INFORMATION SECURITY EXHIBIT

This Information Security Exhibit describes T-Mobile's Information Security Program.

T-Mobile has implemented administrative, technical, and physical safeguards designed to protect the confidentiality, integrity, and availability of its systems, networks, and information. T-Mobile's information security procedures are informed by industry-best practices and the NIST Cyber Security Framework.

To the extent this Information Security Exhibit conflicts with your services agreement with T-Mobile ("Agreement"), this Information Security Exhibit will control. T-Mobile's security procedures are subject to change without notice, including changes to comply with Applicable Law and to maintain conformance with industry-best practices. The invalidity or unenforceability of any provision in this Information Security Exhibit will not affect the other provisions hereof, all of which will remain enforceable in accordance with their terms.

Definitions

For purposes of this Information Security Exhibit, the following terms have the meanings specified below:

(a) "**Covered Incident**" means Security Incident impacting Customer Data protected under applicable state or federal breach reporting laws or regulations to the extent such data is in T-Mobile's possession or under its control.

(b) "**Customer Data**" means data provided by or on behalf of Customer to T-Mobile or obtained by T-Mobile through Customer's use of the Services to the extent such data is in T-Mobile's possession or under its control. Customer Data does not include data created, stored, transmitted, accessed, or used through third-party products or websites.

(c) **"Information Security Program"** means, collectively, programs T-Mobile has in place, including any updates or modifications to such programs, that (a) address privacy and security risks related to the development and management of T-Mobile products and services that process Personal Data (as defined in the Agreement); and (b) are designed to protect the privacy and confidentiality of Confidential Information (as defined in the Agreement), In each case, T-Mobile's Information Security Program contains controls and procedures appropriate to T-Mobile's size, complexity, the nature and scope of activities, and the sensitivity of information processed.

(d) **"Security Incident"** means a data breach, security breach, or similar terms as defined by applicable state or federal laws or regulation that require individual notification in the event of unauthorized access to or acquisition of data protected by such laws and regulations.

Cyber Certifications, Audits, Scorecards, and Accolades

1. **T-Mobile's Trust Center**
    a. T-Mobile maintains a Trust Center, security.t-mobile.com, which provides security documents, assessments, third-party scorecards, and certifications in a self-serve format. The Trust Center also contains information on data security practices, continuity, and other elements of cybersecurity, along with links to T-Mobile's Annual Reports, privacy notices, and access controls.

Administrative Security Measures

2. **Executive Oversight**
    a. T-Mobile's Chief Security Officer (CSO) is responsible for T-Mobile's data security processes. The CSO implements, supervises, and maintains the Information Security Program including daily operational protocols through their reports and assignees.
3. **Vendor Risk Management**
    a. T-Mobile's relationships with third party suppliers and vendors are governed by T-Mobile's Supplier Policies, including the Supplier Code of Conduct, Third-Party Information Security Policy (TISP 600), and Supplier Data Processing Requirements.
        i. T-Mobile's Third-Party Information Security Policy dictates that third parties must have an information security program appropriate for their industry, size, and maturity.

b. T-Mobile also operates a Third-Party Risk Management ("TPRM") Program designed to ensure that the vendors and suppliers meet our high standards for security, compliance, and operational integrity.

i. Pursuant to T-Mobile's TPRM program, T-Mobile evaluates third-party service providers' capability to implement and maintain specific security measures proportionate to the level of access T-Mobile grants the third party.

4. **Security Policy**
   - **a.** T-Mobile has a Cyber Policy Management Program, which governs a comprehensive catalogue of written policies, standards, and details that outline the organization's security controls and governance of the Information Security Program.
   - **b.** T-Mobile reviews the security policies periodically and on an ad hoc basis where a material change in T-Mobile's business practices requires updates to documentation.
5. **Security Awareness and Training**
   - **a.** T-Mobile maintains a security awareness training program for T-Mobile employees and those contractors who have been provisioned T-Mobile credentials.
     - **i.** New employees and in-scope contractors are assigned security training at the time of hire or engagement, and no less than annually thereafter.
     - **ii.** Additional targeted, role-based security training is provided to individuals in roles that entail increased security risks.
   - **b.** T-Mobile's security training curriculum is reviewed on a regular basis and updated when needed.
6. **Personnel Security**
   - **a.** Upon hire, T-Mobile performs background screening on certain employees who have access to Customer Data, subject to applicable law.
7. **Risk Assessment**
   - **a.** T-Mobile conducts regular cyber security risk assessments to evaluate current risks to the organization's operations, assets, and individuals, and to support risk-based decision making.
   - **b.** T-Mobile aligns its risk assessment practices with industry-recognized standards and performs risk assessments at least annually, evaluating key cybersecurity domains and risks associated with those domains.

Physical Security Measures

8. **Data Centers**
   - **a.** At data center facilities, T-Mobile implements robust physical security measures that include enterprise badging and access control systems, alarm monitoring, CCTV systems, physical barriers, strict visitor management protocols, unarmed guards, and secure and locked data cabinets.
   - **b.** T-Mobile regularly assesses its physical security practices as threats change and new safeguards and technologies become available.
9. **Access to Facilities**
   - **a.** T-Mobile maintains physical security measures, operational procedures, and vendor security standards to prevent unauthorized physical access to Customer Data at T-Mobile locations. These security measures vary by location, depending on the facility or area, the type and amount of data or equipment stored, and the risk profile associated with the location.
10. **Secure Disposal**
    - **a.** T-Mobile maintains an asset management standard that addresses the destruction or disposal of sensitive materials stored on physical assets.

Technical Security Measures

11. **Access Controls**
    - **a.** T-Mobile maintains access controls designed to safeguard Customer Data by:
      - **i.** Implementing strong user authentication for system access;

ii. Ensuring that production infrastructure includes appropriate user account and password controls (e.g., the required use of VPN connections, complex passwords with expiration dates, and a two-factor authenticated connection);
iii. Assigning unique IDs to each employee and contractor with access to the T-Mobile corporate network;
iv. Managing access privileges based on job requirements and revoking permissions in a timely manner upon termination of employment or consulting relationships; and
v. Restricting user access to Customer Data based on the principles of least privilege.

12. **Identity Management and Authentication**
    a. T-Mobile maintains an identity management and authentication program that:
        i. Limits access to physical and logical assets to authorized users, processes, and devices;
        ii. Manages access permissions and authorizations;
        iii. Meets or exceeds industry standards for applicable minimum digital identity standards (e.g., password complexity, multi-factor authentication);
        iv. Employs phish-resistant multi-factor authentication where technically feasible for privileged accounts, critical infrastructure, and information systems that store or process Customer Data; and
        v. Prohibits the use of default passwords.
    b. T-Mobile implements measures to authenticate the Customer or the Customer's authorized representatives prior to disclosing Customer Proprietary Network Information (CPNI) based on applicable law, industry best practices, or as requested by Customer.
13. **Logging and Monitoring**
    a. T-Mobile maintains a security logging and monitoring program to maintain situational awareness of its network and endpoints through comprehensive and continuous monitoring activities.
        i. T-Mobile monitors cybersecurity logs via its Security Information and Event Management (SIEM) tools to analyze, identify, and respond to anomalies or suspicious activity.
    b. T-Mobile requires its security teams to review logs to manage and identify anomalies or suspicious activity that include, but are not limited to:
        i. Security events;
        ii. Logs of system components that store, process, or transmit Customer Data or that could impact the security of Customer Data;
        iii. Logs of identified T-Mobile critical systems, applications, and services; and
        iv. Logs of servers and system components that perform security functions.
14. **Firewalls**
    a. T-Mobile uses industry-standard firewall technology to secure its network perimeter and to inspect ingress and egress connections routed through the environment.
    b. T-Mobile uses firewalls and routers to restrict connections between untrusted networks and any system components within the network.
        i. These firewalls and routers work to restrict connections between trusted data centers, servers, applications, production and non-production environments, and endpoints to ensure security from within T-Mobile's network.
    c. To the extent that network traffic traverses T-Mobile's corporate network, T-Mobile enforces an "approve by asset" approach to managing ports between assets that facilitate data transmission.
        i. Consistent with the principle of "deny by default," T-Mobile ensures that no ports on firewalls or boundaries between assets are open without an explicit and approved request.
        ii. Requests to open ports must be accompanied by a documented business justification, ensuring that access is necessary and justified.
        iii. The "approve by asset" methodology does not apply for applications or systems that are hosted off T-Mobile premises.

15. **Vulnerability Scanning and Management**

a. T-Mobile maintains a vulnerability management program that leverages industry-recognized methods to strengthen its infrastructure against evolving attack vectors.
b. New security vulnerabilities are identified using industry-standard sources for security vulnerability information, including alerts from international and national Computer Emergency Response Teams (CERTs), or similar organizations.
    i. T-Mobile-managed network and system assets are scanned weekly.
    ii. Additionally, T-Mobile performs ongoing scans for vulnerabilities in systems and hosted applications, as well as ad hoc scans when new vulnerabilities that could potentially affect systems and applications are identified and reported.
c. Assessments of new vulnerabilities are informed by the Common Vulnerability Scoring System (CVSS). Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact.
d. New, public internet-facing systems are scanned prior to connecting to public internet.

16. **Antivirus**
    a. T-Mobile updates antivirus, anti-malware, and anti-spyware software at regular intervals and centrally logs events to track the effectiveness of such software.
17. **Change Management**
    a. T-Mobile maintains change management practices to reduce the risks associated with unauthorized or improper changes.
    b. Changes to T-Mobile systems and applications are properly approved, developed, tested, and implemented to provide the highest levels of confidentiality, availability, and integrity.
18. **Encryption**
    a. T-Mobile maintains a NIST-aligned enterprise Cryptographic Key Management System that is designed to help ensure the keys used to protect Customer Data against loss, unauthorized access, or unintended disclosure are also well protected.
    b. T-Mobile's data classification and handling standards dictate controls, including encryption or hashing where appropriate, for securing customer data in storage, In use, and in transmission.
    c. Where T-Mobile encrypts data, it uses multiple types of symmetric algorithms to encrypt data at rest or in use. T-Mobile employs encryption techniques that meet or exceed industry standards
    d. T-Mobile isolates encryption keys from the applications and users that access Customer Data.
19. **Data Management**
    a. T-Mobile classifies data based on sensitivity, value, and criticality in accordance with its information security policy suite. This classification supports the implementation of appropriate protection measures and compliance with applicable legal and regulatory requirements.
    b. T-Mobile applies data handling guidelines that promote consistent and secure use of data across the enterprise.
    c. T-Mobile retains, stores, and disposes of data in alignment with its enterprise information governance and retention policies.
    d. T-Mobile may retain Customer Data if:
        i. Required by applicable law or regulatory authority with jurisdiction over T-Mobile; or
        ii. Necessary to provide post-termination services to Customer; or
        iii. Permitted under T-Mobile's information governance and data retention policies.
20. **Patch and Security Update Management**
    a. T-Mobile has a vulnerability and patch management program that works to ensure that:
        i. Updates to software and firmware are managed by T-Mobile's IT department, remediated according to published patching processes, and automated wherever possible.
        ii. System components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed;
        iii. Security updates are installed according to risk and severity, assigning Critical vulnerabilities a 15-day window and High vulnerabilities a 30-day window.
21. **Penetration Testing**

a. T-Mobile employs penetration testing (pen testing) to help ensure the security of its networks and systems.
b. Pen testing for certain assets is performed by request and on a documented regular schedule to identify system and application control weaknesses based on regulatory requirements or business impact.
    i. Internal and external pen testing occurs at least annually and, if relevant, after any significant infrastructure or application upgrade or modification.
    ii. New, public internet-facing systems are scanned prior to connecting to public internet.

22. **Data Backup and Resiliency**
    a. T-Mobile maintains a backup and cyber data resiliency program designed to safeguard digital assets, mitigate data loss risks, and help ensure swift recovery in the event of cyber incidents or system failures.
23. **Asset Management**
    a. T-Mobile maintains an asset inventory program appropriate for its size and maturity that:
        i. Maintains technology asset repositories that establish an inventory of critical assets and software;
        ii. In accordance with T-Mobile policy, helps ensure that technology assets are properly managed throughout the lifecycle of the asset, from procurement through disposal, in T-Mobile structured and semi-structured databases regardless of environment; and
        iii. Helps ensure removable media is protected and used in a restricted manner according to T-Mobile's policy.
24. **Business Continuity and Disaster Recovery**
    a. T-Mobile maintains, and tests at regular intervals, a business continuity and disaster recovery program so that T-Mobile can resume or continue operations in a timely manner under adverse or abnormal conditions.
25. **Responsible Disclosure**
    a. T-Mobile prioritizes methods to acknowledge and respond to security researchers who have identified potential vulnerabilities; and
    b. T-Mobile has a bug bounty program that incentivizes a crowdsourced effort to identify and remediate vulnerabilities before bad actors exploit them.
26. **Incident Response & Covered Incidents**
    a. T-Mobile maintains a robust cybersecurity incident response and handling program designed to detect, analyze, contain, mitigate impact, and recover from incidents resulting from cyber threats.
    b. T-Mobile's incident response program:
        i. Documents the identification, management, and resolution of operational and security issues;
        ii. Supports investigating teams in communicating the status of cyber incidents to internal stakeholders; and
        iii. Includes post-incident reviews to improve the effectiveness of T-Mobile's Information Security Program.
    c. T-Mobile promptly and reasonably investigates cyber incidents, including potential or suspected Security Incidents, and takes remedial actions as necessary;
    d. In the event of a Covered Incident, T-Mobile will:
        i. Identify an employee to serve as Customer's primary information security contact (a "T-Mobile Account Representative"). The T-Mobile Account Representative will be reasonably available to the Customer for the purpose of responding to Customer inquiries associated with a Covered Incident;
        ii. Excepting legal demands or obligations that preclude T-Mobile from providing notice, notify Customer of a Covered Incident promptly and no later than required by applicable law;
        iii. Notify Customer of a Covered Incident by e-mailing Customer at (i) the email notification address identified in Notices section of the Agreement, (ii) in a manner reasonably

calculated to promptly notify Customer, or (iii) by any manner mutually agreed to by the parties;

iv. Cooperate with Customer, including, without limitation, respond to Customer's reasonable inquiries;

v. Unless required by Applicable Law or court order, T-Mobile will not publicly disclose whether Customer was impacted by a Covered Incident without the prior written consent of Customer.

vi. Reasonably cooperate with Customer in any litigation or regulatory proceeding that results from a Covered Incident.