1 PURPOSE

The purpose of this Standard is to define T-Mobile third party risk management and security requirements that help meet T-Mobile’s overall risk management objectives.

Note – this Standard was formerly known as TISS-610 Supplier Security Standard and is now aligned to the Enterprise Third-Party (Supplier) Risk Management program.

2 SCOPE

This Standard sets forth T-Mobile’s requirements for Suppliers to take reasonable measures to implement appropriate technological and procedural controls to protect T-Mobile’s information, business interests, and reputation.

This Standard applies to all Suppliers including, but not limited to, those performing any of the following:

1. Accessing, hosting, retaining, processing, or transmitting non-public T-Mobile information. Refer to the TISS-310 Information Classification Standard for descriptions of information classification levels.
2. Developing, supporting, or managing technology, application(s), service(s), or solution(s) used for T-Mobile business purposes whether residing within T-Mobile’s environment or hosted externally.
3. Any other work or partnership that, in T-Mobile’s view, triggers a need to review or compare a party’s processes, procedures and policies.

2.1 DEFINITIONS

1. AOC – Attestation of Compliance (related to PCI).
2. CPNI – Customer Proprietary Network Information. CPNI is information related to T-Mobile Customer use of telecommunications services, such as: type of service or service plan, origination, destination or location of voice calls, and amount of use of telecommunication services. CPNI also includes information contained in customer bills. (CPNI is not subscriber list information – name, mobile phone number [MSISDN] and billing address.)
4. ESRA – Enterprise Third-Party (Supplier) Risk Assessment
5. ESRAP – Enterprise Third-Party (Supplier) Risk Assessment Program
7. Must – Indicates requirements to be strictly followed in order to adhere to the policy (Standard) and from which deviation is prohibited unless a formal exception has been filed and granted.
8. Non-public T-Mobile information – this includes T-Mobile Restricted, Confidential and/or Internal information. Refer to TISS-310 Information Classification Standard (TISS-310) for examples and descriptions.
9. PCI – Payment Card Industry. Refer to TISS-310 for examples of PCI cardholder information.
10. PII – Personally Identifiable Information. Refer to TISS-310 for examples.
11. Public Data Network – a network established and operated by a telecommunications company, or a recognized private operating agency, for the specific purpose of providing data transmission services for the public. Data traversing a Public Data Network may be routed over numerous providers and via various means (e.g. wired and wireless). Based on routing protocols, network topologies, and network issues, the data may also be routed through a wide range of geographic locations including sent off-planet and returned via satellite.
12. RACI – Responsible, Accountable, Consulted and Informed.
14. SAQ – Self Assessment Questionnaire (related to PCI).
15. Salt – In cryptography, a salt is random data that is used as an additional input to a one-way function that hashes a password or passphrase. Salts defend against dictionary attacks versus a list of password hashes, and against pre-computed rainbow table attacks.
16. Security breach – Actual, probable or reasonably suspected unauthorized access to, or acquisition, use, loss, destruction, compromise or disclosure of, any information maintained on the Supplier Systems.
17. Service accounts – Specially created accounts used to programmatically run a process or service on a server. A service account is often described as any account that does not correspond to an actual profile. Service accounts are usually used for connecting an application to a database, or machine-to-machine connectivity.
18. Should – Indicates the requirements to be followed in order to adhere to the policy (Standard) where possible. It indicates a preferred course of action that does not require a formal exception in case of the inability to meet a requirement.
20. Third Party (a.k.a. Supplier/Vendor/Service Partner) – An external, third-party company, vendor, supplier, service provider or organization rendering services to or on behalf of T-Mobile.
21. T-Mobile Restricted and/or Confidential Information – as defined in TISS-310 Information Classification Standard (TISS-310).
22. User – Anyone who will have, or currently has, access to T-Mobile information and/or communication resources for the limited and express purpose of performing their job responsibilities.

3 ENTERPRISE THIRD-PARTY (SUPPLIER) RISK MANAGEMENT STANDARD

3.1 ENTERPRISE THIRD-PARTY (SUPPLIER) RISK ASSESSMENT PROGRAM - ESRAP

T-Mobile’s Enterprise Third-Party (Supplier) Risk Assessment Program (ESRAP) was established to ensure that T-Mobile meets certain compliance and regulatory obligations to protect T-Mobile Information.

ESRAP includes, but is not limited to, the following domains: anti-corruption, financial health, financial services compliance, security and privacy, and related party transactions.

T-Mobile will complete an Enterprise Third Party (Supplier) Risk Assessment (ESRA) screening form for all Suppliers. All material Supplier risks associated with T-Mobile systems and data must be treated and disclosed to T-Mobile (ESRAP@t-mobile.com).

3.1.1 SUPPLIER RISK MANAGEMENT REVIEW - SRMR

ESRA is used as a trigger to determine if a SRMR is required. This Enterprise Third-Party (Supplier) Risk Management Standard (TRS-610) is the basis for the Supplier Risk Management Review (SRMR) which evaluates a Supplier’s internal controls against the standards included in this document. To complete the SRMR, Suppliers provide a self-attestation via T-Mobile’s Supplier Risk Management (SRM) questionnaire, third party independent audit reports (if available), and other supporting documents as requested. The SRMR is a desk review of those documents.

If the SRMR reveals a gap between the Supplier’s internal controls and this Standard, a remediation plan and/or an exception request may be required.

All Suppliers in scope for T-Mobile’s PCI compliance must provide proof of PCI compliance on request including, but not limited to, their most recent (within the last twelve (12) months) AOC. T-Mobile reserves the right to request additional information/documentation (e.g. ROC, SAQ, RACI) as needed.

Supplier will document which PCI requirements they manage on behalf of or in coordination with T-Mobile.

Note: The SRMR process does not apply to Suppliers that only provide contingent staffing using T-Mobile equipment. A SRMR is generally not required for Supplier’s sub-contractors who simply support the Supplier’s...
work; however, this does not remove the obligation of the Supplier to ensure that T-Mobile’s non-public information is secured appropriately as per this TRS-610, and as required by contractual terms between T-Mobile and Supplier.

3.1.2 Third Party Cybersecurity Assessment Program - CAP


The purpose of the Cybersecurity Assessment Program (CAP) is to identify whether appropriate security controls exist at T-Mobile’s TPS in order to ensure the availability, integrity, and confidentiality of T-Mobile’s data. This CAP review is focused on operational and technical security controls detailed in this TRS-610 Standard.

3.2 Information

T-Mobile has defined an information classification scheme to properly identify all T-Mobile information, TISS-310 Information Classification Standard (TISS-310). The information classification levels are used throughout this Standard. Please contact your T-Mobile representative if you need a copy of TISS-310.

Specific information handling procedures are identified in this Standard, TRS-610, to ensure that appropriate protection exists throughout the life cycle of the information based on T-Mobile’s information classification level.

3.2.1 Information Classification

All T-Mobile information must be classified when created/received according to TISS-310 regardless of where it resides, the form it takes, or the technology used to handle it for the purpose of enforcing appropriate handling procedures as indicated in this Standard.

3.2.2 Information Handling, Storage, and Assets

1. The Supplier is responsible and accountable for managing assets containing T-Mobile non-public information that are under Supplier’s control, and responsible for security controls relevant to any Supplier access to such assets.

2. T-Mobile Restricted and/or Confidential Information must be physically secured when not in use, including but not limited to, papers, manuals, and electronic media.

3. Users should not store T-Mobile non-public information on personal devices/media.

4. T-Mobile Restricted and/or Confidential Information (data) must be encrypted while at rest.

5. In a multi-tenant environment there must be the ability to logically or physically segment data such that data may be accessed for a single tenant only, without inadvertently accessing another tenant’s data (e.g. using unique identifiers or different schemas for each tenant).

6. T-Mobile must be advised if equipment or media containing non-public T-Mobile information is accessed, processed, or retained by Supplier’s sub-contractor/service provider(s) or in any way has the ability to impact T-Mobile’s security.

7. If data will be stored, accessed, processed, and/or retained outside of the United States of America, the Supplier must contact ESRAP@T-Mobile.com for review and approval.

3.2.3 Back-up Information Handling

1. Back-up data containing non-public T-Mobile information must be segregated (physically or by using unique identifiers) from Supplier’s information or Supplier’s client’s/customer’s information with appropriate access controls to prevent unauthorized access.

2. Back-up files should be stored in a remote location or secondary data center to reduce the risk of damage from a disaster at the main site. Back-up files for critical systems must be stored in a secondary location.

3. Back-up restoration procedures and media should be tested at least annually.
3.2.4 Disposal of Information

All non-public T-Mobile Information must be returned to T-Mobile or destroyed as defined in the contractual agreement. When Suppliers are performing media sanitation they must provide T-Mobile a certificate of destruction upon request. Please reach out to ESRAP@T-Mobile.com for the form.

The following destruction methods must be used where applicable (unless other methods are described in the contractual agreement):

<table>
<thead>
<tr>
<th>Media</th>
<th>Disposal Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Paper</td>
<td>Cross-cut shredding, incinerating, or pulping such that there is reasonable assurance the materials cannot be reconstructed.</td>
</tr>
<tr>
<td>Mobile Computing Devices (cell phones, tablets, etc.)</td>
<td>Delete all non-public T-Mobile information on the device(s).</td>
</tr>
<tr>
<td>Electronic Storage Media (hard drives, USB/memory sticks, RAM, tapes, etc.)</td>
<td>Physically destroy or sanitize media using a minimum of three overwrite passes and verify removal of data.</td>
</tr>
<tr>
<td>Optical Disks (CDs, DVDs, etc.)</td>
<td>Use optical disk shredder or disintegrator. Disks can also be incinerated or grinders can be used.</td>
</tr>
</tbody>
</table>

3.2.5 Information Transmission

1. T-Mobile Restricted and/or Confidential Information must be encrypted during transmission over public data networks.
2. When non-public T-Mobile information is being transmitted within the Supplier’s internal network, encryption or appropriate network segmentation must be used (e.g. LAN/VLANs).

3.3 Encryption Requirements

Encryption technologies must be used to protect T-Mobile Restricted and/or Confidential Information. When encryption is required, the following minimum technologies must be used:

1. Secure Shell (SSH)-2, Transport Layer Security (TLS)-1.2 for web based management and other remote access to systems containing or transmitting T-Mobile Restricted and/or Confidential Information.
2. Advanced Encryption Standard (AES), RSA, or other T-Mobile approved encryption algorithms must be used as the basis for encryption implementation.
   a. When using AES authenticated encryption, modes such as Counter with CBC-MAC (CCM) or Galois/Countered Mode (GCM) should be used when technically feasible.
   b. When using RSA, RSA Encryption Scheme - Optimal Asymmetric Encryption Padding (RSAES-OAEP) mode must be used.
3. In situations where there is an absolute need to use technologies that utilize proprietary encryption algorithms, these algorithms must be reviewed, tested, and approved by T-Mobile.
4. Encryption technologies must be used in accordance with government regulations of both the originating and destination countries. Please contact ESRAP@T-Mobile.com if the encryption technology does not meet T-Mobile’s minimum requirements.
5. Proven standard hashing algorithms such as Secure Hash Algorithm (SHA)-2 (SHA-256 or above) must be used when cryptographic hashes are required (e.g. message integrity and digital signatures).
6. For password storage algorithms, the passwords must be hashed with SHA-2 or above and use a per-User account randomly generated salt. The passwords should be hashed with a stronger algorithm such as Password-Based Key Derivation Function 2 (PBKDF2), bcrypt or scrypt.
7. Salts must be random per-User and minimum of sixteen (16) characters in length. The same Salt can be used for security questions pertaining to a specific User.
8. MD5 message-digest algorithm (MD5) must not be used for encryption.
9. Unique T-Mobile specific encryption keys must be used for encrypting T-Mobile Restricted or Confidential Information where possible.

10. For wireless networks, Wi-Fi Protected Access (WPA2) should be used as a minimum basis of security. WPA1 and Wired Equivalent Privacy (WEP) must not be used.

11. The following minimum key lengths must be used for all encryption implementations:
   - 256 bits for hash algorithms
   - 128 bits for symmetric keys (256 bits recommended)
   - AES192 acceptable for IPsec tunneling (256 bits recommended)
   - 224 bits for Elliptic Curve (256 bits recommended)
   - 2048 bits for RSA Keys

3.3.1 CRYPTOGRAPHIC KEY MANAGEMENT

Suppliers must have clearly defined and documented processes for managing cryptographic keys (e.g. encryption, code signing, and/or authentication keys). It is recommended to use current FIPS/NIST standards as a basis.

Note: Cryptographic keys are considered T-Mobile Restricted and must be protected appropriately. Keys must be encrypted and never stored in clear text.

Cryptographic key management must include the following:
1. Equipment used to generate, store and archive keys must be physically protected.
2. Cryptographic keys must never be stored in equipment, documents or systems that are not provisioned to meet secure key management requirements (e.g. log files, ticket tracking systems, knowledge management systems, or training documentation).
3. Access to cryptographic keys must be restricted, limiting to the fewest number of custodians necessary.
4. Cryptographic keys must be changed (re-keyed) periodically:
   a. As deemed necessary and recommended by the associated application, preferably automatically.
   b. At least annually.
5. Old keys must be retired (archived, destroyed, or revoked as applicable).
   a. Encryption keys must be archived
   b. Signing keys must be destroyed
6. Key management procedures must be implemented for recovering keys that are lost, corrupted, or archived.
7. For high security keys, such as root certificate authority or trust anchor keys, key management procedures must be implemented to require split-knowledge and dual control of keys for operations such as export, rotation, or deletion. In some cases, dual control must also be implemented when the key is used for operations, for example using a Public Key Infrastructure (PKI) root Certificate Authority (CA) to sign a subordinate CA certificate. An example of dual control would be to require that two or three people each know only their own part of the key to reconstruct the whole key or the key must be divided and stored in two or more systems/devices.
8. Procedures must include a process for changing the keys in the event an employee with key management access (or knowledge) changes job duties or leaves the company.
9. Suppliers using T-Mobile DNS domains must get their SSL/TLS certificates from T-Mobile.
10. All the certificates used for T-Mobile purposes must have minimum key lengths of at least 2048 bits (RSA).
11. Passwords used to protect cryptographic keys must be as strong as the keys they protect.

For example: A password must be twenty (20) characters long to protect a 128 bit AES symmetric key (or 2048 bit RSA key), where the password is randomly chosen from the printable ASCII characters (a-z, A-Z,
0–9, 32 special) characters. If the password for protecting cryptographic keys is User selected then it must be at least 112 characters long.

12. Virtual or web based key management involves the use of a service (using such methods as HTTPS or custom network protocols) that is used for the distribution of key material to servers/services. The key material includes such data such as private keys or account passwords, and extends to all forms of data used in authentication or data protection. If key management is virtual or web based, please contact ESRAP@T-Mobile.com for further review.

3.4 DISASTER RECOVERY AND BUSINESS CONTINUITY

Supplier must implement and maintain a Disaster Recovery Plan that ensures all T-Mobile information that is identified to be the responsibility of the Supplier is backed-up and protected, is capable of being recovered, and that the integrity of all such recovered T-Mobile information is retained. This applies in the event that Supplier’s network, application(s), interfaces, database(s), system(s) or facility(ies) experience a security breach or any significant interruption or impairment of operation, or any loss, deletion, corruption or alteration of data. Requirements for scope, recovery time, level of confidentiality, frequency of back-up, and security must be in accordance with the terms in an approved contract. For specific Business Continuity requirements based on tiering (e.g. Tier 1 requires full geographically dispersed Active-Active redundancy) please contact ESRAP@T-Mobile.com.

Back-up plans for individual systems should be tested at least annually to ensure that they meet the requirements of the Business Continuity Plan. For critical systems, back-up plans must cover all in-scope systems, information, applications, security, and data necessary to recover the complete system that is within Supplier’s control in the event of a disaster. Documentation that a recovery plan is in place must be provided to T-Mobile upon request.

3.5 SYSTEM AUDITING, LOGGING AND MONITORING

All network and information systems used for T-Mobile services, in conjunction with the terms of contractual agreements, must be auditable and include the following requirements:

1. T-Mobile Restricted and/or Confidential Information must be protected as per the security requirements in Section 3.2.1 and not be contained in log files with the exception of supporting temporary debugging processes. Log files containing T-Mobile Restricted and/or Confidential Information must be deleted from all logging systems immediately upon bug resolution.

2. Procedures must ensure system activities are monitored for authorized use, access, and logging.

3. The level of auditing and logging must take into consideration the criticality of the application/process/system, the value, sensitivity and criticality of the information involved, the system interconnection, past audit results, misuse, and system infiltration.

4. Auditing and Logging must cover events including but not limited to: authorized access, privileged operations, unauthorized access attempts, system alerts or failures, initialization of the audit logs, changes to or attempts to change system security settings and controls, and logging of errors and faults.

5. All the events in the audit logs must be time-stamped. System times (clocks) must be synchronized via NTP (Network Time Protocol) to ensure the accuracy of audit logs. Where feasible, the clocks should be standardized to UTC time.

6. Log files for systems, applications, or databases supporting T-Mobile non-public information must be reviewed for anomalies on a regular basis, at least monthly. More frequent log reviews may be required by T-Mobile, dependent on the sensitivity of the system/data. T-Mobile may request evidence that log reviews are being done.

7. Log file retention for systems, applications, and/or databases supporting T-Mobile information:
   a. must be stored to log server(s) or media that is difficult to alter;
   b. must be stored for a minimum of six (6) months (recommended twelve (12) months);
   c. must be backed up; and
   d. In the event of a security breach T-Mobile may request to review log files.
3.6 **Logical Access Control**

1. Access rights to systems storing and/or processing T-Mobile non-public information must be granted on a need-to-know and least-privilege basis using controls such as role-based access and segregation of duties.

2. Remote access to T-Mobile’s internal environment must be approved by a management-level single point of contact (of the Supplier) that will be responsible for enforcing T-Mobile’s security requirements defined in this TRS-610. This access must be reviewed for renewal at least every ninety (90) days.

3. Multi-factor authentication must be implemented for all remote elevated (privileged) network access for systems supporting T-Mobile. *(Multi-factor authentication requires the use of authentication elements from two (2) or more categories of something one has, something one knows, and/or something one is. Some examples are: a Smart Card plus password; or a security (electronic or software-based) token plus a password; or biometrics plus a password. The combination of a User ID and password does not qualify as multi-factor authentication.)*

4. User IDs must be unique and assigned to a specific individual. Group/Shared/Generic accounts must not be used.

5. User access rights to systems or information supporting T-Mobile must be deactivated within seventy-two (72) hours upon employee/contractor voluntary termination, leave of absence, or change in job duties no longer requiring access. In the event of an involuntary termination, access must be removed immediately.

6. Creation of local admin groups and/or file shares must be added based on minimum necessary permissions and role based appropriateness.

7. User access to each system, application, or database supporting T-Mobile must be documented and reviewed every ninety (90) days, at a minimum. Inactive User accounts with no activity for more than ninety (90) days must be removed and/or disabled. *The review does not extend to T-Mobile Customers who may be Users accessing a public facing system or application.*

3.7 **Network Security Controls**

Appropriate network security controls must exist in Supplier’s environment to ensure the confidentiality, integrity, and availability of the network, network devices, and information which support T-Mobile. If any of the following areas are not technologically possible, Supplier must notify [ESRAP@T-Mobile.com](mailto:ESRAP@T-Mobile.com) for determination of acceptable mitigation.

1. Appropriate network security controls (e.g. firewalls, IDS/IPS, WAF), must exist within Supplier’s network to protect the network segment dealing with T-Mobile non-public information. The capability of Users to connect to, and transmit/share T-Mobile non-public information between shared and segregated networks must be restricted based on business requirements and/or least-privilege basis.

2. Networks must have routing controls enabled to ensure access control requirements are met and the network is protected from breaches or attacks.

3. All access control lists and firewall rule sets affecting access to systems supporting T-Mobile must be reviewed and approved by Supplier’s management at least every six (6) months.

4. All remote access to T-Mobile networks must be through T-Mobile approved methods. Please contact [ESRAP@T-Mobile.com](mailto:ESRAP@T-Mobile.com) to ensure appropriate connectivity.

3.8 **Password Complexity**

The following (3.8.1, 3.8.2 and 3.8.3) are requirements for systems supporting T-Mobile or systems accessing T-Mobile’s environment.

3.8.1 **Service Account Passwords**

For service accounts (a.k.a., system passwords) that are not limited to either connecting an application to a database, or providing machine-to-machine connectivity, the following requirements apply:

1. All service accounts must have an identified owner.
2. Service account passwords must:
a. contain a minimum of thirty (30) characters, sixty (60) characters are recommended;
b. require a mixture of both upper and lower case characters;
c. include at least one (1) number and;
d. include at least one (1) special character (where technically feasible).

3. A password generation tool should be used to create randomized service account passwords.

4. Systems must maintain a record of previous passwords, and prevent re-use of at least the last five (5) previously-used passwords.

5. Service account passwords must be changed at least annually, or earlier in case of security issues.

6. Service account passwords must not be shared beyond those with a demonstrated need to know.

7. Passwords that are improperly disclosed must be changed immediately upon discovery.

8. System must not be able to select and change its own service account passwords.

9. System must lock service account after five (5) invalid login attempts and the account owner or system administrator must be notified to unlock the account.

10. Service accounts must only be used for their approved service and not shared with systems or applications for which they were not provisioned.

11. Service account passwords must be immediately changed when a person with knowledge of the password leaves the organization or changes roles and no longer requires access.

12. Service account passwords must not be placed in ticket tracking systems.

13. Service accounts must not be allowed to log in to systems interactively (e.g. with a human at a keyboard, rather than systematically). If interactive logins are possible (e.g. Database administrators) then the passwords for such accounts must be changed every 90 days in line with the privileged/administrator account requirement (refer to Section 3.8.3 Admin Account/Privileged Accounts).

14. Service accounts must not be given interactive root or local administrator rights.

15. Service accounts must have the minimum access (least privilege) required to run properly.

16. Service accounts must not be used as a group, team, or universal administration account.

17. All default service account passwords must be changed upon installment of the system or application and prior to launch in a production environment.

3.8.2 USER ACCOUNT PASSWORDS

The following are requirements for User accounts on systems supporting T-Mobile or systems accessing T-Mobile’s environment. (These requirements are not intended for T-Mobile Customers – see Section 3.15 Customer-Facing Applications, Systems and Activities.)

1. Systems must enforce strong User passwords to:
   a. contain a minimum of eight (8) characters;
   b. require a mixture of both upper and lower case characters;
   c. include at least one number, and;
   d. include at least one special character (where technically feasible).

2. Passwords must not be shared.

3. Systems must:
   a. Prevent re-use of the five (5) previously-used passwords.
   b. Reset first-time passwords to a unique value for each User and force password to be changed on first use.
   c. Lock screens and require Users to re-enter their password after no more than thirty (30) minutes of idle activity.
d. Prevent passwords from displaying in clear text when being entered.

e. Enforce password changes at least every ninety (90) days.

f. Allow Users to select and change their own passwords and include a confirmation procedure to allow for input errors.

g. Automatically disable portable identification credentials (e.g. smart cards, identity tokens, RSA keys) that require the provision of a password to operate after five (5) consecutive invalid attempts. Systems must require an authorized administrator to unlock or reset the password on the locked account after proper authentication of the User.

h. Lock a User account after five (5) consecutive invalid login attempts and reset the password on the locked account after proper authentication of the User or a thirty (30) minute lock-out period.

4. User credentials (e.g. User ID and password) must be hashed or encrypted during the authentication process when transmitted using a secure communications channel (refer to Section 3.3 for Encryption Requirements).

5. Passwords/authentication data must be hashed at rest any time the password is stored (e.g. written to a disk, file or database, and salting must be implemented where feasible).

6. All default passwords must be changed upon installment of the system or application, and prior to launch in a production environment.

3.8.3 **Admin Account/Privileged Accounts**

1. Admin/Privileged account passwords must be a minimum of fifteen (15) alphanumeric characters long, where technically feasible; where not technically feasible the system maximum must be used. If an account (privileged or other) has been compromised or suspected of being compromised, the affected passwords on systems must be immediately changed.

2. Privileged accounts (e.g. administrators) must be separated from User accounts.

3. Passwords of Admin/Privileged accounts must not be shared.

4. When a Privileged account User leaves the organization or changes roles, passwords must be changed immediately for all systems and administrative accounts to which the User had access.

5. Lock the account after five (5) consecutive invalid login attempts and reset the password on the account after proper authentication of the User or a thirty (30) minute lock-out period.

6. Group, shared, or generic accounts and passwords must not be used for system administration activities.

7. Passwords must be changed at least every ninety (90) days.

8. All default passwords must be changed upon installment of the system or application, and prior to launch in a production environment.

3.9 **Mobile Device Security**

This section applies to Users who transmit, receive, or store T-Mobile Restricted and/or Confidential Information (e.g. email, attachments to email) via mobile devices. Mobile devices include, but are not limited to, smart phones, tablets, or handheld computing devices.

1. Mobile devices should be set for a maximum timeout for the device/system to lock after fifteen (15) minutes of inactivity.

2. A data wipe (of T-Mobile Restricted and Confidential Information) must be performed:

   a. after ten (10) unsuccessful password or passphrase attempts;

   b. after device is reported lost/stolen;

   c. on decommissioned devices, and/or;

   d. upon termination of Supplier services.
3. Users must enable the password controls for a mobile device containing T-Mobile Restricted and/or Confidential Information. Passwords on devices must not be simple and must require at least a four (4) character password (e.g. cannot be "1234, 1111, 9999"). Where possible, use of complex passwords must take precedence over using PINs.

4. Users should change the handheld security password/passphrase at least every ninety (90) days.

5. Users should not have the ability to disable password protection on mobile devices.

   To enforce the above controls, it is recommended that Suppliers should use a Mobile Device Management solution.

3.10 Physical Controls

Physical security controls must be in place to protect T-Mobile Restricted and/or Confidential Information from unauthorized physical access, theft, and/or damage. The following controls are related to physical locations providing back-end services to T-Mobile, including but not limited to: data centers, call centers, collection agencies, financial services, invoice processing, etc.

1. All areas of the premises storing and/or processing T-Mobile Restricted and/or Confidential Information must be housed in secure areas and protected by a defined perimeter with appropriate security barriers and entry controls.

2. Facilities must be protected by intrusion alarms.

3. Alarms must be monitored twenty-four (24) hours per day, three hundred sixty-five (365) days per year.

4. Data centers must be equipped with dry fire suppression equipment or appropriate fire suppression equipment to prevent water damage to equipment supporting T-Mobile.

5. Access must be restricted to authorized personnel only.

6. Visitors must be required to present government issued photo identification prior to receiving access. Visitors awarded access to non-public areas must be escorted in any area supporting T-Mobile.

7. Visitor logs must be maintained and retained for at least thirty (30) days for locations providing back-end services to T-Mobile.

8. Visitor badges should expire at the end of the work day.

9. Access rights to facilities must be reviewed at least every ninety (90) days and updated as needed.

10. Access rights to facilities must be removed within seventy-two (72) hours upon employee/contractor voluntary termination, leave of absence, or those no longer requiring access. In the event of an involuntary termination, access must be removed immediately.

11. CCTV or other surveillance devices must be used to monitor individual physical access to sensitive areas and exterior entries where appropriate. The collected information must be reviewed and correlated with other entries. This data must be stored for a minimum of thirty (30) days for areas storing, processing, or transmitting T-Mobile Restricted and/or Confidential Information.

12. Physical access controls must exist for all network devices (e.g. wireless access points, gateways, and routers), data centers, telecommunications network facilities, and ancillary areas (e.g. generator, or UPS storage rooms); to ensure appropriate access by authorized individuals only.

3.11 Change Management

Ensure that changes to all systems and applications supporting T-Mobile are properly approved, developed, tested, and implemented in a controlled and consistent manner to provide a level of confidentiality, availability, and integrity consistent with the importance of the services provided.

1. Changes on all network devices, applications, systems, or databases include:
   a. Application changes – code or configuration
   b. Application patches
   c. System updates or patches
   d. Hardware changes
2. Documented change control process must exist to include:
   a. Technical documentation and relevant user manuals must be updated.
   b. Documented evidence of approvals and testing.
   c. Testing plans and results must be documented and retained.
   d. Back-out plans must be documented prior to implementation.
   e. Emergency change procedures must be documented to include an established emergency approval authority.

3.12 Vulnerability and Patch Management

1. Supplier must have documented auditable vulnerability and patch management processes in place for networks, hosts, and applications supporting T-Mobile including, but not limited to:
   a. System inventory
   b. Grouping and prioritization of technology resources
   c. Use of IT inventory and scope of related duties
   d. Managing remediation of vulnerabilities, threats, etc.
   e. Prioritizing vulnerability remediation
   f. Maintaining an organization-specific remediation database
   g. Testing remediation prior to deployment
   h. Deployment of vulnerability remediation
   i. Distribution of vulnerability and remediation information to administrators
   j. Verifying remediation was effective

2. Authenticated vulnerability scans must be performed for new systems/applications and/or enhancements to existing systems/applications prior to production deployment. Supplier must retain vulnerability scan results supporting T-Mobile systems/applications for at least twelve (12) months from the date of the scan.

3. Upon request, Supplier must provide T-Mobile a copy of the most recent technical vulnerability assessment for systems supporting T-Mobile. As defined in the contractual agreement T-Mobile may also request scans or perform scans on the Suppliers environment and any application that is being developed on behalf of T-Mobile.

4. Vulnerability scans must be performed at least every ninety (90) days for the following:
   a. Authenticated scans and un-authenticated scans must be performed for internal/external web applications, hosts, network and web applications.
   b. Un-authenticated scans must be performed for external host and network scans.

5. Vulnerability scans must be performed after any significant change in the network, host ,application or system environment such as:
   a. New system component installations
   b. Changes in network topology
   c. Firewall rule modifications
   d. Application/hardware/software updates

6. Rescans must be performed to ensure the identified vulnerabilities are corrected.

7. Network intrusion and monitoring systems must immediately send notification to administrative personnel of unusual activity and suspected compromises.

8. T-Mobile must be informed of vulnerabilities that may materially impact security as it relates to T-Mobile systems and data.
   a. High vulnerabilities (e.g. CVSS Base score of 7.0 or higher) must be remediated within thirty (30) days of vendor release/notification.
   b. Medium vulnerabilities (e.g. CVSS 6.9 to 4.0) - must be remediated within ninety (90) days of vendor release/notification.
9. Supplier must ensure systems and applications are not operated past their End of Support lifecycle. All
operating systems and applications must be on current, vendor supported versions (i.e. versions that still
receive patches and updates).
10. Suppliers must subscribe to vendor notifications of security threats and patches for each technology
platform/application supporting T-Mobile.
11. Secure Configuration Management - Suppliers must develop, maintain, and test security baseline
configurations (hardened configuration) for platforms supporting T-Mobile based on industry-accepted
system-hardening standards, which may include but are not limited to:
   a. Center for Internet Security (CIS)
   b. International Organization for Standardization (ISO)
   c. SysAdmin Audit Network Security Institute (SANS)
   d. National Institute of Standards Technology (NIST)

### 3.13 **Anti-Malware**

1. All systems supporting T-Mobile (e.g. external/internal servers, mobile computing systems, firewalls, web
application firewalls, routers, and end User equipment) must be installed with current anti-malware
software appropriate for their operating system, if applicable anti-malware technology exists.
2. All anti-malware software must be actively running, updated with current definitions, and capable of
generating logs. Centralized alerting must be enabled and monitored as part of the anti-malware solution.
3. End Users must not disable, bypass, or interfere with the anti-malware software security.
4. The anti-malware software must be enabled for periodic scans.
5. Alerts must be generated in the event that the anti-malware software is disabled on systems supporting
T-Mobile (e.g. external/internal servers, database servers, file servers, firewalls, web application firewalls
and routers).
6. Care should be taken to protect against the introduction of malicious code during maintenance and
emergency procedures which may bypass normal malicious code protection controls.
7. Quick response procedures must be formally documented to detail actions in the event of a malware
attack.

### 3.14 **Secure System and Software Development**

This section applies to systems or applications specifically developed for T-Mobile. *It does not apply to
commercial off-the-shelf software.*

1. To prevent errors, loss, unauthorized modification, or misuse of information in applications, appropriate
controls must exist to ensure correct processing. These controls must include the validation of input data,
internal processing, and output data.
2. Software applications must be developed based on industry best practices and include information
security throughout the software development life cycle (SDLC). T-Mobile may request documentation on
Supplier’s SDLC process. SDLC must use the following minimum guidelines:
   a. Defined duties based on job responsibility (refer to Section 3.16 Segregation of Duties).
   b. Separate development, test, and production environments.
   c. Application code must be limited to appropriate personnel.
   d. Remove test data, vendor default accounts, test accounts and passwords before production
systems become active or are released to customers.
   e. Where technically possible, use stored procedures rather than scripts.
3. Production data must NOT be used for development and testing.
4. Developers should have knowledge of secure coding techniques such as the OWASP Guidelines for web
development (http://www.owasp.org) or other industry known best practices.
5. A code review checklist should be followed to ensure the following elements, at a minimum, are addressed: structure, documentation, inputs, invalid characters, variables, arithmetic operations, loops and branches, defensive programming, error handling, access control, authentication and session management, efficiency, and support.

6. Custom application code must be reviewed as per Section 3.11 Change Management - to identify vulnerabilities prior to production release.

7. Applications must include strong authentication mechanisms, including the use of minimum password or PIN lengths (refer to Section 3.8 Password Complexity), lockout enforcement after five (5) consecutive incorrect login attempts, and logging and monitoring of failed login attempts. Additionally, where applicable, brute force prevention techniques, such as CAPTCHA, must be utilized to help mitigate automated password guessing attacks.

8. Custom Code developed for systems or applications supporting T-Mobile must be peer-reviewed, documented, and tested for security vulnerabilities as applicable, including, but not limited to, the following:
   a. Injection flaws (e.g. SQL injection)
   b. Cross Site Scripting (XSS)
   c. Broken authentication/session management (e.g. use of account credentials and session cookies)
   d. Insecure Direct Object Reference
   e. Cross Site Request Forgery (CSRF)
   f. Security misconfiguration
   g. Insecure cryptographic storage
   h. Failure to restrict URL access
   i. Insecure communications
   j. Insufficient Transport Layer Protection
   k. Un-validated redirects and forwards
   l. Buffer overflows
   m. Improper error handling

   T-Mobile may request the documentation related to such reviews and testing.

9. Applications must disable output of specific detailed error messages to the client (end User equipment) and display only a common generic message.

10. Applications dealing with T-Mobile Restricted and/or Confidential Information must be developed taking into consideration the sensitivity of the information being handled.
   a. T-Mobile Restricted Information must be masked during display in systems/applications where applicable (e.g. Social Security Numbers, bank account numbers, payment card numbers, passwords).
   b. Cookies created for T-Mobile business purposes must not contain User PII data, and must be encrypted and configured correctly. Sharing of cookies with third-parties must be as per the T-Mobile Privacy Policy.

3.15 Customer-Facing Applications, Systems and Activities

Requirements in this section are specific to systems or applications that are or will be accessed by existing or potential T-Mobile Customers:

1. Customer-facing applications, systems, and/or activities that utilize customer CPNI (Customer Proprietary Network Information) must meet CPNI compliance requirements as defined in T-Mobile’s CPNI policy, including practices for authentication of customers, notice of account changes, and unauthorized access incident tracking (refer to Definitions – Section 2.1 for additional description). Please contact your T-Mobile representative to determine if CPNI is in scope and request the CPNI Policy (TISD-1039), if applicable.
2. All projects/systems must be able to collect, track, and honor user preferences with respect to data collection. Specific requirements will be provided in project requirements documents or statement of work, and could include:
   a. the capability to display a prominent notice and obtain affirmative consent of the User when collecting sensitive information about them;
   b. capability to obtain and track consent and include links to detailed notice, or
   c. the option of opting out of data collection.

   Requirements will be driven in part by principles stated in the T-Mobile Privacy Policy.

3. A unique randomly generated password should be used for initial value or reset password. The system should require a password change on first authentication.

4. Only the Customer (or potential Customers) must have the ability to create their authentication credentials, except for temporary credentials.

5. Customer account passwords must be complex with a minimum of eight (8) alpha-numeric characters.

6. Customer passwords, including secondary passwords and answers to security questions, must be hashed (as per Encryption Requirements - Section 3.3).

### 3.16 Segregation of Duties

Segregation of duties (a.k.a. Separation of duties) refers to dividing roles and responsibilities so that a single person cannot subvert a critical process.

1. Software developers must not have access to write/update code in production systems. They may have read only access to such systems to perform their job responsibilities.

2. Software developers must not have access to migrate changes into the production environment (the purpose is to have segregation of duties, so if, for example, code is developed by one developer on the team, another developer on the team can migrate the code to production).

3. In the event of an emergency break fix in production, logging of access and events must occur (e.g. firefighter process). Once they are done, the person must document what changes were made associated to the event.

4. Development, testing, and production environments must be properly separated. Functionality and operations should not overlap.

5. Supplier-developed applications must be reviewed for vulnerabilities by individuals other than the developers of the application.

6. At no time shall a person be responsible for auditing the systems that they are also responsible for maintaining.

7. While implementing segregation of duties, the principles of least-privilege and need-to-know must be implemented.

### 3.17 Incident Reporting

Supplier must have the capacity to immediately notify T-Mobile of any Security Breach and must assist T-Mobile in investigating the Security Breach in accordance with terms of an approved contract, work order, or master service agreement. Supplier must have technical, administrative and physical security measures in place so that vulnerabilities are disclosed responsibly, and that information about a Security Breach impacting T-Mobile information is not disclosed to the public until authorized to do so by T-Mobile.

### 3.18 Call Centers

This section applies to Suppliers (Service Partners) performing Call Center activities on behalf of T-Mobile, related to existing or prospective T-Mobile Customers.

1. Call center production floor environments must be paperless and not allow for the printing of T-Mobile information, unless pre-approved in writing by T-Mobile.
2. Devices that may record audio, video and images (e.g. cameras, mobile devices) are not permitted on call center production floor environments, unless pre-approved in writing by T-Mobile. If Supplier uses audio, video, or image recording devices for call center security, use of such devices shall be in compliance with applicable law, and any recordings of call center activity must be stored with reasonable security safeguards and access controls to limit access to authorized investigative personnel.

3. Call center computers supporting T-Mobile must be configured to prevent Users/agents from storing T-Mobile non-public information to their computer or to removable media (e.g. tapes, disks, USB drives, removable external hard drives, CDs, DVDs).

4. Call center computers supporting T-Mobile may only electronically connect to approved communication and support systems. Access to the Internet is generally not permitted, though may be allowed subject to the call center passing certain security controls and in agreement with contractual terms acceptable to T-Mobile.

5. Instant Messaging applications must be pre-approved for use by T-Mobile in writing for those Users/agents who access T-Mobile Restricted and/or Confidential Information.

6. Call Centers handling T-Mobile’s Customer Proprietary Network Information (CPNI) must have T-Mobile’s annual security and privacy awareness training programs for workers with access to CPNI. Training sessions must be conducted and materials distributed to personnel prior to commencement of services for T-Mobile. Please contact your T-Mobile representative to determine if CPNI is in-scope and request assistance if needed.

3.19 SECURITY & PRIVACY AWARENESS
Suppliers with access to T-Mobile Restricted and/or Confidential Information must have annual security and privacy awareness training programs based on the relevant role and responsibilities within the organization.

3.20 EXCEPTIONS/INABILITY TO MEET STANDARDS
In the event the Supplier is unable to meet any of the requirements in this Standard TRS-610, please notify ESRAP@T-Mobile.com to discuss compensating controls or to determine if mitigation is required.

4 REFERENCES
1. TISS-310 Information Classification Standard
2. T-Mobile Privacy Policy
3. TISD-1039 Handling Customer Proprietary Network Information (CPNI)
4. TLS-210 Records Retention Schedule Standard