

SPRINT MOBILITY MANAGEMENT PRODUCT ANNEX

The following terms and conditions in this Sprint Mobility Management Product Annex ("Annex"), together with the Sprint Standard Terms and Conditions for Communication Services ("Standard Terms and Conditions") and the agreement ("Agreement") under which Customer is purchasing Sprint Mobility Management, govern Sprint's provision of Sprint Mobility Management to Customer. Terms not otherwise defined herein will have the meanings set forth in the Standard Terms and Conditions and the Agreement.

1. SERVICE COMPONENTS

1.1. **Eligibility.** Only Corporate Liable Lines are eligible for Sprint Mobility Management.

1.2. Device Management

A. Device Security

- (1) **Description.** Security management has two components. The device password component provides Customer with a power-on password that requires a specific password prior to use. The device disablement component protects any device and any information on that device by permitting Customer to erase all information not resident in the read-only memory (returning the device to its original factory settings) on the device with the sending of a specific command to that device.
- (2) **Technical Support.** Customer may contact Sprint for technical support by contacting the Sprint-provided toll-free customer service number provided to Customer. Customer must designate one authorized contact and one alternate authorized contact that will contact Sprint for technical support. Only these designated contacts will be eligible to contact Sprint on Customer's behalf.

B. Configuration Management. Configuration management installs applications, upgrades, or other system enhancements over-the-air (OTA) directly to each Customer device without requiring each Customer device to be tethered to any computer. Configuration management also configures Customer's devices per Customer-specific requirements and specifications OTA using the device client. Customer will be responsible for selecting and testing the interoperability of applications or files for each specific device prior to sending applications/files to Sprint

C. General

- (1) **Self-Care Portal.** The customer will have the ability to manage aspects of device security and device configuration through the use of a web-based customer portal. The portal is intended to be used by the Customer administrator for the aforementioned purposes as well as general user administrative activity.
- (2) **Devices.** Selected Sprint devices will be supported by the Device Management portion of the Service. Selected multi-Carrier devices also will be supported by the Device Management portion of the Service. Sprint reserves the right to modify the selected devices at any time without advance notice to the customer.
- (3) **Back Up and Restore.** The customer will have the ability to back up data stored on the aforementioned handheld devices. The handheld device data will be backed up on a predetermined schedule and available to be restored to an individual using the Sprint Mobility Management Device Management service. This service will be assessed an additional fee. Customers must purchase Device Management in order to receive the back up and restore functionality. This feature is only available for handset memory back up not to exceed 100MB per device, and will not back up data stored on any Scan Disk cards.
- (4) **Customer Data.** The provision of the Device Management portion of the Service requires Customer to provide Sprint or any Sprint service provider, on an ongoing and timely basis, data required to perform the Device Management, including, without limitation, data on business units, assignment of wireless devices to business units, assignment of personnel to business units, assignments of personnel to wireless devices, and the identification of business unit managers along with Customer's determination of the appropriate level of data access for each manager.

1.3 Mobile Security

Devices. Sprint supports selected devices. Sprint reserves the right to modify the selected devices at any time without advance notice to the customer.

- A. Compliance.** Compliance has 3 components: Policy Management allows the Customer to enforce many user and group policies from a portal. Remediation allows the Customer to update non-compliant programs automatically. Asset Management allows the Customer to manage devices and user profiles online.
- B. Data Protection.** Data Protection allows the Customer to secure corporate data with Authentication, Data Encryption and a Mobile VPN client. With authentication, the Customer can enforce password policies across all devices. Data Encryption allows the customer to encrypt the full device, files and memory cards with AES or

3DES encryption. A Mobile IPSec VPN client is also included and allows end users to securely connect to the corporate network. This product does not include the VPN appliance. Additional charges will apply for the VPN appliance and management.

- C. **Threat Prevention.** Sprint Mobile Security protects certain mobile devices from viruses, worms and other malicious code with a Windows Mobile Firewall and Mobile Anti-Virus client. This firewall is currently available for Windows Mobile handheld devices. The Mobile Firewall will monitor and restrict network traffic based on source, destination, IP ports and applications. The Mobile Anti-Virus client scans, identifies and removes malicious codes.
- D. **Self-Care Portal.** The customer will have the ability to manage aspects of device security and device configuration through the use of a web-based customer portal. The portal is intended to be used by the Customer administrator for administrative purposes such as sending a "kill pill," adding a user, executing reports, etc.

1.4 **Premium Support.** Sprint offers dedicated representatives for each account that is accessible via a dedicated toll-free number. This level of support is only available for Customer's telecom manager and should be used for Device Management (including device disablement), device and accessory ordering, priority device support, and other services as designated by Sprint. This level of support is available from 8am-5pm (central time), Monday through Friday. Customer's telecom manager may request device disablement on a 24 hours a day, 7 day a week basis.

2. PARTIES' RESPONSIBILITIES

2.1. Customer's Responsibilities

- A. **Management.** Customer will provide a dedicated telecom manager and back up to serve as the primary interface with Sprint for the duration of the Sprint Mobility Management implementation process. The telecom manager's commitment will include, among other items, attend and participate in implementation meetings, collect Customer data, complete all necessary forms, coordinate Customer's implementation procedures, ensure Customer's employee perform all required functions.
- B. **Information.** Prior to deployment of Sprint Mobility Management, Customer will identify staffing contacts, provide a list of subscriber or employee data (including full names, email addresses, department names, employee ID, various Customer hierarchies, wireless phone numbers, and landline phone numbers), complete the Device Management option, and complete all device management training. After deployment of Sprint Mobility Management, Customer will report any changes to Sprint.

2.2. Sprint Responsibilities

- A. **Staffing.** Sprint will provide personnel that will assist with the management, implementation, and supervision of Sprint Mobility Management. The personnel will also lead work sessions to address escalation issues, and manage overall Service support efforts.
- B. **Customer Care.** Sprint will provide Customer with customer care to provide day-to-day Service support, assist in the device configuration, enforce password management and device disablement, manage OTA application distribution and management, provide required forms, and communicate with all other Sprint personnel regarding Sprint Mobility Management for Customer.

3. SECURITY AND REPORTING

- 3.1. **Security.** Customer will take reasonable care to maintain the operability of the Service, which care shall include reasonable accommodation for service and other intermittent periods for routine hardware and software maintenance. Notwithstanding such care, Sprint makes no representation that the Service will be available at any particular time, or for a particular length of time. Due to the nature of multiple interacting computers and programs involved in the operation of the Service, Sprint disclaims any warranty of security, availability or reliability of Sprint Mobility Management. Customer should take whatever precautions deemed necessary or advisable to prevent security issues from occurring.
- 3.2. **Reporting.** Customer will keep records relating to Sprint Mobility Management. At Sprint's request and upon 30 days' prior written notice, Customer agrees to accurately complete and fully execute any reports provided by Sprint indicating the quantity of Sprint Mobility Management applications used, on what type of computers or devices Sprint Mobility Management is installed, and the version number of installed Sprint Mobility Management applications.