Enterprise Third-Party (Supplier) Information Security Standard

Approved by: Cyber Security & Privacy Policy Approver

1 HERE'S THE DEAL

The purpose of this TISS-610 Enterprise Third-Party (Supplier) Information Security Standard ("Standard") is to define T-Mobile's third-party information security requirements that help meet T-Mobile's overall risk management and security objectives.

Note – This Standard is aligned to the Enterprise Third-Party (Supplier) Risk Management Program. T-Mobile will complete an Enterprise (Supplier) Risk Management Program (ESRAP) intake for all Suppliers. The Cyber Assessment is triggered based off the results of the ESRAP intake.

2 WHAT'S IN-SCOPE

This Standard applies to all T-Mobile Third-Parties (suppliers) and T-Mobile personnel responsible for managing the supplier(s). This standard defines the security requirements that must be evaluated upon collaborating, changes in-scope-of-work and changes in the vendor security environment.

Third-Parties (Suppliers) includes, but not limited to, those performing any of the following:

1. Accessing, hosting, retaining, processing, or transmitting non-public T-Mobile information.
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.

3 ROLES & RESPONSIBILITIES

3.1 SUPPLIER

Supplier is responsible for completing cyber assessment questionnaire and adhering the security requirements in this Standard to implement appropriate technological, procedural, and physical requirements controls to protect T-Mobile customers.

3.2 T-MOBILE'S SUPPLIER CYBER RISK MANAGEMENT (SCRM) TEAM

SCRM partners with T-Mobile's Enterprise (Supplier) Risk Management Program (ESRAP) to ensure T-Mobile meets certain compliance and regulatory obligations to protect T-Mobile customers and information, as defined in the Scope. As part of T-Mobile's broader Digital Security Organization (DSO), SCRM performs detailed Cyber Assessments to ensure suppliers are compliant with the Standard.

4 T-Mobile Third-Party (Supplier) Information Security Requirements

4.1 Information Handling Requirements

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

4.1.1 Information Classification

T-Mobile has defined an information classification scheme to properly identify all T-Mobile information. The information classification levels are used throughout this Standard. T-Mobile will determine the classification of the information you will be accessing, processing, and/or storing. Suppliers with multiple engagements at T-Mobile, must adhere to the requirements of the highest classification level they will be accessing, processing, and/or storing.

4.1.2 Information Handling for Customer Facing Applications, Systems and Activities

1. Customer-facing applications, systems, and/or activities that utilize Customer Proprietary Network Information (CPNI) must meet CPNI compliance requirements as defined in T-Mobile's CPNI requirements including practices for authentication of customers, notice of account changes, and unauthorized access incident tracking.
2. All systems/applications must be able to collect, track, and honor user preferences with respect to data collection including, but not limited to:
    a. 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 a detailed notice, or
    c. Provide the option of opting out of data collection.
3. CPNI information must be stored within the boundaries of the United States.

4.1.3 Disposal of information Assets

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 SCRM@T-Mobile.com for the form.

When destruction is carried out by a disposal vendor, it is essential the information is protected continuously from the time at which the information asset is sent for destruction, until the time the disposal vendor has picked up the data.

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

Information Assets	Disposal Method
Paper	Cross-cut shredding, incinerating, or pulping such that there is reasonable assurance the materials cannot be reconstructed.
Mobile Computing Devices (cell phones, tablets, etc.)	Delete all non-public T-Mobile information on the device(s).
Electronic Storage Media (hard drives, USB/memory sticks, RAM, tapes, etc.)	Physically destroy or sanitize media in accordance to NIST-800-88 Guidelines for Media Sanitization and verify removal of data.
Optical Disks (CDs, DVDs, etc.)	Use optical disk shredder or disintegrator. Disks can also be incinerated or grinders can be used.

4.2 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.

4.3 Encryption Requirements

Encryption technologies must be used to protect T-Mobile Confidential and/or Restricted information. T-Mobile Confidential and/or Restricted data must be encrypted at rest and in-transit (over public data networks and/or within the Supplier's internal network).

1. Information Transmission: SSHv2, TLS1.2 or higher.
2. Encryption Standard: AES, RSA
    a. At Rest:
        i. Symmetric: AES 256 or higher
        ii. Asymmetric: RSAES-OAEP
    b. In-Transit:
        i. HTTPS, SSH, SFTP, Direct connection (dedicated circuit only for your scope of work with T-Mobile).
3. Usage of Proprietary Encryption Algorithm(s): must be reviewed, tested, and approved by T-Mobile.
4. Hashing Algorithm/Password Storage: SHA 2, Bcrypt, Scrypt, Other (upon approval of T-Mobile)
5. Wireless Networks: WPA2 (WPA1 and WEP must not be used)
6. MD5 and less must not be used

7. Unique T-Mobile encryption keys should be used for encryption of T-Mobile Confidential and/or Restricted information, where possible.
8. Salts must be random per user and a minimum of 16 characters in length.
9. User credentials must be encrypted during the authentication process when transmitted using a secure communications channel.
10. Passwords/authentication data must be hashed at rest any time the password is stored. Passwords must not be stored or transmitted in clear text (human readable form).

4.3.1 CRYPTOGRAPHIC REQUIREMENTS

Supplier must have clearly defined and documented processes for managing cryptographic keys.

1. Keys must be physically protected.
2. Keys must never be stored in locations that do not meet secure key management requirements.
3. Keys must be changed annually. Old keys must be retired or destroyed.
4. For high security keys, dual control or MFA must be implemented.
5. Key access must be restricted on a need to know basis.
6. Keys must be changed when employees with key access change job duties or leave the company.
7. Supplier using T-Mobile DNS domains must get their SSL/TLS certificates from T-Mobile.
8. All certificates used for T-Mobile purposes must have minimum key lengths of at least 2048 bits (RSA).
9. Passwords used to protect cryptographic keys must be as strong as the keys they protect.

4.4 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. Quick response procedures must be formally documented to detail actions in the event of a malware attack.
3. 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.
4. End Users must not disable, bypass, or interfere with the anti-malware software security.

4.5 FACILITIES – PHYSICAL SECURITY

Physical security controls must be in-place to protect T-Mobile non-public information from unauthorized physical access, theft, and/or damage. The following controls are related to physical locations providing services to T-Mobile, including but not limited to: data centers, call centers, collection agencies, financial services, single tenant offices, multi-tenant offices, invoice processing, etc.

1. T-Mobile non-public information must be physically secured when not in use, including but not limited to, papers, manuals, and electronic media.
2. All areas of the premises storing and/or processing T-Mobile non-public information must be housed in secure areas and protected by a defined perimeter with appropriate security barriers and entry controls.
3. Facilities must be protected by intrusion alarms.
4. Alarms must be monitored twenty-four (24) hours per day, three hundred sixty-five (365) days per year.
5. Data centers must be equipped with dry fire suppression equipment or appropriate fire suppression equipment to prevent water damage to equipment supporting T-Mobile.
6. Access must be restricted to authorized personnel only.
7. Visitors must be required to present government issued photo identification prior to receiving access. Visitors awarded access to non-public areas must be escorted at all times in any area supporting T-Mobile.
8. Visitor logs must be maintained to provide an auditable trail of visitor activity. Visitor logs must be readily available for one year.
9. Visitor badges must expire automatically at the end of the work day.
10. Access rights to facilities must be based on business need and regularly reviewed and updated.
11. Access rights to facilities must be removed immediately upon notification of separation or a change in job responsibilities that no longer require physical access to the facility.
12. 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 non-public Information.
13. 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.

4.6 Change Management

Suppliers must have documented change management processes. Changes to all systems and applications supporting T-Mobile must be 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
    e. Emergency changes
    f. Production data 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.

4.7 Network Security

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 SCRM@T-Mobile.com for determination of acceptable mitigation.

1. Appropriate network security controls 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 on a least-privilege basis.
2. Network 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 related to systems supporting T-Mobile must be reviewed and approved by Supplier's management at least every 6 months.

4.8 Data Access Management

1. The Supplier is responsible and accountable for managing assets containing T-Mobile non-public information that are under the Supplier's control, and responsible for security controls relevant to any Supplier access to such assets.
2. Supplier with access to T-Mobile Confidential and/or Restricted information must have annual security and privacy awareness training programs based on the relevant role and responsibilities within the organization.

3. 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.
4. 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.
5. Back-up data containing non-public T-Mobile information must be segregated (physically or by using unique identifiers) from Supplier's information and Supplier's client's/customer's information with appropriate access controls to prevent unauthorized access.
6. If mobile devices will be utilized to transmit, receive, or store T-Mobile non-public information, a mobile device management solution must be used with the capability to remotely lock and wipe lost/stolen devices and to enforce disposal of information.

4.8.1 Logical Access Controls

1. Access right to systems accessing, processing, and/or storing T-Mobile non-public information must be granted on a least privilege basis. Access rights must be reviewed at least every 90 days. Inactive User accounts with no activity for more than 90 days must be removed and/or disabled.
2. Remote access to T-Mobile's environment(s) must be approved by a management-level single point of contact of the Supplier that will be responsible for enforcing T-Mobile security requirements.
3. MFA must be implemented for all remote elevated (privileged) network access for systems supporting T-Mobile.
4. User IDs must be unique and assigned to specific individuals.
5. User access rights to systems or information supporting T-Mobile must be deactivated within 72 hours upon Supplier's employee/contractor voluntary termination 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.

4.8.2 Password Complexity

1. Passwords (including default passwords) must be changed upon installment of the system or application, prior to launch in a production environment.
2. Group, shared, or generic accounts and passwords must not be used. Accounts must have an identified owner.
3. Passwords must not be displayed in clear text when being entered.
4. Systems must maintain a record of previous passwords and prevent re-use of at least the last 5 previously-used passwords.
5. Systems must lock accounts (User, Admin/Privileged, Service) after 30 minutes of idle activity or after 5 consecutive invalid login attempts.

The following are requirements for Account Types supporting or accessing T-Mobile environments.

Account Type	Requirements
User	1. Passwords must contain a minimum of 8 characters, and require: a mix of upper and lower case characters, include at least 1 number, and include at least one special character. 2. First time passwords must be a unique value and system must force password change on first use. *Note: If User chooses first password value, system does not need to force password change on first use.* 3. Password changes must be forced at least every 90 days.
Admin/ Privileged	1. Passwords must contain a minimum of 15 characters or, if not technically feasible, the system maximum. Passwords must meet the same complexity requirements as User accounts. 2. Admin/Privileged accounts must be separate from User accounts. 3. Passwords must be changed for all systems and user administrative accounts user had access to when user leaves organization or changes roles. 4. Password changes must be forced at least every 90 days.
Service (aka system passwords)	1. Passwords must contain a minimum of 30 characters (60 is preferred), and must meet same complexity requirements as User accounts. A password generation tool should be used to generate randomized passwords. 2. Must not be given interactive root or local administrator rights. 3. Passwords must be changed at least annually, or earlier in the case of security issues. 4. Passwords must not be shared beyond those with a demonstrated need to know. 5. Systems must not be able to select and change its own service account passwords. 6. Passwords must be immediately changed when a person with knowledge leaves the organization or changes roles. 7. Passwords must not be placed in ticket tracking systems.

	8. Must only be used for their approved service and not shared with systems/applications for which they were not provisioned.

4.8.3 Segregation of Duties

Segregation of duties (aka 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/migrate code or changes to code in production systems.
2. Users must not be responsible for auditing the systems they are also responsible for maintaining.
3. While implementing segregation of duties, the principles of least privilege and need-to-know must be implemented.

4.9 Secure System and Software Development

Note: This section applies to systems or applications specifically developed or customized for T-Mobile. It may not apply to commercial off-the-shelf software without any customization.

1. Software applications must be developed based on industry best practices and include security through 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.
    b. Separate development, test, and production environments.
    c. Application code must be limited to appropriate personnel.
    d. Test data, vendor default accounts, tests accounts and passwords must be removed before production systems become active or are released to customers.
    e. Production data must not be used for development and testing.
    f. Secure code review checklist followed to ensure the following elements 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.
2. Applications must have strong authentication mechanisms, including user of minimum passwords or PIN lengths, lockout enforcement after 5 consecutive invalid login attempts, and logging and monitoring of failed login attempts.
3. Custom code must be peer reviewed, documented, and tested for security vulnerabilities. T-Mobile may request the documentation related to such reviews and testing.
4. Applications with non-public T-Mobile information must be developed taking into consideration the sensitivity of the information being handled.

a. Information must be masked during display in systems/applications where applicable (e.g., Social Security Numbers, bank account numbers, payment card information, passwords)
b. Cookies created for T-Mobile purposes may not be linked or linkable to an identifiable individual and must be encrypted and configured correctly. Sharing of cookies with third-parties must be as per the T-Mobile Privacy Policy.

5. For customer facing applications, customer (or potential customers) must have the ability to create their authentication credentials, except for temporary credentials

4.10 VULNERABILITY & PATCH MANAGEMENT

Supplier must have documented, auditable vulnerability and patch management processes in-place for networks, hosts, and applications supporting T-Mobile. Processes must include, but are not limited to:

1. 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.
2. Authenticated vulnerability scans must be performed for new systems/applications and/or enhancements to existing systems/applications prior to production deployment.
3. Supplier must retain vulnerability scan results supporting T-Mobile systems/applications for at least twelve (12) months from the date of the scan. Supplier must provide T-Mobile a copy of the most recent technical vulnerability assessment for systems supporting T-Mobile.
4. 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) and Supplier must subscribe to vendor notifications of security threats and patches for each system/application supporting T-Mobile.
5. 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.
   c. Lower risk vulnerabilities (e.g., CVSS below 4.0) - must be remediated within one hundred eighty (180) days or as requested by T-Mobile.
6. Suppliers must develop, maintain, and test security baseline configurations (hardened configuration) for platforms/systems supporting T-Mobile based on industry-accepted standards (i.e., CIS/SANS, ISO, NIST).

4.11 AUDITING & LOGGING

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

1. T-Mobile Confidential and/or Restricted data must not be contained in log files.
2. Procedures must ensure system activities are monitored for authorized use, access, and logging.
3. Level of auditing & logging must take into consideration the criticality of the application/process/system, the value, sensitivity and criticality of the information involved, 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, service accounts, unauthorized access attempts, systems alerts or failures, initialization of the audit logs, changes to or attempts to change system security settings and controls, errors and faults.
5. All events in the logs must be time-stamped. System times (clocks) must be synchronized via NTP (Network Time Protocol) to ensure accuracy of logs.
6. 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 6 months.

4.12 SERVICE PARTNER CALL CENTERS

This section applies to Suppliers performing Call Center activities on behalf of T-Mobile related to existing or prospective T-Mobile customers. For Call Center physical security requirements refer to section 4.5.

1. The following is only allowed on production floors if pre-approved by T-Mobile in writing:
   a. Paper and the ability to print T-Mobile information.
   b. Usage of devices that may record audio, video and images. Any use of such equipment must comply with applicable law, and must be stored with security safeguards and access controls to limit access on a least-privilege basis.
   c. Access to the Internet
   d. Usage of Instant Messaging applications by agents with access to T-Mobile Confidential and/or Restricted information.
2. Computers supporting T-Mobile may only electronically connect to approved communication and support systems.
3. Call Centers handling T-Mobile's CPNI must have T-Mobile's annual security and privacy awareness training for workers with access to CPNI. Training sessions must be conducted, and materials distributed to personnel prior to commencement of services for T-Mobile. T-Mobile will determine if CPNI is in-scope.

4.13 External Audits

1. T-Mobile may request evidence of external audits and certifications.
2. Suppliers in scope for Sarbanes Oxley (SOX) and/or financial services must provide SSAE 16 or 18 SOC 1, Type 2 report upon request.
3. All suppliers in-scope for T-Mobile's PCI program must provide proof of PCI compliance, including but not limited to, their most recent (within the last 12 months) Attestation of Compliance for the scope of services supporting T-Mobile, for e.g., locations, payment applications, third-party service providers. T-Mobile reserves the right to request additional information/documentation, for e.g., Report on Compliance, Self-Assessment Questionnaire, compensating control worksheet, as needed. Supplier will document which PCI requirements they manage on behalf of or in coordination with T-Mobile.

5 Questions? - Get Help

- Contact SCRM@T-Mobile.com with any questions.

6 Exceptions

All cases of non-adherence to a T-Mobile Information Security policy, standard or procedure must be reported to SCRM@T-Mobile.com for evaluation. All material Supplier risks associated with T-Mobile customers, systems, and data must be treated and disclosed to T-Mobile (SCRM@T-Mobile.com).

7 More Info

1. T-Mobile Privacy Policy
2. Supplier Code of Conduct
3. T-Mobile CPNI Information