Individual Agreement

Rules of Behavior for General Users

In accordance with the *TxDOT Acceptable Use Policy*, this Individual Agreement lists the minimum responsibilities and behavioral expectations for individuals granted user privileges to TxDOT information resources technology (IRT), including TxDOT data. The rules below describe acceptable, what is allowed, and unacceptable, what is prohibited, behavior. Individuals granted access to TxDOT IRT or TxDOT data have an obligation to protect it and to comply with TxDOT policies as well as Information Security controls and standards; applicable local, state, and federal laws; and regulatory requirements to help prevent unauthorized or accidental disclosure, modification, or destruction of information and information resources. This includes reading, acknowledging, and adhering to these provisions and conducting their work in accordance with TxDOT Human Resources Policy that specifies employee "*Conduct and Expectations*" as well as "*Prohibited and Restricted Conduct.*"

As defined in *Texas Government Code, §2054.003(7), "*Information resources means the procedures, equipment, and software that are employed, designed, built, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information, and associated personnel including consultants and contractors."

As defined in *Texas Government Code, §2054.003(8)*, TxDOT IRT includes the "data processing and telecommunications hardware, software, services, supplies, personnel, facility resources, maintenance, and training."

As defined in the *TxDOT Data Classification Policy*, "TxDOT data is information that is written, produced, collected, assembled, or maintained under a law or ordinance or in connection with the transaction of official business by TxDOT; for TxDOT; where TxDOT owns the information, has the right of access to the information, or spends or contributes public money for the purpose of writing, producing, collecting assembling, or maintaining the information; or by an officer or employee of TxDOT in the officer or employee's official capacity and pertaining to official business of the government body. This includes intellectual property, state records, and travel information."

This Individual User Agreement includes Rules of Behavior for seven areas:

- Using TxDOT IRT and Data
- Using Passwords and Credentials
- Using Internet, Email, and Web Storage
- Protecting TxDOT data
- Protecting Privacy
- Using Non-TxDOT Devices
- Using Secure Locations.

Rules of Behavior for Using TxDOT IRT and Data

Acceptable Use

- I understand that access to TxDOT IRT and data is restricted to authorized users with assigned responsibilities.
- I will use TxDOT IRT or data solely for the purpose authorized by my work duties and specified by TxDOT.
- I will adhere to TxDOT's information security and privacy protections such as TxDOT's policies, standards, and other security mechanisms.
- I will limit personal use of TxDOT IRT so that it does not disrupt my productivity, interfere with the mission or operations of TxDOT, or violate TXDOT policies.
- I understand that all content created on behalf of TxDOT is TxDOT property and that TxDOT has the right to review, examine, archive, retrieve, restore, investigate, and delete this content.
- I understand that my actions and activities with TxDOT IRT are subject to monitoring, recording, and auditing; I understand that I cannot expect to have privacy for activities regarding TxDOT IRT.
- I will complete all required training (security and privacy awareness, role-based training) within 60 days of getting access and I will update it annually or as required by TxDOT policies.
- I will properly secure TxDOT IRT and data when leaving it unattended, regardless of my location. This includes using a password-enabled lock screen, locking devices assigned to me, or logging off completely.
- I will comply with TxDOT's Using Information Resources Technology Outside the United States of America policy when I need to take TxDOT IRT or data outside the USA.
- I will report all suspected information security incidents to the TxDOT Service Desk as soon as possible.
- I will report all potential privacy breaches to ITD_Privacy@txdot.gov.

Unacceptable Use

- I will **not** conduct TxDOT Confidential or Regulated business over unsecured or public Wi-Fi networks without first connecting to the TxDOT virtual private network (VPN).
- I will **not** conduct TxDOT business using any of the specific items nor categories of software, applications, hardware or equipment either made by developers or manufacturers that appear on the Prohibited Technologies list.
- I will **not** install items from the Prohibited Technologies list on a device that I use to conduct TxDOT business.
- I will **not** allow TxDOT IRT or data to be accessed or used by applications or technologies named on the Prohibited Technologies list.
- I will **not** allow unauthorized users, services, applications, or devices to access or use TxDOT IRT or data. For example, this may require shielding TxDOT IRT and data from microphones and cameras when required.

- I will **not** circumvent or bypass security safeguards or access controls, reconfigure systems, install nor load unauthorized or unlicensed software, nor make configuration changes without proper official authorization.
- I will **not** create or operate unapproved nor unauthorized web sites or services.
- I will **not** use personal devices or devices issued by other organizations to conduct TxDOT business except in accordance with TxDOT's Rules of Behavior for Using Non-TxDOT Devices.
- I will **not** carry, bring, or use devices that have prohibited technology enabled when I am inside or near a Secure Location or in a meeting that has been designated as a Secure Meeting.

Rules of Behavior for Using Passwords and Credentials

Acceptable Use

- I will protect my passwords and other access credentials from disclosure and compromise.
- I will promptly change my password when required by TxDOT or if I suspect that it has been compromised.
- I will always use authorized credentials such as identity, password, or passcodes, assigned to me.
- I will turn off web browser's synchronization functions to ensure that my personal data and TxDOT data do not become commingled.
- I will report all suspected and identified password compromises to TxDOT Service Desk as soon as possible.
- I will be accountable for actions taken using my password and login credentials.

Unacceptable Use

- I will **not** share passwords nor provide passwords to anyone, including system administrators, nor will I use a password that was not assigned to me.
- I will **not** use business passwords or credentials for personal purposes.
- I will **not** use personal passwords or credentials for business purposes.

Rules of Behavior for Using Internet, Email, Web Storage

Acceptable Use

- I will limit my personal use of the internet during official working hours, in accordance with the Human Resources Policy "Social Media – Personal Use by Employees," and to the extent that it does not violate TxDOT security and privacy policies.
- I will disseminate only authorized TXDOT information related to my official job and duties.
- I agree that the only time I will forward chain letters, email spam, inappropriate messages, unapproved newsletters, or broadcast messages is to report this activity to spam@TxDOT.gov.

- I will immediately report to spam@TxDOT.gov all unsolicited email requests for personal or organizational information, or requests to verify accounts or security settings.

Unacceptable Use

- I will **not** use personal email, storage, or services to store or transmit TxDOT data nor to conduct TxDOT business.
- I will **not** auto-forward TxDOT email to unauthorized email accounts.
- I will **not** use TxDOT email to create personal sites, subscribe to personal services, nor to create personal memberships.
- I will **not** navigate to prohibited websites using a TxDOT-issued device.

Rules of Behavior for Protecting TxDOT Data

Acceptable Use

- I will access only the TxDOT IRT and data for which I have been authorized and to which I have been assigned explicit work duties.
- I will take all necessary precautions to protect TxDOT data from unauthorized access, use, duplication, modification, destruction, theft, disclosure, loss, damage, or abuse, in accordance with TxDOT policies.
- I will protect information where it is stored regardless of media or format and to prevent it from being disclosed to unauthorized persons or groups. This includes, but is not limited to:
    - Encrypting Sensitive, Confidential, or Regulated data when it is transmitted via email, attachment, media, etc.;
    - Disseminating, transporting, and storing passwords and encryption keys separately from the encrypted files, devices, and data;
    - Securely disposing of electronic and hard copy files that contain Sensitive, Confidential, or Regulated data when it is not needed and in accordance with the TxDOT Records Management policy.
- I will report all suspected or known security incidents, TxDOT data breaches, and suspicious activities to the TxDOT Service Desk immediately.
- I will properly dispose of Sensitive, Confidential, or Regulated TxDOT data in accordance with TxDOT's sanitization standards.

Unacceptable Use

- I will **not** store Sensitive, Confidential, or Regulated data in public folders, on unauthorized devices or services, or other unsecure physical or electronic locations.
- I will **not** share, store, copy, nor disclose Sensitive, Confidential, or Regulated information with third-party organizations nor use unauthorized third-party applications to store Confidential or Regulated information.
- I will **not** conceal, remove, change, duplicate, tamper, falsify, or destroy TxDOT data except as required by my job duties and with prior authorization.

- I will **not** attempt to access nor use Confidential or Regulated information for anything other than authorized purposes.
- I will **not** dispose nor destroy official state records without Records Management approval.

Rules of Behavior for Protecting Privacy

Acceptable Use

- I will collect information about individuals only as required by my assigned duties and authorized by a program-specific law, after complying with any applicable notice and other legal requirements.
- I will release information to members of the public (including individuals, organizations, the media, individual Members of Texas Legislature, etc.) only as allowed by the scope of my duties, applicable TxDOT policies, and the law.
- I will use information about individuals (including personally identifiable information and protected health information) only for the purposes for which it was collected and consistent with conditions in stated privacy notices such as those provided to individuals when the data was collected.
- I will ensure the accuracy, relevance, timeliness, and completeness of information about individuals, as is reasonably necessary and to the extent possible.

Unacceptable Use

- I will **not** use TxDOT data for private gain.
- I will **not** misrepresent myself or TxDOT or for any unauthorized purpose.

Rules of Behavior for Using Non-TxDOT Devices

The following rules apply when using a device that was **NOT** issued by TxDOT, including personal devices or cell phones, tablets, desktop and laptop computers, and other internet capable devices to conduct TxDOT business.

Acceptable Use

- I will access only data that has been classified as Public or Sensitive, in accordance with the TxDOT Data Classification policy.
- I will only create, store, process, or transmit TxDOT Public or Sensitive data.
- I will use the TxDOT multifactor authenticator as needed when I conduct TxDOT business on any device.
- I will notify the TxDOT Service Desk immediately if a device that I used to conduct TxDOT business is lost or stolen.
- I will notify the TxDOT Service Desk immediately if the device I use for TxDOT business becomes compromised with malware, a virus, or any suspicious attack.
- I agree that TxDOT will not reimburse me for any costs associated with using a non-TxDOT device to conduct TxDOT business.

- I agree that I am solely responsible for setting up, administering, and managing devices not issued by TxDOT.
- I will ensure all non-TxDOT devices used to conduct TxDOT business are patched and maintained.
- I agree that TxDOT may uninstall, delete, or otherwise remove TxDOT data or applications at any time.
- I will set a device passcode or biometric authentication on all non-TxDOT devices used to access TxDOT data or TxDOT IRT.
- I will follow all applicable Rules of Behavior when conducting TxDOT business on any device.

Unacceptable Use

- I will **not** access TxDOT's wired or wireless networks, except for the TxDOT Guest Wi-Fi, with any device that was not issued by TxDOT.
- I will **not** connect non-TxDOT devices to TxDOT's wired or wireless networks for any purpose nor by any means, including charging cords, Bluetooth, or Wi-Fi.
- I will **not** save any TxDOT passwords to non-TxDOT devices. This includes passwords to web sites, password vaults, or phone-based password logs.
- I will **not** create, store, process, or transmit TxDOT Confidential or Regulated data using a device that was not issued by TxDOT.
- I will **not** conduct TxDOT business on a device that has items named on the Prohibited Technologies list installed.
- I will **not** bring into a designated Secure Location a device that was not issued by TxDOT and that has installed software or applications named on the Prohibited Technologies list.

Rules of Behavior for Using Secure Locations

Acceptable Use

- I will conduct TxDOT business identified by the Chief Information Security Officer (CISO) as requiring a Secure Location only in a designated area that meets the definition of a Secure Location.
- I will contact the Information Security Office through InfoSecurity@txdot.gov to determine if a business function requires a Secure Location. Only those business functions and locations officially approved by the CISO require a Secure Location.
- I will use either a physical or virtual Secure Location that can be clearly marked and that can be isolated to prevent prohibited technologies from accessing, overhearing, or seeing the information in the area when notified that a meeting requires a Secure Location.
- I understand that Secure Locations may be a designated location in a TxDOT facility or an impromptu arrangement at a telework or travel location as long as they include these qualities:
    - Doors that can be closed to limit microphones from picking up the discussion.

- Curtains, blinds, or other opaque barriers to limit cameras from seeing the information.
- For online meetings that use audio and video technologies, a Secure Location means all participants can close doors and cover windows to provide the needed isolation.

Unacceptable Use

- I will **not** bring into a Secure Location a device purchased from a company named on the Prohibited Technologies list nor any device containing prohibited technologies.

Signature

I have read the Individual Agreement *Rules of Behavior for General* and understand and will comply with the provisions stated herein. I understand that any exception to this Agreement must be authorized in advance and in writing by the designated TxDOT officials. I understand that violations of this Agreement or other TxDOT policies and standards; state or federal laws; or regulations can result in disciplinary action, which may include termination of employment; removal or debarment from work on TxDOT contracts or projects; revocation of access to TxDOT information, information systems, or facilities; criminal or civil penalties; or imprisonment.

User's Name (Print):	
User's Signature:	
Date Signed:	