Workforce Solutions Information Security Standards and Guidelines

Revised: October 2021

Information Security Standards and Guidelines

TABLE OF CONTENTS

Information Security Standards and Guidelines

I. 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, volunteer, or visitor, who has access to a customer's Personally Identifiable Information (PII) whether in electronic or paper format.

II. 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.

Information Security Standards and Guidelines

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 OneDrive/SharePoint for file sharing system.

5. 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 as soon as possible.

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

7. 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.

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

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

Information Security Standards and Guidelines

10. 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.

11. 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.

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

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

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

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

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

17. 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.

18. 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.

19. 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.

20. Users must not divulge modem phone numbers to anyone unless doing so is a function of their responsibilities.

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.

III. 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. The agreement, Code of Conduct ***and Equal Opportunity Employee Acknowledgement Form*** shall be reaffirmed annually.

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. Diversity, EEO, and Discrimination Prevention Training
    d. Human Trafficking
    e. ***WIOA Discrimination Complaint Process***
        - ***For EO Officers, Office/ Contract Managers, Monitors, and Navigators***

Note: All Workforce Solutions staff, whether they access Workforce Solutions systems or not, must complete trainings and agreements within 30 days of hire or contract start date. They also must complete all annual trainings in October each year.

4. All users must successfully complete KnowBe4 training within 30 days after activating an account and annually, in October, thereafter. 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 Information Security staff 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.

Information Security Standards and Guidelines

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). The Contract LISO must submit this reconciliation to Workforce Security no later than the 4th working day of every month. This reconciliation must include a review 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 standards and guidelines. 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.

Information Security Standards and Guidelines

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 Officers 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 (1) CyberSecurity Awareness Training, (2) ***Fraud Awareness Training,*** (3) Diversity, EEO, and Discrimination Prevention Training, (4) Human Trafficking Training and (5) WIOA Discrimination Complaint Process (if applicable) before the LISO can request access to Workforce Solutions information system. Any staff that receive a wrksolutions email must complete 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).

    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 at H-GAC. Access rights will be granted when the Board LISO receives a copy 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.

- 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.

- 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 ***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.

g. Refer to the Desk Aid for Local Information Security Officers for guidance

15. Board LISO

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

b. The Board LISO must 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. The Board LISO assures the appropriate security documents are signed and the User successfully completes the on-line trainings (1) CyberSecurity Awareness Training, (2) ***Fraud Awareness Training***, (3) Diversity, EEO, and Discrimination Prevention, (4) Human Trafficking and (5)Workforce Investment Act Discrimination Complaint Process (if applicable).

d. The Board LISO will only retain the usage agreement signed by the user when first hired.

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

f. The Board LISO will submit requests to RACF administration to add and remove local LISO's.

g. The Board LISO is 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. The Board LISO must reconcile the Users recorded in Workforce Solutions user database attached to the board to the Users stationed at the board. In addition, the Board LISO must ensure the Users at all Workforce Solutions locations are reconciled. This reconciliation must occur no later than the 6th working day of every month.

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. The Board LISO must coordinate with H-GAC Data Services Department if a User needs a Workforce Solutions email account.

IV. 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.

V. Personally Identifiable Information (PII)

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

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

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

- Unauthorized individuals cannot access or view PII in print form
- Store documents containing PII in a locked location when not actively using the documents.
- Adequate disposal, i.e. shredding, of PII in print form.
- Maintaining PII and other sensitive information in accordance with TWC standards for information security set forth in WD Letter 13-08, issued April 1, 2008 and titled "Security of Personal Identity Data" and subsequent update;
- PII and other sensitive information is stored in an area that is physically safe from access by unauthorized individuals;
- A tracking log of PII 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;
- PII 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 PII, in electronic or print format, from a Workforce Solutions location unless authorized by H-GAC Contract Liaison or other Workforce Board staff.

Information Security Standards and Guidelines

PII 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 with PII to customers

*As identified by signage such as "Employees Only"

Workforce Solutions staff and contractors must be aware that failure to comply with all PII requirements, and failure to take appropriate action to prevent any improper use or disclosure of PII and other sensitive 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 PII and other sensitive information for unauthorized purposes.

Required Compliance Reviews

Each contractor must conduct Information Security reviews at each location where there is Personally Identifiable Information (PII), in physical or electronic format. Contractors will use the Workforce Solutions Information Security Review report found in the Information Security section at this link http://www.wrksolutions.com/staff-resources/system-resources/information-security-and-mis.

- 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.

VI. 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 Personally Identifiable Information (PII). PII 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 PII 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 PII is not transmitted to unauthorized users. All PII and other sensitive 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-Mail 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.

l. 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.

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

6. Staff using TEAMS must comply with all TWC requirements and under no circumstance will PII 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.

VII. 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 an y 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 Information Security Coordinator.

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

***Confidentiality Notice:** This communication, including any attachments thereto, is intended only for the use of the individual or entity to which it is addressed and contains information that is privileged, confidential, and exempt from disclosure under applicable law. If you are not the intended recipient, you are hereby notified that you have received this document in error and that any review, dissemination, distribution, or copying of the message and attachments thereto is strictly prohibited.

VIII. 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 the highest level of protection possible 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 PII) 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.

IX. 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.

X. 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 PII must not be left in a vehicle unattended for significant periods of time. If PII must be left in a vehicle for a short time, the PII 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

s

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 PII 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.

XI. Media Disposal

The Workforce Solutions Media Disposal 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 of media that contain protected, confidential and/or sensitive information. Media includes, but is 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

Reuse or disposal of 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.

XII. 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/SpecialPublications/NIST.SP.800-88r1.pdf

XIII. 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 ma y have access either as a granted right or by accidental exposure.

All employees, providers, and vendors are prohibited from using or installing an y 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.

XIV. 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
   - Personally Identifiable Information (PII)
   - 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.

XV. INFORMATION SYSTEMS SECURITY

All Workforce Solutions contractors are expected to adhere to the Cybersecurity Framework developed by the National Institute of Standards and Technology (NIST)) to maintain the confidentiality, integrity and availability of Workforce Solutions information resources.

1.0 Breach of Security Policy Purpose

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.

This policy focuses on data security and data security breaches and how Workforce Solutions should respond to such activity. Workforce Solutions is committed to protecting customers, employees, partners, and the agency from illegal or damaging actions by any individual or entity, whether knowingly or unknowingly.

SCOPE

This policy applies to anyone who collects, accesses, maintains, distributes, processes, protects, stores, uses, transmits, disposes of, or otherwise handles confidential and protected data on Workforce Solutions' network.

Information Security Standards and Guidelines

POLICY

This policy mandates that any individual who suspects that a theft, breach, or exposure of Workforce Solutions protected data or sensitive data has occurred must immediately provide a description of what occurred via e-mail to supervisor/ manager, local IT, and WorkforceSecurity@wrksolutions.com immediately.

The contractor management and H-GAC IT team 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, the contractor management will follow the appropriate procedure to notify WorkforceSecurity@wrksolutions.com.

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.***

1.1 Incident Response Team

As soon as a breach of security incident containing Workforce Solutions protected data or sensitive data is identified, the process of removing all access to that resource will be initiated.

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

- ***Chief Finance Officer,***
- ***Director of Human Services,***
- ***Director of Data Services,***
- ***Director of Communications,***
- ***Director of Intergovernmental Relations,***
- ***Facilities Administrator,***
- ***Human Resources 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, and***
- ***Additional individuals as deemed necessary by the Executive Director.***

1.2 Communication and Responsibilities

When breach of security incident of private data has been confirmed:

1. ***The contractor management will notify WorkforceSecuirty@wrksolutions.com of the theft, breach or exposure incident.***
2. ***The contractor management and H-GAC IT team will analyze the breach or exposure to determine the root cause, how the breach or exposure occurred, the types of data involved, the number of internal/external individuals and/or organizations impacted.***
3. ***Workforce Solutions will work with outside legal counsel to decide how to communicate the breach to employees, the public, and others who may be directly affected.***

1.3 Enforcement

Any Workforce Solutions personnel found in violation of this policy may be subject to disciplinary action, up to and including termination of employment. Any third-party partner company found in violation may have their network connection terminated.

2.0 Incident Response Plan

OVERVIEW

In accordance with industry 'best practices', Workforce Solutions has implemented various procedures, policies and guidelines to protect the confidentiality, integrity and availability of our critical data and computing resources. This plan is a procedural document intended to prepare Workforce Solutions to address security incidents. Regular testing and refinement of this plan will help Workforce Solutions prepare for adverse security incidents and ultimately help to manage and minimize risk.

It is anticipated that as new technologies, guidelines, and requirements are introduced, this plan will need to be modified and should be reviewed annually. This function will be performed by members of H-GAC IT team.

RESPONSE PHASES

Responding to an incident may involve a series of steps or phases, each with its own distinct goals and objectives. There are different types of security incidents that can occur with varying levels of severity, and not all incidents will require focus on each step. An incident can range from anything such as a power outage or hardware failure to the most extreme incidents such as a violation of agency policy by disgruntled employees or being hacked by state sponsored hackers.

Information Security Standards and Guidelines

The phases of a security incident response plan at Workforce Solutions are as follows:

1. ***Preparation: Prepare IT team members to be ready to handle potential incident; conduct end -users cyber security awareness training; and keep Disaster Recovery Plan up-to-date.***
2. ***Identification: Determine whether an event actually is a security incident. Determine the priority, scope, and root cause of the incident.***
3. ***Containment: Limit damage from the incident and isolate the affected systems to prevent further damage.***
4. ***Eradication: Find the incident's origin and remove affected systems from the production environment.***
5. ***Recovery: Allow affected systems back into the production environment and ensure no threat remains. Update and document the details of the remediation process in the Workforce Solutions Disaster Recovery Plan document.***
6. ***Evaluation: Document and analyze the incident so staff can learn from it and improve future response efforts. Any resulting amendments, accommodations, or revisions to current policies and procedures will be presented, reviewed, and approved by the Executive Director.***