Workforce Solutions
Standards & Guidelines

Information Security

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.

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 leaving their computers unattended must either 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 a public peer-to-peer file sharing system to transfer files or use Instant Messaging to communicate with others.

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

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

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

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

16. 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.

17. 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.

18. 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.

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

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

21. 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.

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 before access is given to an account. Additional documentation may also be required.

2. Users of Workforce Solutions systems must have on file a signed Workforce Solutions Information Resources Usage Agreement and such agreement shall be reaffirmed annually.

3. All Users must successfully complete the Texas Work Commission on-line training (IT Security Awareness Training and Fraud Prevention and Detection Training) before access is given to an account and annually thereafter.

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

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

6. 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.

7. 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.

8. In the event of termination of employment, change in job, or temporary leave status necessitating the removal or addition of a User's access to one or more information resources, contractor staff 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
   - There are changes (adding or removing) to the User's access to information resources.

   a. 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 may not submit reports for a month in the same month. Contractors will use the report format attached to WS Issuance 11-15.

   b. 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.

   c. 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.

9. 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.

   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.

   b. Staff and LISO must sign the appropriate security document and successfully complete the TWC on-line trainings (IT Security Awareness Training and Fraud Prevention and Detection Training) **before** the LISO can request access to Workforce Solutions information system. The original security documents, including but not limited to:
      - signed Workforce Solutions Information Resources Usage Agreement
      - IT Security Awareness Training Certificate
      - Fraud Prevention and Detection Training Certificate

      must be kept at the contractor's office. The LISO will forward a copy (fax, email, etc.) of the signed Workforce Solutions Information Resources Usage Agreement 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. 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 for the RACF system for Users attached to their location.

   d. The Contractor LISO will maintain a file of all security documents 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. Reconcile the Users recorded in the Workforce Solutions user database attached to the contractors' locations (contractor administration location and career office). The LISO must submit this reconciliation to Workforce Security no later than the 4th working day of every month. Contractors may not submit reports for a month in the same month. This reconciliation must include a review to ensure the level of access is appropriate for the employee's job duties.

f. 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:

g. 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.

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

10. 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 (at a minimum: Workforce Solutions Information Resources Usage Agreement) are signed and the User successfully completes the TWC on-line trainings (IT Security Awareness Training and Fraud Prevention and Detection Training). This must be done when the User is hired and during the annual re-certification of users. The security documents must be retained by the Board LISO.

d. The Board LISO will add, remove, and reset passwords for the RACF system for Users attached to the Board administrative office and for Office LISO and Contractor LISO staff.

e. 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.

f. 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.

g. 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.

h. 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.

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

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:
    - Contain at least one upper case letter, one lower case letter, and one number,
    - Are at least 8 characters in length,
    - Passwords must not have consecutive duplicate characters such as 99 or BB,
    - Passwords must not have consecutive-count numbers or letters, such as 1234 or ABCD,
    - Passwords are not words in any dictionary including slang, dialect, jargon, etc,
    - Passwords are not based on personal information such as names, birthdates, etc,
    - Passwords should be easily remembered, and
    - 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 her password has been compromised, it must be changed immediately and her supervisor notified of the suspected compromise.

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 indentifying 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 electronic display or in printed material.**

To protect PII stored or transmitted electronically or in print form, contractor 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.
- 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.

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/policiesandprocedures.html.

- 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 twenty 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.

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 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. Confidential Workforce Solutions material transmitted over external network connections must be 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.

3. To 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.

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

5. E-Mail Users must 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.

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

7. Individuals must 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.

8. Individuals 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.

9. Workforce Solutions IT management, 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.

10. Workforce Solutions IT retains the right to examine any non-encrypted E-Mail item for subject and/or content to determine E-Mail abuse.

11. Workforce Solutions IT 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.

12. Workforce Solutions IT 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.

13. All Users of Workforce Solutions E-Mail systems shall 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.

14. All Users of Workforce Solutions E-Mail systems shall use caution in selecting the "Reply to All" function of Workforce Solutions E-Mail client application.

15. All Users of Workforce Solutions E-Mail systems shall 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.

16. All Users of Workforce Solutions E-Mail systems shall not publish their Workforce Solutions E-Mail address on any internet website outside the authority of Workforce Solutions.

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 Information Security Coordinator.

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 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.

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.

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 at the end of every work day—in locked cabinets or locked rooms.
3. Shred documents that include customer identity data that is not filed.
4. Laptop computers must be secured when not in use.

5. Documents with customer identity data must not be in plain view.
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.

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

Disposal of media will follow the requirements published in Texas Administrative Code rule subsection 202.28 to ensure removal of any electronic protected, confidential and/or sensitive information. See http://info.sos.state.tx.us/pls/pub/readtac$ext.TacPage?sl=R&app=9&p_dir=&p_rloc=&p_tloc=&p_ploc=&pg=1&p_tac=&ti=1&pt=10&ch=202&rl=28

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://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf

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 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.