CUSTOMER PROPRIETARY NETWORK INFORMATION POLICY

T-Mobile’s customers have a right, and we have a duty, under federal law, to protect the confidentiality of customer proprietary network information or “CPNI.” Meeting this obligation is the responsibility of every employee and each of us must ensure that we only access, use, or disclose CPNI as required or permitted by law, this Policy, and our operating procedures.

**Defining CPNI:** CPNI includes network information collected about T-Mobile customers’ use of telecommunications services. CPNI includes data such as “call detail information” (information that identifies the caller, the recipient, the number called or the number of any participant to the call, the duration of the call, the location from which a call was made, the number of calls answered or not answered, the cost, or the time of day – all organized by individual customer phone number), details regarding sending or receiving SMS/MMS messages (as opposed to message content), minutes used/remaining, account charges and balance, rate plan, and the features to which a customer subscribes or uses.

**Informing our Customers:** When it comes to personal information, including CPNI, we say what we do . . . and do what we say. We publish a Privacy Policy online to inform our customers about our information practices. Our Privacy Policy and our methods and procedures are designed to ensure, at a minimum, full compliance with the CPNI rules. Accordingly, every employee must read and be familiar with our privacy commitments to our customers.

**Use of CPNI for Marketing:** The FCC’s CPNI rules allow us to use CPNI to market our own communications-related products and services to our customers without their consent. But even then, we give our customers the choice of whether or not to receive marketing communications from us. We will not access, use, or disclose CPNI to market the products or services of others (including our affiliates) without our customer’s prior approval. Any use of CPNI for marketing purposes is subject to supervisory & legal review and approval and T-Mobile record-keeping requirements.

**Safeguarding CPNI:** We implement reasonable measures designed to safeguard CPNI.

Version 1.1 (March 2012)
T-Mobile Employee or Representative Access to CPNI: Access to CPNI by T-Mobile employees or T-Mobile contractors or vendors must be authorized and limited to those with a legitimate need or business purpose.

Customer Access to CPNI: To protect our customers’ CPNI, we employ customer authentication procedures whenever a customer calls, uses the Internet, or visits our stores to request access to their CPNI. Our policy is to not provide call detail records in response to customer-initiated calls.

Use: CPNI may be accessed, used, or disclosed in the ordinary course of business to provide service, collect and bill for service, and as otherwise permitted by law. All of these uses are subject to supervisory & legal review and approval procedures.

Disclosure: Disclosure of or access to CPNI by T-Mobile contractors or vendors is permitted only when there is a valid business reason and when adequate security procedures and contractual confidentiality provisions are in place.

DOJ Requirements: T-Mobile has certain obligations under its agreement with the Department of Justice to store CPNI only in the United States, to limit access to authorized personnel only, and to report breaches of security.

Unauthorized Access: Any unauthorized use, disclosure, or access to CPNI must be immediately reported to the Investigations team and we have developed various tools for this purpose (e.g., Electronic Incident Reports; privacy@T-Mobile.com; Integrity Hotline). We will report any unauthorized access to law enforcement as required by law and notify our customers accordingly.

Training: T-Mobile will conduct periodic training of those employees and representatives who have access to or who use CPNI in the ordinary course of business to ensure compliance with this Policy and T-Mobile CPNI operating procedures as to when they are, and are not, authorized to access, use, or disclose CPNI. Supervisors must ensure their employees attend the training and otherwise receive the necessary instructions for dealing with CPNI.

Employee Discipline: Failure to follow this Policy or other T-Mobile operating procedures for CPNI will result in discipline up to and including termination.

Compliance with the Law: Designated officers and managers directly responsible for implementing the Company’s CPNI operating procedures will semi-annually certify that there are operating procedures in place designed to ensure compliance with the FCC’s rules governing CPNI. As part of our CPNI program and
compliance efforts, all officers and managers will strive for continuous improvement, monitor progress, and take corrective action when necessary.

**Responsibility for this Policy:** The T-Mobile Privacy Office is responsible for this Policy and will keep it up-to-date to reflect our business practices and changes in the law. Questions about the requirements of this Policy should be directed to the Privacy Office.