files (Ex. Drop Box/ Google Drive) or use Instant Messaging to communicate with others. Users must use Workforce Solutions managed file sharing system.

6. Any Workforce Solutions Information Resources User who becomes aware of a weakness, incident, misuse, or violation of any policy related to the security and protection of those resources must report such to her supervisor and follow the proper procedure defined in 14.2.3.2 Breach of Security as soon as possible.

7. Users may not attempt to access any data, program, or system for which they do not have approved authorization or explicit consent.

8. Users of Workforce Solutions Information Resources must protect all account information that may allow access to any system under the authority of Workforce Solutions. This includes account identifiers, passwords, personal identification numbers, access tokens or any other information, or device used for User identification and/or authorization.

9. The use of any unapproved, unlicensed, or otherwise unauthorized software is prohibited.

10. This includes any activity that adversely affects the functionality of a User's workstation or violates software license requirements.

11. Users must not intentionally access, create, store, or transmit any material that may be offensive, indecent, or obscene unless such action is specifically within the scope of job duties for their position.

12. Any activity which may harass, threaten, or abuse others, degrade the performance of information resources, deprive, or reduce an authorized User's access to resources or otherwise circumvent any security measure or policy is prohibited.

13. Users must not purposely engage in unauthorized activity that may circumvent the department computer security measures.

14. The unauthorized copying of otherwise legal and licensed software is prohibited.

15. Unauthorized duplication of software may be a violation of copyright laws.

16. A User shall not use any Workforce Solutions information resource in such a manner that she may gain personal benefit.

17. Users must use appropriate safeguards to protect state-owned software and hardware from damage, loss, or theft.

18. If a User is in possession of a department owned or leased computer that is used off-site, at the User's home, or at any location not under the authority of Workforce Solutions, that User must follow the same policies, standards and guidelines established for use of such equipment located at or in any Workforce Solutions location.

19. Any User of Workforce Solutions owned, or leased equipment used in an environment out of the authority of Workforce Solutions must protect that equipment from use and abuse by non-Workforce Solutions approved Users. Users of such equipment must not allow the use of such equipment by any family member or other non-employee or unauthorized User.

20. Users of Workforce Solutions information resources must not engage in any act that would violate the purposes and goals of Workforce Solutions as specified in its governing documents, rules, regulations, and procedures.

21. Users must not divulge IP addresses of Workforce Solutions systems.

22. Users must not intentionally store or transmit any materials for which they or Workforce Solutions does not hold copyright permissions. This includes, but is not limited to, audio, video, software, data, or any other digital information.

3. ACCOUNT MANAGEMENT

Account Management establishes the standards for the creation, monitoring, control, and removal of User accounts. The Account Management standard shall apply equally to all User accounts without regard to their status or category.

User accounts are the means by which access is granted to Workforce Solutions information resources. Accounts are granted to Workforce Solutions employees, Board staff, volunteers,

vendors, contractors, students, and others determined to have a need. These accounts assist in establishing accountability for systems use and are a key component in the protection of data; its confidentiality and integrity.

1. All Users must sign Workforce Solutions Information Resources Usage Agreement, Code of Conduct and Equal Opportunity Employee Acknowledgement Form before access is given to an account.

2. Users of Workforce Solutions systems must have on file a signed Workforce Solutions Information Resources Usage Agreement, Code of Conduct and Equal Opportunity Employee Acknowledgement Form within 30 days of employment. The agreement, Code of Conduct and Equal Opportunity Employee Acknowledgement Form shall be reaffirmed annually during the month of October.

3. All Users must successfully complete the following on- line trainings before access is given to an account and annually, in October, thereafter:
    a. Cybersecurity Awareness Training
    b. Fraud Awareness Training
    c. Equal Employment Opportunity Training
    d. Human Trafficking
    e. WIOA Discrimination Complaint Process
        i. For EO Officers, Office/ Contract Managers, Monitors, and Navigators
    f. FNS Civil Rights Training

4. All users must register and successfully complete the following trainings within 30 days after activating an account and annually, in October*, thereafter:
    a. Omnilert (Registration)
    b. Sysaid (Registration)
    c. KnowBe4*
    d. Veterans Triage*

    If a user fails a simulated phishing attempt, the user must complete an additional testing for each failed attempt within 30 days.

5. EO Officers, office/contract managers, monitors, and navigators must successfully complete the Texas Work Commission Complaint Process on- line training in addition before access is given to an account and annually thereafter.

6. All accounts must be identifiable using a unique User ID.

7. Accounts, other than service/maintenance accounts, must uniquely identify a specific User.

8. Account access levels will be reviewed, at a minimum, every month for appropriateness. Appropriateness shall be reviewed and affirmed by the appropriate Local Information Security Officer.

9. Workforce Solutions Local Information Security Officers (LISO) are:

    a. Responsible for adding, modifying, disabling, or deleting the accounts of individuals with access to Workforce Solutions Information Services, and

    b. Must have a documented process to modify a User account to accommodate situations such as name changes, account changes and permission changes, and

    c. Must have a documented process for periodically reviewing existing accounts for approved access, and

    d. Must provide a list of accounts for the systems they administer when requested by authorized Workforce Solutions management, and

    e. Must cooperate with authorized Workforce Solutions management investigating security incidents.

10. In the event of termination of employment, or temporary leave status (including FMLA), office LISOs must notify workforce security by email (WorkforceSecurity@wrksolutions.com) that the User will no longer need access to Workforce Solutions information systems. Notification must occur no later than the day the staff is scheduled to exit employment or begin temporary leave.

11. In the event of change in job duties or position, office LISOs must notify workforce security by email (WorkforceSecurity@wrksolutions.com) that there are changes (adding or removing) to the User's access to information resources. Notification must occur no later than the day the staff changes job duties or position.

12. In addition, no later than Noon on the first working day of the following month, each contractor will provide a list to Workforce Security of the individuals hired and terminated the previous month. Contractors will use the report format attached to WS Issuance 11-15. Contractors can be penalized for not submitting timely updates on staff status as referenced

in WS Issuance 11-15.

a. All access accounts established for contractors, consultants, vendors and/or maintenance accounts must be deleted immediately upon termination or completion of the contract period. All extension of access periods for these accounts must be reflected in appropriate contract changes.

b. All non-Workforce Solution users of non-public Workforce Solutions Information Resources shall be required to sign an agreement establishing the requirement for notification of User changes brought about by an employee termination or transfer. These accounts shall be deleted, removed, or reassigned in compliance with application- specific requirements.

c. Reconcile the Users recorded in the Workforce Solutions user database attached to the contractors' locations (contractor administration location and career office) monthly to ensure the level of access is appropriate for the employee's job duties.

13. Each contractor is responsible for compliance of their staff with these standard operating procedures. To that effect, each contractor must appoint a Contractor Local Information Security Officer and a backup. If the contractor operates career offices, each career office must also have a Local Information Security Officer and a backup.

14. Each contractor must establish internal procedures to ensure compliance with these standards and guidelines. Include in these procedures the specific duties of the Contractor LISO and the Office LISO, if applicable. Duties of Local Information Security Officer include but are not limited to:

a. Provide a security orientation to the User upon hire. The LISO must provide staff with sufficient training and support reference materials to allow them to properly protect information resources. The LISO must ensure Workforce Solutions Information Security Standards and Guidelines are available to staff and should not provide access to any Workforce Solutions systems prior to the completion of the required testing.

b. Staff must sign the appropriate security documents and successfully complete the on-line trainings before the LISO can request access to Workforce Solutions information system. Any staff that receive a wrksolutions email must complete Veterans Triage and KnowBe4 email training and any remedial

training if test phishing emails are failed within 30 days of receiving the emails. The original security documents must be kept at the contractor's office, including but not limited to:

- Signed Workforce Solutions Information Resources Usage Agreement
- Signed Code of Conduct
- Equal Opportunity Employee Acknowledgement Form
- Cybersecurity Awareness Training Certificate
- Fraud Awareness Training Certificate
- Diversity, EEO, and Discrimination Prevention Certificate
- Human Trafficking Certificate
- WIOA Discrimination Complaint Process Certificate (if applicable)
- KnowBe4 Security Awareness Certificate
- Veterans Triage Training Certificate
- FNS Civil Rights Training

The LISO will email a copy of the signed Workforce Solutions Information Resources Usage Agreement, Code of Conduct and Equal Opportunity Employee Acknowledgement Form to Workforce.Security@wrksolutions.com. Access rights will be granted when the Board LISO receives a cop y of this document.

c. Maintain rights to RACF (TWC Mainframe) for each location operated by the contractor for staff who need this access. This requires the appointment of Office LISOs who are responsible for the staff at that location.

   i. The Contractor or Office LISO must complete the TWC RACF Managers Training module part 1 and 2. The LISO must complete this training prior to taking management actions for their location.

   ii. The Contractor or Office LISO will add and remove staff for the RACF system at their location. The LISO is also responsible for resetting passwords and assign rights for the RACF system for Users attached to their location.

d. The Office LISO will maintain a file of all usage agreements and training certificates for monitoring review. The Contractor and Office LISO will use the Workforce Solutions user database to manage information about the User's location, position, and the identification of the information systems the staff needs to accomplish her responsibilities.

e. LISO must notify workforce security by email (WorkforceSecurity@wrksolutions.com) in the event of termination of employment or a change in job status necessitating the removal or addition of a User's access to one or more data systems.

f. If the User is transferring from one location to another location managed by the same contractor, the LISO will notify workforce security by email (WorkforceSecurity@wrksolutions.com) with the information about the new office. In addition, the LISO will review the data systems accessed by the User and determine if all are appropriate and request workforce security add or remove access as appropriate.

15. Board LISO must establish internal procedures to ensure compliance with these standard operating procedures. Include in these procedures the specific duties of the Board LISO. Duties of the Board Local Information Security Officers include but are not limited to:

a. Assign a designated backup in the office to perform Board LISO duties when the Board LISO is not available.

b. Provide each Board user, including staff of special contractors without an assigned LISO, with sufficient training and support reference materials to allow them to properly protect information resources. The Board LISO must ensure Workforce Solutions Information Security Standards and Guidelines are available to staff.

c. Assures the appropriate security documents are signed and the User successfully completes the on-line trainings.

d. Retain the usage agreement signed by the user when first hired.

e. Reset passwords for Board staff and RACF office LISO system users attached to the Board administrative.

f. Submit requests to RACF administration to add and remove local LISO's.

g. Responsible for updating Workforce Solutions user database directly for Users attached to the board office and for updating Workforce Solutions user database with information transmitted from the Office or Contractor LISO's. In addition, the Board LISO takes steps to add access to the appropriate

Workforce Solutions databases as requested.

h. Reconcile the Users recorded in Workforce Solutions user database attached to the board to the Users stationed at the board.

i. In the event a user managed by the Board LISO will no longer be working at the board office, the Board LISO must update Workforce Solutions database before the end of the last workday of that User at that location.

j. If the User will no longer be employed by the board, the Board LISO must remove location and employer attachments and note the removal of access to data systems.

k. Coordinate with H-GAC Data Services Department if a User needs a Workforce Solutions email or any systems managed by HGAC.

4. PASSWORDS

The Workforce Solutions Password Standard establishes rules related to the User authentication process, including the creation, distribution, safeguarding, termination, and reclamation of those mechanisms. Exceptions to this policy may be allowed temporarily for certain legacy systems.

1. All passwords must comply with the Workforce Solutions Password Standard in force at the time of creation.

2. User chosen passwords must adhere to a minimum length and format as defined by current password guidelines:
    a. Contain at least one upper case letter, one lower case letter, and one number,
    b. Are at least 8 characters in length,
    c. Passwords must not have consecutive duplicate characters such as 99 or BB,
    d. Passwords must not have consecutive-count numbers or letters, such as 1234 or ABCD,
    e. Passwords cannot include words in any dictionary including slang, dialect, jargon, etc.,
    f. Passwords are not based on personal information such as names, birthdates, etc.,
    g. Passwords should be easily remembered, and
    h. Passwords should never be the same as the User ID.

3. Users must not write down passwords and store them near their computers.

4. Users must not share their passwords.

5. If a password's security is in doubt, it must be changed immediately.

6. If a User suspects password has been compromised, it must be changed immediately, and their supervisor notified of the suspected compromise.

5. SENSITIVE PERSONAL INFORMATION (SPI)

Sensitive Personal Information (SPI) is information that can be used to distinguish or trace an individual's identity, either alone or when combined with other confidential or identifying information that is linked or linkable to a specific individual. Examples of SPI include, but are not limited to: SSN, addresses, home phone numbers, birthdates, medical and disability-related information, financial information, and computer passwords.

Authorized users of Workforce Solutions Information Resources are responsible for the security of SPI stored or transmitted electronically or in print form. Any electronic device or document containing SPI must be encrypted or otherwise protected. Do not allow unauthorized individuals to view SPI on any printed or electronic media. Please see the chart below for the following is the minimal expectation for SPI barriers.

To protect SPI stored or transmitted electronically or in print form, contractors must ensure:

- Unauthorized individuals cannot access or view SPI in print form.

- Store documents containing SPI in a locked location when not actively using the documents.

- Adequate disposal, i.e., shredding, of SPI in print form.

- Maintaining SPI and other confidential information in accordance with TWC standards for information security set forth in WD Letter 02-18, issued April 15, 2024, Change 1, and titled "Handling Sensitive Personal Information and Other Confidential Information - Update" and WD-17-07, issued April 16, 2024, and titled “Storage and Use of Disability-Related and Medical Information - Update.

- SPI and other confidential information is stored in an area that is physically safe from access by unauthorized individuals;
- A tracking log of SPI stored off-site is maintained;
- If records are stored off-site, the storage facility verifies that it can maintain the security of confidential and sensitive files by meeting the two-barrier minimum standard;
- Electronic media and removable media are kept in a secured area under the immediate protection and control of an authorized employee or are locked in a secure place. When not in use, they must be returned promptly to a proper storage area or container;
- Any electronic and removable media containing SPI or confidential data must be securely encrypted while in transit or at rest.
- SPI is stored on hard disks only if office-approved security access control devices (hardware and software) have been installed; are receiving regularly scheduled maintenance, including upgrades; and are actively being used.
- Prohibit transportation of SPI, in electronic or print format, from a Workforce Solutions location unless authorized by H-GAC Contract Liaison or other Workforce Board staff.

SPI Barrier Expectations

Area	During Hours of Operation	After hours	Additional Barrier
Restricted*	Staff serves as an escort to all visitors and monitors visitor activity	Locked building, security guard	Out of plain sight
Secured	Authorized staff only	Locked building, security guard	Locked; access control
Public	Staff monitored	Locked building, security guard	Locked; staff distributes documents

*As identified by signage such as "Employees Only"

Workforce Solutions staff and contractors must be aware that failure to comply with all SPI requirements, and failure to take appropriate action to prevent any improper use or disclosure of SPI and other confidential information for an unauthorized purpose, is subject to sanctions or other actions as deemed necessary by TWC, up to and including termination of contracts and recoupment of funds, or criminal or civil prosecution. Workforce Solutions staff and contractors **must hold accountable** individuals who improperly use or disclose SPI and other confidential information for unauthorized purposes.

Required Compliance Reviews

Each contractor must conduct Information Security reviews at each location where there is Sensitive Personal Information (SPI), in physical or electronic format. Contractors will use the Workforce Solutions Information Security Review report found in the Information Security section at this link Information Systems Onboarding (sharepoint.com)

- Daily Reviews - Authorized staff will conduct daily reviews. If the daily reviews for the location do not reveal violations of Information Security Policies and Procedures for 20 consecutive business days, reviews for that location will step to weekly reviews.

- Weekly Reviews - Authorized staff will conduct weekly reviews. If the weekly reviews for the location do not reveal violation of Information Security Policies and Procedures for thirteen consecutive weeks, reviews for that location will step to monthly reviews.

- Monthly Reviews - Authorized staff will conduct monthly reviews.

If a reviewer identifies a violation of Information Security Standards and Guidelines, at any stage, the review process begins again at the Daily Review level.

Contractor must designate staff to maintain the Information Security Review Document. Each location must maintain the review documents for that location.

6. E-MAIL USE

The growth of use and the increase in vulnerabilities related to electronic communications has seen a corresponding increase in the need for policies governing the use of, and protections

directed to, those communications. The e-mail standards for staff and authorized users include:

1. The following activities are prohibited:
    a. Sending e-mail that is intimidating or harassing,
    b. Using e-mail for conducting personal business,
    c. Using e-mail for purposes of political lobbying or campaigning,
    d. Violating copyright laws by distributing protected works,
    e. Posing as anyone other than oneself when sending e-mail, except when authorized to send messages for another when serving in an administrative support role, as a delegate, or when using a "pool" account,
    f. Using unauthorized e-mail software,
    g. Sending or forwarding chain letters,
    h. Sending unsolicited messages to large groups except as required in conducting department business,
    i. Sending excessively large messages or enclosures, and
    j. Sending or forwarding e-mail that is likely to contain malicious code

2. All staff or user activity on Workforce Solutions information resources assets is subject to logging and review.

3. Staff and users have no right to privacy with regard to e-mail. Management has the ability and right to view employees' e-mail. Recorded e-mail messages are the property of Workforce Solutions. Thus, they are subject to the requirements of the Texas Public Information Act and the laws applicable to state records retention.

4. Workforce Solutions IT management:

    a. In consultation with other Workforce Solutions management, reserves the right to filter and/or block any e-mail item, inbound or outbound, which is determined to place Workforce Solutions, its systems and/or networks at an unacceptable level of risk.

    b. Retains the right to examine any non-encrypted e-mail item for subject and/or content to determine e-mail abuse.

    c. Shall, in consultation and aligned with industry best practices, filter and/or block any attachment or enclosure to any e-mail that places Workforce Solutions systems and/or networks at an unacceptable level of risk.

d. May identify a listing of key words and phrases that are common to "spam" and shall filter those e-mail words and phrases on all inbound e-mail items in order to prevent those items from entering Workforce Solutions systems and/or networks.

5. All staff and users of Workforce Solutions e-mail systems shall:

a. Ensure confidential Workforce Solutions material transmitted over external network connections is encrypted or otherwise protected as required by rule or law. Where possible, staff should identify customers in correspondence by TWIST, WIT, or system ID other than the Social Security Number.

b. Use email encryption when sending emails with Sensitive Personal Information (SPI). S P I should not be sent in the subject or body of an e-mail in clear text. If email encryption is not available, then staff must manually encrypt all SPI documentation. Email encryption can be added by typing "[securemessage]" anywhere in the subject line of your message. If staff needs to manually encrypt, please refer to the program's default encryption method (ex. Word, Excel, PDF).

c. Ensure that SPI is not transmitted to unauthorized users. All SPI and other confidential data transmitted via email or stored on Laptop/notebook computers, CDs, DVDs, thumb drives, smart phones, etc., must be encrypted using **FIPS 140-2 standards.**

d. Not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of Workforce Solutions or any unit of Workforce Solutions unless authorized (explicitly or implicitly) to do so.

e. Not send, forward or receive confidential Workforce Solutions information through non-Workforce Solutions approved e-mail accounts. They may not use non- Workforce Solutions email accounts to perform their official Workforce Solutions duties.

f. Not send sensitive or confidential information in the body of an email that is sent to other non-Workforce Solutions recipients.

g. Refrain from forwarding multiple copies of received e-mail items that are

not directly connected to the Workforce Solutions business process without the explicit consent of the recipient.

h. Use caution when sending mass emails to customers. Users must always use the Blind Carbon Copy (BCC) function when sending such emails.

i. Use caution in selecting the Reply to All" function of Workforce Solutions e-mails client application.

j. Not send, forward or store confidential Workforce Solutions electronic information utilizing non-Workforce Solutions owned mobile devices such as, but not limited to, laptop/notebook computers, personal data assistants or other hand-held devices, two- way pagers or digital/cellular telephones without written permission.

k. Refrain from signing up for "mailing lists" or registering for non-agency related events or websites using their Workforce Solutions e-mail address. Users shall also refrain from posting to public newsgroups or "web boards", blogs, etc. using their Workforce Solutions e-mail address.

I. Not publish their Workforce Solutions e-mail address on any internet website outside the authority of Workforce Solutions.

m. Not access any Workforce Solutions databases outside designated office locations unless authorized by management.

n. Provide system credentials to the assigned staff and their supervisor.

6. Staff using Texas Educating Adults Management System (TEAMS) must comply with all TWC requirements and under no circumstance will SPI be released except in accordance with Family Educational Rights and Privacy Act (FERPA).

7. All new laptop and notebook computers must have encrypted hard drives.

7. IMAGING DEVICES

The Workforce Solutions Imaging Devices Security Standard establishes those rules necessary to mitigate risks associated with the increased use of devices that have the capability to capture images for storage and/or transmission. Such devices include, but are not limited to, Cellular Telephones with camera capabilities (built-in or attached), Personal Digital Assistants (PDA) with camera capabilities (built-in or attached), Laptop/Notebook Computers with camera capabilities (build-in or attached) and/or Digital cameras, digital video recording devices of any sort.

1. The use of such devices is allowed to the extent that there is a Workforce Solutions business reason. In any case the owner is responsible for the protection of all sensitive, confidential, or private information to which employees, contractors, vendors, visitors, or others may have access either as a granted right or by accidental exposure.

2. Any device that has the capability to capture, store, and/or transmit an image of any document, person, or environment (still or in motion) under the authority of this standard shall have the image capturing function disabled while in restricted Workforce Solutions environments.

3. Exemptions to this policy include dedicated document scanning devices and other equipment designed specifically to capture document images for archival storage.

4. Requests for any other exemptions to this policy must be approved in writing prior to use of the device. The exemption approval authority shall be the H-GAC.

5. Machines programmed to receive faxes are in a secured or restricted area.

8. INTERNET/ INTRANET/ EXTRANET USE

For the purpose of this standard, the term Internet shall include Intranet and/or Extranet. This standard includes:

1. Software for browsing the Internet is provided to Users for business, research and allowed incidental/limited personal use only.

2. All software used to access the Internet must be part of Workforce Solutions standard software suite or approved for use by the appropriate Workforce Solutions authority.

3. All software used to access the Internet must incorporate vendor provided security patches.

4. All software used to access the Internet shall be configured to provide an appropriate level of protection to Workforce Solutions systems and networks.

5. No offensive or harassing materials may be made available via any Workforce Solutions Internet site.

6. No personal commercial advertising may be made available via any Workforce Solutions Internet site.

7. Internet access provided by Workforce Solutions may not be used for personal gain or non- Workforce Solutions personal solicitations.

8. Confidential Workforce Solutions material (including SPI) transmitted over external network connections or saved in Cloud Storage authorized by Workforce Security must be encrypted.

9. Users may not install or use encryption software on Workforce Solutions computer resources that has not been reviewed and approved for use by Workforce Solutions Information Security. Users may not use encryption keys that are unknown to their supervisor.

10. All electronic files are subject to the same records retention rules that apply to the same document in non-electronic formats.

11. Incidental personal use of Internet access is permitted but must not inhibit the use of network resources for business purposes.

12. Incidental personal use of Internet access is restricted to Workforce Solutions approved Users; it does not extend to family members or other acquaintances or visitors to any Workforce Solutions office.

13. Incidental use must not interfere with the functionality of any Workforce Solutions system or network or the normal performance of an employee's work duties.

14. Incidental use must not result in any direct costs to Workforce Solutions.

9. PRIVACY POLICIES

The purpose of Workforce Solutions Privacy Standard is to clearly communicate Workforce Solutions Information Services Privacy expectations to Users of Workforce Solutions Information Resources. The standard includes:

1. Internal Users of Workforce Solutions information resources should have no expectation of privacy with respect to the use of those resources.

2. External Users of Workforce Solutions information resources should have the expectation of privacy, except in the case of suspected wrongdoing, with respect to Workforce Solutions information resources. However, aggregate information from the analysis of logs may be used without compromising individual privacy.

3. Electronic files created, sent, received, or stored on Workforce Solutions owned, leased, administered information resources, or otherwise under the custody and control of Workforce Solutions are not private and may be accessed by Workforce Solutions IT employees at any time without knowledge of the resource User or Owner.

4. To enforce security, Workforce Solutions IT may log, review, and otherwise utilize any information stored on or passing through Workforce Solutions information resources.

5. To enforce security, Workforce Solutions IT may capture User activity such as telephone numbers dialed, or web sites visited.

10. MAINTAINING A SECURE ENVIRONMENT

Workforce Solutions staff handle the personal, confidential information of our customers. It is essential that staff act to protect the customers' identity information. Each contractor must develop local procedures that protect customer identity information in the workplace.

1. Staff shall secure customer identity information so that other customers do not have access to it, whether hard copy or electronic format.

2. Confidential information should be secured when not attended-in locked cabinets or locked rooms.

3. Shred documents that include customer identity data that is not filed.

4. Laptops, portable storage devices, mobile phones, and files containing SPI must not be left in a vehicle unattended for significant periods of time. If SPI must be left in a vehicle for a short time, the SPI must be placed in the trunk, if available, or out of plain sight. The vehicle must be locked. Staff transporting files must immediately remove and secure files when they arrive at their destination.

5. Documents with customer identity data must not be in plain view, nor should these documents be in an unsecured area. Drawers and file cabinets should be locked when not attended.

6. Documents with customer identity data that is transported on a laptop or other portable storage device must be password protected.

7. Ensure staff do not share passwords.

8. Ensure staff log off of computers when leaving them unattended.

9. Ensure customer data is transmitted over the telephone only to the customer after establishing the identity of the customer.

10. All SPI removed from an office must be documented using a sign-out and sign-in protocol or other logging method that maintains a record of custody.

11. REMOVABLE MEDIA

The Workforce Solutions Removable Media Security Standard establishes those rules necessary to protect the data and the networks of Workforce Solutions and satisfies compliance requirements of state and federal rule and law with regard to disposal and reuse of media that contain protected, confidential and/or sensitive information. These devices include, but are not limited to:

- Diskettes, tapes and/or compact disks
- Memory cards/sticks used in various portable digital devices
- Firewire/USB "Flash"/Key/Pen/Thumb drive memory devices
- Portable mass storage devices
- Personal audio/video players

Sensitive Workforce Solutions data stored on removable media must be encrypted

1. In the event of loss or theft of the removable media, the description of the data and index or table of contents must be provided with the report of loss or theft.

2. All removable media must be scanned for malicious code content prior to use in Workforce Solutions systems or networks.

3. Reuse or disposal of removable media will follow a data sanitization guideline in compliance with NIST Special Publication 800-88, to assure removal of any electronic protected, confidential and/or sensitive information: http://nvlpubs.nist.gov/nistpubs/Specia1Publications/NIST.SP.800-88r1.pdf

12. WIRELESS COMPUTING

Workforce Solutions establishes these rules necessary to mitigate risks associated with the use of devices that have the capability to connect to networks without the use of wires or cables, such as but not limited to:

- Wireless base and/or access points (built-in or free-standing)
- Personal Digital Assistants (PDA) or cellular/digital PDA-based telecommunication devices (smart phones or PC phones) with wireless connectivity capabilities (built-in or free-standing)
- Laptop/Notebook/tablet computers with wireless connectivity capabilities (built-in or free-standing)

- Wireless transmitting and/or receiving devices used to transfer audio, video, image, or data of any sort.

The User is responsible for the protection of all sensitive, confidential, or private information to which they may have access either as a granted right or by accidental exposure.

All employees, providers, and vendors are prohibited from using or installing any device which functions in wireless mode in order to access data, transfer data or connect in any manner to Workforce Solutions networks or systems without the approval and assistance of Workforce Solutions IT staff.

13. ONE DRIVE

OneDrive for Business is a personal online storage space hosted at Microsoft data centers. It is provided to employees with a @wrksolutions.com email domain and is included in your Office 365 subscription. The Workforce Solutions administrator has activated this service so that you can use it within Workforce Solutions intranet to store work files securely and with ease. This policy outlines the acceptable use of Microsoft OneDrive for Business. Inappropriate use compromises the Workforce Solutions network systems and exposes it to risks that include virus attacks and legal issues.

1. Security and Proprietary Information
   Security practices must be followed to ensure that OneDrive for Business is used properly in conducting Workforce Solutions business. The following data are considered confidential, and storage is strictly prohibited on OneDrive for Business:

   - Social Security Numbers
   - Credit Card numbers
   - Bank account information
   - Sensitive Personal Information (SPI)
   - Protected Health Information (PHI)
   - Password credentials
   - Data sets which are subject to confidentiality restrictions, copyrighted, and/or licensing, included in the Data Map inventory

2. Data Responsibility and Recovery

   a. Employees are responsible for adhering to Workforce Solutions retention

policies and managing their data responsibly.

b. To protect the agency from data spillage, only share with specific individuals, never with "everyone" or "public".

c. Use caution when sending links to shared folders. Like e-mail attachments, links can be forwarded with the consequence that information can be shared to unintended recipients.

d. OneDrive for Business is not intended to be used as a permanent storage. When a document has been finalized, it must be moved to SharePoint or the network shared storage.

e. All files saved to OneDrive will be treated in a same manner to files saved on a Workforce Solutions computer.

f. There will not be any backups performed by Data Services on these files. If you accidentally delete a file or folder in OneDrive, you may be able to recover it later from the OneDrive recycle bin. Items in the recycle bin are automatically deleted after 90 days.

14. INFORMATION SYSTEMS SECURITY

14.1 INTRODUCTION

This policy manual outlines the agency wide information security policies and procedures for Workforce Solutions. All employees, contractors, volunteers, and any other Workforce Solutions personnel granted access to Workforce Solutions' information resources and data must understand and follow all policies stated herein.

14.1.1 PURPOSE AND BENEFITS

This manual is to establish specific information security policies, procedures, and responsibilities for the management and control of the agency's information assets, protocols, and procedures. The policies in this manual apply to all information assets processed and/or stored on equipment that is owned or leased by Workforce Solutions including stand-alone and networked systems, telecommunications systems, remote access, client-server environments and gateways to non--agency systems.

Any program may, based on its individual business needs and specific legal and federal requirements, exceed the security requirements put forth in this document, but must, at a minimum, achieve the security levels required by this policy.

This policy acts as an umbrella document to all other security policies and associated standards. This policy defines the responsibility to:

- Protect and maintain the confidentiality, integrity and availability of information and related infrastructure assets.
- Manage the risk of security exposure or compromise.
- Assure a secure and stable information technology (IT) environment.
- Identify and respond to events involving information asset misuse, loss, or unauthorized disclosure.
- Monitor systems for anomalies that might indicate compromise.
- Promote and increase the awareness of information security.

Failure to secure and protect the confidentiality, integrity, and availability of information assets in today's highly networked environment can damage or shut down systems that operate critical infrastructure, financial and business transactions, and vital government functions; compromise data; and result in legal and regulatory non-compliance.

This policy benefits programs and services by defining a framework that will assure appropriate measures are in place to protect the confidentiality, integrity, and availability of data; and assure staff and all other affiliates understand their role and responsibilities, have adequate knowledge of security policy, procedures and practices and know how to protect information.

14.1.2 ROLES AND RESPONSIBILITIES

Contract management are responsible for the development, outline, update, and enforcement of the Workforce Solutions information security policies. All policies and protocols created are to be presented to and approved by Workforce Solutions Board contract manager.

14.1.3 SCOPE

This policy encompasses all systems, automated and manual, for which the agency has administrative responsibility, including systems managed or hosted by contractors, consultants and third parties on behalf of the agency. It addresses all information, regardless of the form or format, which is created or used in support of business activities.

14.2 POLICIES

The goal of the policies section is to define policy and requirements as defined and adopted by

Workforce Solutions. This section is divided into five functions of the cybersecurity framework defined by the National Institute of Standards and Technology (NIST 800-53): Identity, Protect, Detect, Response, Recovery.

14.2.1 IDENTITY

The Identify function assists in developing an organizational understanding to managing cybersecurity risk to systems, people, assets, data, and capabilities. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs.

14.2.1.1 ENTERPRISE SECURITY POLICY, STANDARDS AND GUIDELINES

Introduction

The purpose of defining an enterprise-wide security policy, standards, and guidelines is to maintain the organization's security policy framework, standards, and guidelines, it defines the acceptable use policy for agency information resources and contributes to the definition of enterprise standards and secure configuration standards to ensure alignment to security specifications and risk management requirements.

Policy

The agency shall develop an enterprise-wide security policy defining the standards and guidelines used to protect the organizations information, assets, employees, and services. The policy shall align itself with the agency's business objectives while meeting the necessary security requirements as defined by this policy and as required by our granters and funding agencies. This policy shall be presented to contract management for review and approval and shall be officially endorsed by the Executive staff of the agency. The policy shall be updated by contract management on an annual basis and as needed.

14.2.1.2 SECURITY OVERSIGHT & GOVERNANCE

Introduction

Security oversight and governance is the set of responsibilities and practices exercised by the board and/or executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise's resources are used responsibly.

Policy

The agency shall establish a committee consisting of members from the Executive and Leadership Team. The Committee shall review major information technology projects and initiatives presented by the senior management staff. The Committee, along with senior management staff, shall evaluate the Information Security Standards and Guidelines upon update and provide updates to the policy to best integrate with the agency's goals and business requirements.

14.2.1.3 INCIDENT RESPONSE TEAM

Introduction

In the event of a cybersecurity incident, is important to have the response team, roles, and responsibilities clearly defined to minimize any confusion during the response and recovery process. The appropriate members of the agency and leadership need to be involved to ensure the correct decisions are made and all possible resources are available.

Policy

The Director will chair an Incident Response Team to handle the breach or exposure. The team will include members from:

- Appropriate contract management
- Workforce Solutions Board contract manager
- H-GAC Information Security Manager
- The affected program or department that uses the involved system or output or whose data may have been breached or exposed
- Additional departments based on the data type involved
- Additional individuals as deemed necessary by the Director

14.2.1.4 INFORMATION SECURITY RISK MANAGEMENT

Introduction

Information security risk management is the assessment and evaluation of risk within the information resources and technology to ensure that business operations can deliver programs and services efficiently and effectively within acceptable tolerances and potential negative outcomes.

Policy

The agency shall formally identify and document all programs and services held under Workforce Solutions and its contractors, vendors, and consultants. Upon identification, the agency program stakeholders shall formally identify business risks, business appetite for those risks, and negative outcomes if the named risks are encountered. Entities are responsible for selecting the risk assessment approach they will use based on their needs and any applicable laws, regulations, and policies. Risk assessment results, and the decisions made based on these results, must be documented.

14.2.1.5 DATA/APPLICATION MAPPING AND OWNERSHIP

Introduction

Data/Application Mapping and Ownership is an important part of the information security model. It lays out the applications and data that the organization owns and uses, and it defines who is responsible for the data and application and maintaining and protecting it from the business perspective.

Policy

Workforce Solutions contractors shall identify all applications and data sets used by the agency and the owner(s) or point of contact(s) of those assets. This identification should be recorded for the agency to reference and be reviewed on an annual basis. The organization will designate a staff that shall be tasked with coordinating with the stakeholders to review and amend the list.

14.2.1.6 DATA CLASSIFICATION AND PRIVACY POLICY

Introduction

Data classification and privacy policy provides a framework for securing the agency's data from risks including, but not limited to, unauthorized destruction, modification, disclosure, access, use, and removal. This policy outlines measures and responsibilities required for securing data resources and complying with state and federal law.

Policy

Agency data shall be classified into three different categories:

- **Confidential and Protected Data**
  - **Protected Health Information (PHI)** - Any information about health status, provision of health care, or payment for health care that is created or collected and can be

linked to a specific individual.

- **Sensitive Personal Information (SPI) -** Any information that relates to an identified or identifiable living individual. Separate pieces of information, which together could lead to the identification of a particular person, also constitute personal data.

- **Licensed Data**
  Data that is specifically protected by copyrights, licenses, or other confidentiality agreements.
- **Public Domain Data**
  All agency data, unless specifically exempted by statute, licensing, copyrighting, and confidentiality agreements or are otherwise designated as protected, shall be considered public domain data.

Contract management shall be advised of data sets which are protected and are not to be distributed outside of the agency without authorization from the department director in custody of the data. Any use or attempt to use the protected data sets without appropriate authority may result in disciplinary actions or possible termination. Furthermore, unauthorized distribution of the protected data may subject the offender to civil and/or criminal prosecution.

14.2.1.7 CONTRACTORS AND CONSULTANTS

Introduction

Contractors and consultants are an integral part of the daily operation, function, and development of the agency programs and services. Often, they require the equivalent access to information and resources as the staff of the agency and should be treated in the same manner as agency staff.

Policy

All entities who have access to agency data, network, and/or resources shall be required to adhere to the same security requirements and practices defined within this policy. All accounts created for contractors or consultants shall be formally requested should be easily identified within the system they have access to.

14.2.1.8 ASSET TRACKING AND ASSIGNMENT

Introduction

Tracking of assets such as computer hardware, appliances, software, and other equipment helps to ensure all devices are accounted for and are properly patched and updated for vulnerabilities. An inventory of assets also ensures that equipment is properly disposed of, and the appropriate personnel are made aware of the disposal.

Policy

Qualifying assets in accordance with the "Contract Management Standards and Property" shall be properly tagged and inventoried in an asset tracking system. Document details can be found on the Workforce Solutions website at Contract Management - Workforce Solutions (wrksolutions.com).

14.2.1.9 TECHNOLOGY HARDWARE/SOFTWARE/SERVICES ACQUISITION

Introduction

As the agency's business model and function evolves, new technology hardware, software, and services are needed to meet those needs. It is important that the procurement of resources are done in an appropriate manner to ensure that they meet the agency's needs and requirements. Cost, implementation, intended function, security, robustness, and adaptability all need to be considered when bringing in those new resources.

Policy

All purchases of technology resources, shall follow appropriate guidance in the "Contract Management Standards and Property" at Contract Management - Workforce Solutions (wrksolutions.com).

14.2.1.10 VULNERABILITY ASSESSMENT

Introduction

Through routine patching and updates, many threat vectors can be mitigated and prevented. However, implementation of new software and services, newly developed internal applications, and modifications to the network and endpoint configurations, can allow for unintended behavior and give the threat actor an opportunity for exploitation. A routine scan and inspection of the organization's applications and resources by an outside entity can help detect these unforeseen exploits. Penetration testing can also cover resources outside of the general technology space and include areas such as physical entry to the facility, staff manipulation and social engineering, and executive impersonation. Vulnerability assessment can cover a wide gamut of technologies, services, and resources. The organization should determine how wide of a scope the penetration and vulnerability testing should cover.

Policy

The agency hosting software or services shall conduct a vulnerability assessment of its public and

private network and resources on an annual basis. The assessment shall be conducted by a third-party vendor, consultant, or service provider.

Additionally, any service providers that have publicly accessible resources must conduct a vulnerability assessment or use a different third-party service.

Note: The CISA Cyber Hygiene Services is a free service available at cisa.gov and can be used to fulfill this requirement.

14.2.2 PROTECT

The Protect Function outlines appropriate safeguards to ensure delivery of critical infrastructure services. The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event.

14.2.2.1 DATA ENCRYPTION AND CRYPTOGRAPHY

Introduction

Data encryption ensures that data is only readable by the intended audience. Unauthorized viewers should not be able to access, read, or decode the data without possessing the correct decryption key or permissions.

Policy

Workforce Solutions specifies the following data encryption requirements:

- All devices shall have their data encrypted using industry standard encryption standards and methods. Mobile devices such as laptops, tablets, smart phones, and any other portable devices shall have their storage medium encrypt the data that is written to it.
- All portable storage mediums such as thumb drives, external drives, and USB storage devices must be encrypted prior to use and approved by the agency management. These devices shall not contain any data that is sensitive, private, or personally identifiable in nature.
- All information that is deemed sensitive, private, or personally identifiable shall be transmitted using agency adopted and approved methods. These methods must ensure that the data is encrypted using industry accepted standards. This includes, but not limited to email, file sharing services, file storage services, document management systems, and web and cloud services.

14.2.2.2 DATA BACKUP

Introduction

Data backup is a vital process to ensure the agency's data is intact, available, and secure. In the event where Workforce Solutions systems are compromised, tampered, degraded, or destroyed, systems should be recoverable from any one of the data backup mediums, depending on the circumstances and urgency of the situation.

Policy

For agencies hosting software or services: Data backup should follow the well-known and industry best practice of the 3-2-1 Rule:

- There should be three (3) copies of data
- On two (2) different media
- With one (1) copy being off-site.

The backup target media or backup strategy should provide a means to mark the data immutable or be "air gapped" to prevent data deletion by privileged accounts.

14.2.2.3 DATA STORAGE AND TRANSMISSION

Introduction

Data storage is the retrievable retention of data. Electronic, electrostatic, or electrical hardware or other elements (media) into which data may be entered, and from which data may be retrieved. Data transmission is the process of sending digital or analog data over a communication medium to one or more computing, network, communication, or electronic devices. This storage and transfer must be protected in a manner that will preserve the data against unauthorized access, modification, and destruction, whether intentional or accidental.

Policy

Any electronic data that is defined to contain sensitive, confidential, or restricted information shall be stored on a medium or device that is able to provide industry standard encryption, protection, and redundancy methods.

Data that is to be transmitted outside of the private network of the agency shall be sent using approved methods that meet industry standards for encryption and protection methods.

Data that is identified to not be of sensitive, confidential, or restricted in nature do not require

encryption protection but should still be stored and transmitted on a medium that provides redundancy protection.

14.2.2.4 DATA RETENTION

Introduction

Data retention policy is a recognized and proven protocol within an organization for retaining information for operational use while ensuring adherence to the laws and regulations concerning them. The objectives of a data retention policy are to keep important information for future use or reference, to organize information so it can be searched and accessed at a later date and to dispose of information that is no longer needed.

Policy

The programs and services owners and stakeholders shall identify the data retention requirements they are required to adhere to as specified by their grantor, funding agencies, and any governing bodies and laws applicable. Programs and services shall also develop plans to properly manage their data and ensure all data is retained as required and deleted or destroyed when appropriate.

14.2.2.5 DATA DESTRUCTION AND MEDIA SANITIZATION

Introduction

Proper data destruction and media sanitization are necessary to ensure application configuration and data are not exposed to unauthorized parties. The issue of media disposal and sanitization is driven by the information placed intentionally or unintentionally on the media. Electronic media used on a system should be assumed to contain information corresponding with the security categorization of the system's confidentiality. If not handled properly, release of these media could lead to an occurrence of unauthorized disclosure of information. This policy establishes rules necessary to protect the data and the networks of Workforce Solutions and satisfies compliance requirements of state and federal rule and law with regard to disposal of media that contain protected, confidential and/or sensitive information.

Media types may include but not limited to:

- Hard disk drives (external or internal)
- Backup tapes
- Optical disks of any type (CD, DVD, Blu-Ray, Magneto Optical, WORM etc.)
- Diskettes
- Memory cards/sticks
- Firewire/USB "Flash"/Key/Pen/Thumb drive memory devices
- Portable mass storage devices

- Audio/video players/recorders

Policy

Prior to the disposal or handoff of electronic storage media, it is required to remove all data on the system in accordance with NIST 800-88 guidelines. To support this policy, contractors must follow the structured data sanitization process outlined below.

Data Destruction and Sanitization Procedures

The following procedures are designed to guide organizations in securely erasing data from electronic media:

Level 1: Basic Data Cleaning (Clear)

- **Step 1**: Identify the media type (e.g., HDD, SSD, optical disk).
- **Step 2**: Backup any necessary data before proceeding.
- **Step 3**: Encrypt the hard drive to add an extra layer of security.
- **Step 4**: Delete the encryption keys to render the encrypted data inaccessible.
- **Step 5**: Clear the data using software tools to overwrite all storage areas of the media. For PCs, perform a reset using the "Remove files and clean the drive" option:
    - **For Windows**: Go to *Settings > Update & Security > Recovery > Reset this PC > Remove everything > Remove files and clean the drive.*
    - **For macOS**: Use Disk Utility in Recovery Mode to erase the disk with security options set to ensure thorough cleaning.
- **Step 6**: Verify the erasure with a data recovery tool.
- **Step 7**: Document the process, including the date, method used, and verification results.

Level 2: Intermediate Data Cleaning (Purge)

- **Step 1**: Identify the media and data sensitivity.
- **Step 2**: Backup necessary data.
- **Step 3**: Purge the data using cryptographic erasure or degaussing.
- **Step 4**: Verify the erasure using data recovery tools.
- **Step 5**: Document the process, detailing the encryption, key deletion, or degaussing.

Level 3: Advanced Data Cleaning (Destroy)

- **Step 1**: Identify the media and data sensitivity.

- **Step 2**: Backup necessary data.
- **Step 3**: Arrange for physical destruction by a certified media destruction company.
- **Step 4**: Obtain a certificate of destruction and document the process.

Note: Organizations are required to select the appropriate level of sanitization based on the sensitivity of the data stored on the media

14.2.2.6 CLOUD COMPUTING STANDARDS AND REQUIREMENTS

Introduction

Cloud computing services can vary greatly on the platform it is hosted on, how the application is developed, and the protections implemented to keep data and access secure. It is important that any cloud services we adopt and implement, that they meet or exceed a baseline of requirements. These requirements have been defined at the State level through the TX-RAMP programs.

Policy

The agency shall prioritize any cloud computing services, as defined by the NIST SP 800-145 document, to meet or exceed the Texas Risk and Authorization Management Program (TX-RAMP) requirements.

14.2.2.7 REMOTE ACCESS

Introduction

Remote access is defined to be the access of information or an application outside of the domain the resource(s) reside. This typically implies the access is provided through an intermediary such as a VPN portal, proxy, or firewall.

Policy

All personnel and consultants of the agency shall be required to formally obtain permission by the stakeholders of the resource, and access shall be implemented and controlled by Workforce Security staff in accordance with the access control policies defined.

14.2.2.8 GEOGRAPHIC RESTRICTIONS ON DATA ACCESS

Introduction

This policy is designed to protect sensitive state and federal data by restricting both the use of

organizational information systems and access to organizational information from outside of the United States. The purpose is to ensure that information systems and data remain secure and compliant with geographic restrictions in order to mitigate risks associated with unauthorized access.

Policy

Information systems, including but not limited to laptops, desktops, smartphones, tablets, and any hardware used to access, store, or process state or federal data, managed by Workforce Solutions contractors, vendors, and consultants, are prohibited from being taken outside the United States, including the 50 states and the District of Columbia. Additionally, access to organizational information, including state or federal data, is strictly prohibited from any location outside of the United States.

14.2.2.9 PERSONAL DEVICES

Introduction

On December 7, 2022, Governor Greg Abbott required all state agencies to ban the video-sharing application TikTok from all state-owned and state-issued devices and networks over the Chinese Communist Party's ability to use the application for surveilling Texans. https://gov.texas.gov/uploads/files/press/State_Agencies_Letter_I.pdf. 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.

In addition to TikTok, Workforce Solutions may add other software and hardware products with security concerns to this policy and will be required to remove prohibited technologies which are on the DIR prohibited technology list. Prohibited Technologies | Texas Department of Information Resources. Throughout this Policy, "Prohibited Technologies" shall refer to TikTok and any additional hardware or software products added to this Policy.

Policy

Except where approved exceptions apply, the use or download of prohibited applications or websites is prohibited on all Workforce Solutions devices, including cell phones, tablets, desktop and laptop computers, and other internet capable devices.

The Workforce Solutions must identify, track, and control program 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.

Workforce Solutions must manage all program owned mobile devices by implementing the security controls listed below:

a. Restrict access to "app stores" or non-authorized software repositories to prevent the install of unauthorized applications.
b. Maintain the ability to remotely wipe non-compliant or compromised mobile devices.
c. Maintain the ability to remotely uninstall un-authorized software from mobile devices
d. Deploy secure baseline configurations, for mobile devices, as determined by Workforce Solutions.

1. Personal Devices Used for Workforce Solutions Business

If an employee or service provider has a justifiable need to allow the use of personal devices to conduct Workforce Solutions business, the service provider may submit to the Board staff for review their plan to implement a mobile device management platform that complies with the considerations of objective #2 of the Statewide Plan for Preventing Use of Prohibited Technologies.

Employees and contractors may not install or operate prohibited applications or technologies on any personal device that is used to conduct Workforce Solutions business. Workforce Solutions business includes accessing any Workforce Solutions owned data, applications, email accounts, non-public facing communications, Workforce Solutions email, VoIP, SMS, video conferencing, CAPPS, Texas.gov, and any other Workforce Solutions databases or applications.

2. Identification of Sensitive Locations

Sensitive locations must be identified, cataloged, and labeled by the agency. A sensitive location is any location, physical, or logical (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, sensitive personal data and 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.

3. Network Restrictions

DIR has blocked access to prohibited technologies on the Workforce Solutions network. To ensure multiple layers of protection, Workforce Solutions will also implement additional network-based restrictions to include:

a. Configure agency firewalls to block access to Workforce Solutions wide prohibited services on all agency technology infrastructures, including local networks, WAN, and

VPN connections.

b. Prohibit personal devices with prohibited technologies installed from connecting to agency or Workforce Solutions technology infrastructure or Workforce Solutions data.

c. Provide a separate network for access to prohibited technologies with the approval of the executive head of the agency.

4. Ongoing and Emerging Technology Threats

To provide protection against ongoing and emerging technological threats to the Workforce Solutions' sensitive information and critical infrastructure, DPS and DIR will regularly monitor and evaluate additional technologies posing concerns for inclusion in this policy.

DIR will host a site that lists all prohibited technologies including apps, software, hardware, or technology providers. The prohibited technologies list current as of January 23, 2023, can be found at Addendum A. New technologies will be added to the list after consultation between DIR and DPS. Please see linked site above.

Workforce Solutions will implement the removal and prohibition of any listed technology. Workforce Solutions may prohibit technology threats in addition to those identified by DIR and DPS.

5. Exceptions

Exceptions to the ban on prohibited technologies may only be approved by the executive head of Texas Workforce Commission. This authority may not be delegated. All approved exceptions to the TikTok prohibition or other statewide prohibited technology must be reported to DIR.

Exceptions to the policy will only be considered when the use of prohibited technologies is required for a specific business need, such as enabling criminal or civil investigations or for sharing of information to the public during an emergency. For personal devices used for state business, exceptions should be limited to extenuating circumstances and only granted for a pre- defined period of time. To the extent practicable, exception-based use should only be performed on devices that are not used for other state business and on non-state networks. Cameras and microphones should be disabled on devices for exception-based use.

14.2.2.10 ACCESS CONTROL

Introduction

Access control is the process of granting or denying specific requests for obtaining and using information and related information processing services.

Policy

Access controls shall be available and implemented on all applications, programs, and data sets

managed or owned by the agency. Access to these resources shall be formally submitted to the stakeholders of the resources. The program or data owner shall designate an authoritative contact who shall approve or deny access request. The implementation of the access shall be managed by another contact outside of owner. Revocation of access shall follow the same procedures as the granting of access.

14.2.2.11 CHANGE MANAGEMENT

Introduction

Change Management establishes a set of rules and administrative guidelines to manage changes in a rational and predictable manner. In addition, it provides for the necessary documentation of any changes made to reduce any possible negative impact to the users of systems. Changes include, but are not limited to implementation of new functionality, interruption of service, repair of existing functionality, removal of existing functionality, office openings, office closures, relocations, office manager changes, and contact information changes.

Policy

All changes to agency resources must be initiated formally through the process defined by Workforce Security. The process must include provisions to make and record the formal request, the person or group that completes the request, and the reproduceable logging of the change activity.

- No later than two weeks in advance of the closing, moving, or opening of a Workforce Solutions office or satellite office, the Local Information Security Officer (LISO) must:
    - Submit the Request for Change in Directory of Offices form (Y-9) (See Instructions) to H-GAC Board staff at WorkforceSecurity@wrksolutions.com.
- The LISO must also submit Y-9 form within 24 hours of reporting a change in management at an office.

14.2.2.12 SECURITY AWARENESS TRAINING

Introduction

To protect the agency's information resources, it is critical for employees to understand their responsibilities and accountability regarding information security. To achieve the agency's security goals, all Workforce Solutions employees are required to be trained on security policies, procedures, and technical security controls. The purpose of this policy is to define the agency's information cybersecurity awareness training program and to outline the plan and procedure for

its implementation and enforcement.

Policy

The cybersecurity awareness training program shall be conducted upon hire and annually in October. The content and training program shall meet the Texas state requirements as defined in HB 3834 and address the responsibilities and requirements of the cybersecurity training program.

Staff of agency programs and services that involve information of sensitive nature shall be required to attend additional security awareness training that includes agency specific policies and procedures with a focus on managing data of such nature.

14.2.2.13 IDENTITY MANAGEMENT AND AUTHENTICATION

Introduction

Managing access and rights is imperative in controlling unauthorized and unintentional viewing, copying, modifying, and deleting of data and resources. Utilizing a centralized identity management service will allow for a more convenient way to authenticate against services while ensuring the method of authentication adheres to industry standards and guidelines.

Policy

Identity management and authentication shall be implemented on all data sets and applications managed and utilized by personnel of the agency and by personnel of outside entities. The method of authentication shall incorporate industry standards including, but not limited to, encryption, multi-factor authentication, complex, rotating, and time limited passwords.

Additionally, all accounts with elevated privileges or roles will be required to have multi-factor authentication enforced on those accounts.

14.2.2.14 ENDPOINT SECURITY

Introduction

Endpoint security provides defense against many threats. It can act as both telemetry on networks notifying of malicious activity and as a response agent mitigating and preventing further intrusion into the network. The ability to monitor activities on the endpoints and report malicious activity is important for rapid detection and response. It can also serve to manage endpoints and harden its security profile by providing other features such as URL filtering, external media usage rules, data

loss prevention policies, etc.

Policy

All computing endpoints shall have installed a reputable end point security software and shall maintain updates to the agent and apply malware definitions as soon as it is available. Maintenance agreements and subscriptions for the security solution should never be allowed to expire and malware definitions go out-of-date. When appropriate, a centrally managed endpoint detection and response (EDR) tool or service will be the preferred security solution.

14.2.2.15 INTERNET CONTENT AND URL FILTERING

Introduction

The internet provides easy and convenient access to information and allows for easier planning for contingencies. As more services move to the cloud, work and productivity becomes increasingly dependent on it. However, it also allows easier access to malicious content, whether intentionally or unintentionally. Mechanisms that help prevent access to malicious resources are needed to protect us from this.

Policy

All desktops, laptops, and mobile devices managed by Workforce Solutions contractors, vendors, and consultants shall have a means of managing access to content on the internet and what URLs are accessed. Management of access should allow for granular control to internet resources by web address or URL, by categories of the content, and/or by the classification of the application. The point of control can be executed at the network level, device level, or at any other level that is appropriate for the situation or technology.

14.2.2.16 EMAIL FILTERING

Introduction

Email continues to be one of our most widely used communications tool. As such, it also remains as one of the largest targets for malicious and threat actors to gain access and infiltrate networks. Email protocol is still a very insecure at its core, and thus requires many layers of protection to filter out malicious content and nefarious activity.

Policy

Email services behind all domains managed by Workforce Solutions shall have an email filtering and protection services applied to all inbound and outbound messages. The filtering and protection services should implement modern industry standards that include, but not limited to, spam and malicious content filtering, attachment file scanning, malicious link scanning, phishing email filtering, and data loss prevention rules.

14.2.2.17 STAFF ONBOARDING

Introduction

A well-defined process to bring on new members of the agency's workforce is vital. It provides a good image of the agency, ensures everyone has the knowledge of agency policies and procedures, and to provide them with adequate resources to have a successful start.

Policy

The onboarding process shall be initiated by the contract/ office LISO with the request for access to data sets and application defined by contract management. Onboarding steps should ensure that the new staff acknowledges all agency policies, have all accounts and access properly setup according to procedure, complete all trainings required, and equipment properly configured, updated, assigned, and tracked.

14.2.2.18 STAFF OFFBOARDING

Introduction

A well-defined process to offboard staff is necessary to ensure access to all information and resources are properly revoked and data ownership transferred to the appropriate personnel. Improperly revoking access to resources can leave unaccounted avenues of access and unintended exposure.

Policy

The offboarding process shall be initiated by the contract/ office LISO. Offboarding steps shall ensure that the departing staff's accounts are properly revoked, data properly transferred to the appropriate personnel, and equipment be retrieved in a timely manner.

14.2.2.19 DATA LOSS PREVENTION (DLP)

Introduction

Data Loss Prevention (DLP) is a process or solution designed to detect and prevent potential data breach incidents where sensitive data may be disclosed to unauthorized personnel by malicious intent or inadvertent mistake. Detection of data at risk can be performed while in use at the endpoint, while in motion during transmission across the network, and while at rest on data storage devices.

Policy

Contract management shall implement Data Loss Prevention measures on all systems that contain information deemed sensitive, private, or restricted. Contract Management shall work with the stakeholders of the system to document and implement an appropriate policy that meets the business requirement while preventing the disclosure of information to unauthorized personnel.

14.2.2.20 ACQUISITION AND DEVELOPMENT OF SERVICES AND APPLICATIONS

Introduction

Programs and services managed by the agency are ever changing. Requirements for these programs are always adapting to meet new needs and fulfill new tasks and duties. As such, new applications are always being adopted to help manage these programs and services, and old applications are always being retired as they are no longer needed. It is important that these new applications meet industry standard security requirements, that they are maintained throughout its lifecycle, and is properly retired and information archived to fulfill agency requirements.

Policy

The agency shall have:

- Contract management team determine security requirements and allocation of resources to protect the application or service.
- Contract management team develop and document a Software Development Life Cycle for the system. Please see the SDLC guidelines for more information on this requirement.
- Contract management team shall develop and implement a plan for ongoing security and privacy control assessments.

14.2.2.21 INFORMATION SYSTEMS CURRENCY

Introduction

Information Systems Currency ensures that the necessary knowledge, skills, hardware, software, and supporting infrastructure are available at a reasonable cost to support information systems

operations. It includes the monitoring and planning of future system developments that enable the organization to leverage modern technology and reduce technical debt.

Policy

The stakeholders and the network admin team shall develop and implement a plan for periodic review of the information system. The review shall consist of an evaluation of the solution to meet the business requirements and the currency of the performance and security features of the implementation. The system shall be updated or modified to meet modern security protocols and standards while maintaining or enhancing business functionality

14.2.3 DETECT

The Detect Function defines the appropriate activities to identify the occurrence of a cybersecurity event. The Detect Function enables timely discovery of cybersecurity events.

14.2.3.1 SUSPICIOUS OR ABNORMAL ACTIVITY

Introduction

Our end users are our eyes and ears into the daily activity of the agency. They are the most familiar with their business and understand best what is normal or abnormal. Along with our automated reporting systems, we depend on our end users to tell us how our systems are performing and whether there is something abnormal.

Policy

All suspicious or abnormal activity, whether physically observed or through system logs or alerts, shall be immediately reported to the supervisor for further action.

14.2.3.2 BREACH OF SECURITY

Introduction

Compromises in security can occur at every level of computing from an individual's desktop to the most protected systems on the network. Incidents can be accidental or deliberate attempts to break into system. Incidents could also be categorized as benign or malicious in purpose or consequence. Each incident requires careful response at a level equal with its potential impact to security of individuals and/or the agency.

Policy

Agency personnel who suspect that a theft, breach, or exposure of Workforce Solutions protected data or sensitive data has occurred must immediately provide a description of what occurred using the WFS Incident Report form to **incidentreports@wrksolutions.com** and your HGAC contract manager. This e-mail address is a distribution to key Board staff at Workforce Solutions. Additional details can be found in the Incident Reports SharePoint page.

Workforce Solutions will investigate all reported thefts, data breaches, and exposures to confirm if a theft, breach, or exposure has occurred. If a beach of security incident has occurred, Workforce Solutions Board staff will follow the appropriate procedure to notify the incident response team.

For the purposes of this policy a "breach of security incident" is any accidental or malicious act with the potential to:

- Result in misappropriation or misuse of confidential personal information such as Social Security Number, health records, financial transactions, etc. of an individual or individuals;
- Significantly imperil the functionality of the information technology infrastructure of the agency's network;
- Provide for unauthorized access to Workforce Solutions resources or information;
- Allow Workforce Solutions information technology resources to be used to launch attacks against the resources and information of other organizations.

14.2.3.3 ACTIVITY LOGS

Introduction

Logs record data so that systems and networks can be appropriately monitored to maintain use for authorized purposes and an awareness of the operating environment, including detecting indications of security problems.

This policy defines requirements for security log generation, management, storage, disposal, access, and use. Security logs are generated by many sources, including security software, such as antivirus software, firewalls, and intrusion detection and prevention systems; operating systems on servers, workstations, and networking equipment; databases and applications.

Policy

All hosts and networking devices must perform security log generation for all components (e.g., OS, service, application). All security events must be logged and must be set to capture levels of detail to indicate activity. Alerts shall be generated for events that can prevent the recording of logs such

as capacity limits. Logs shall be maintained for a minimum of 180 days.

14.2.4 RESPONSE

The Response Function includes appropriate activities to take action regarding a detected cybersecurity incident. The Respond Function supports the ability to contain the impact of a potential cybersecurity incident.

14.2.4.1 INCIDENT RESPONSE PLAN

Introduction

The Incident Response Plan outlines the general steps for responding to computer security incidents. In addition to providing a standardized process flow, it identifies the incident response stakeholders and establishes their roles and responsibilities; describes incident triggering sources, incident types, and incident severity levels; and includes requirements for annual testing, post-incident lessons-learned activities, and collection of IR metrics for use in gauging IR effectiveness.

Policy

The agency shall develop Incident Response plans that defines the following:

- A standardized process flow.
- Identify response stakeholders and establish their roles and responsibilities.
- Describe incident triggering sources, incident types, and severity levels.
- Requirements for annual testing
- Identify post-incident lessons-learned activities
- Collect metrics to gauge incident response effectiveness.

14.2.4.2 LOST OR STOLEN PROPERTY

Introduction

Lost and stolen devices can pose a security threat to the organization's network and data. It is imperative that staff who have determined that a device used to for any work-related purposes should be reported immediately so that the appropriate response can be executed.

Policy

Staff shall immediately notify their supervisor/manager. Service Provider/Sub-Recipient shall notify Workforce Solutions Property Control Officer, Contract Managers, and Workforce Security of the lost or stolen device. Workforce Solutions contract manager shall initiate the appropriate response to identify the scope and remediate the threat as defined by the response plan. Additional information can be found in the "Contract Management Standards and Property" at Contract Management - Workforce Solutions (wrksolutions.com).

14.2.5 RECOVER

The Recover Function identifies appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident. The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity incident.

14.2.5.1 BUSINESS CONTINUITY PLAN

Introduction

In the event that an incident occurs that affects the operation of the business, it is important to have a well-defined plan that allows for the continuing operation of the business while the recovery process is being carried out.

Policy

Workforce Solutions business continuity plan shall follow appropriate guidance in the "Business Continuity Plan" at System Resources - Workforce Solutions (wrksolutions.com).

14.2.6 DISASTER RECOVERY PLAN

Introduction

The principal objective of the disaster recovery plan is to develop, test and document well-structured and easily understood plan which will help service providers recover as quickly and effectively as possible from an unforeseen disaster or emergency which interrupts information systems and business operations.

Policy

All service providers will develop and maintain a disaster recovery plan tailored to their operations and approved by H-GAC contract manager.

15 CHANGE LOG

- Issue 1 Final (October 2022) - Approved version.
- Issue 2 Draft A (February 21, 2023)-Added Section 15.2.2.7 - Mobile Device
- Issue 3 Final (September 2024) - Changed all instances of Personally Identifiable Information (PII) to Sensitive Personal Information (SPI). Added Knowbe4 and Veteran training to section 3.14.b, Revised vulnerability assessment requirement section 14.2.1.10, Removed section 11 Media Disposal and combined with new Data Destruction and Media Sanitization section 14.2.2.5. Added Geographic Restrictions on Data Access section 14.2.2.8. Added the requirement to submit Y-9 form for office openings, office closures, relocations, office manager changes, and contact information changes to section 14.2.2.11.
- Issue 3 Final (October 2024) – Added FNS Civil Right mandatory training to section 3.3