Personal Communication Devices and Voicemail Policy

Last Update Status: *Retired*

1. Overview

See Purpose.

2. Purpose

This document describes Information Security's requirements for Personal Communication Devices and Voicemail for <Company Name>.

3. Scope

This policy applies to any use of Personal Communication Devices and <Company Name> Voicemail issued by <Company Name> or used for <Company Name> business.

4. Policy

4.1 Issuing Policy

Personal Communication Devices (PCDs) will be issued only to <Company Name> personnel with duties that require them to be in immediate and frequent contact when they are away from their normal work locations. For the purpose of this policy, PCDs are defined to include handheld wireless devices, cellular telephones, laptop wireless cards and pagers. Effective distribution of the various technological devices must be limited to persons for whom the productivity gained is appropriate in relation to the costs incurred.

Handheld wireless devices may be issued, for operational efficiency, to <Company Name> personnel who need to conduct immediate, critical <Company> business. These individuals generally are at the executive and management level. In addition to verbal contact, it is necessary that they have the capability to review and have documented responses to critical issues.

4.2 Bluetooth

Hands-free enabling devices, such as the Bluetooth, may be issued to authorized <Company Name> personnel who have received approval. Care must be taken to avoid being recorded when peering Bluetooth adapters, Bluetooth 2.0 Class 1 devices have a range of 330 feet.

4.3 Voicemail

Voicemail boxes may be issued to <Company Name> personnel who require a method for others to leave messages when they are not available. Voicemail boxes must be protected by a PIN which must never be the same as the last four digits of the telephone number of the voicemail box.

4.4 Loss and Theft
Files containing confidential or sensitive data may not be stored in PCDs unless protected by approved encryption. Confidential or sensitive data shall never be stored on a personal PCD. Charges for repair due to misuse of equipment or misuse of services may be the responsibility of the employee, as determined on a case-by-case basis. The cost of any item beyond the standard authorized equipment is also the responsibility of the employee. Lost or stolen equipment must immediately be reported.

4.5 Personal Use
PCDs and voicemail are issued for <Company Name> business. Personal use should be limited to minimal and incidental use.

4.6 PCD Safety
Conducting telephone calls or utilizing PCDs while driving can be a safety hazard. Drivers should use PCDs while parked or out of the vehicle. If employees must use a PCD while driving, <Company Name> requires the use of hands-free enabling devices.

5. Policy Compliance

5.1 Compliance Measurement
The Infosec team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions
Any exception to the policy must be approved by the Infosec Team in advance.

5.3 Non-Compliance
An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6 Related Standards, Policies and Processes

None.

7 Definitions and Terms

The following definition and terms can be found in the SANS Glossary located at:
https://www.sans.org/security-resources/glossary-of-terms/

- Bluetooth
- Confidential or sensitive data

8 Revision History

Date of Change	Responsible	Summary of Change
Dec 2013	SANS Policy Team	Converted to new format and retired