|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Information Security Policies | | | | | |
| Personally Owned Device Security Policy | | | | | |
| Policy # | CPL-04-08 | Effective Date | MM/DD/YYYY | Email | policy@companyx.com |
| Version | 1.0 | Contact | Policy Contact | Phone | 888.641.0500 |

**Table of Content**

[Purpose 1](#_Toc457904527)

[Scope 1](#_Toc457904528)

[Policy 1](#_Toc457904529)

[Mobile Computing Configuration and Data Management 2](#_Toc457904530)

[Video and Still Camera Features 3](#_Toc457904531)

[Maintenance and Support 3](#_Toc457904532)

[Authentication and Access 4](#_Toc457904533)

[Lost or Stolen Mobile Devices 4](#_Toc457904534)

[Mobile Device Management System 4](#_Toc457904535)

[Device Monitoring 5](#_Toc457904536)

[Violations 5](#_Toc457904537)

[Definitions 5](#_Toc457904538)

[References 6](#_Toc457904539)

[Related Documents 6](#_Toc457904540)

[Approval and Ownership 7](#_Toc457904541)

[Revision History 7](#_Toc457904542)

Purpose

This policy defines the information security requirements for the protection of sensitive information on all personally-owned devices (PODs)

This policy addresses the current controls that are required to maintain information security when employing portable devices that are not owned by the organization. While this is widely known in the industry as BYOD, or Bring Your Own Device, we have chosen to identify the devices as “personally owned,” which makes ownership of the device a bit clearer. Also the BYOD moniker may convey to some that the organization is encouraging the use of personal devices, which some organizations may want to keep to a minimum. Regardless of what it is called this trend, the proliferation of personal devices in the workplace is growing exponentially and must be addressed. Every organization should have a policy like this one to ensure that all employees and partners are aware of the restrictions on the use of their own devices in the workplace.

.

Scope

This policy applies to all Company X employees and third parties who use PODs to perform Company X business functions.

Policy

Configuration of Mobile Devices

**Approved Configuration of Mobile Computing Devices** – Personally-owned devices (PODs) must not be used to store Company X business information unless they have been configured with the necessary controls and approved for such use by the Information Security Manager.

**Device Wipe at Termination** – All Company X information must be deleted or wiped from an employee’s or partner’s POD upon termination of employment or contract.

**Jailbroken and Rooted Devices** – Jailbroken or rooted devices must not be used to connect to any Company X computer or communications system.

Smartphones and Tablet Computers

This section is applicable for any organization that is not using a full-featured mobile device management system to control the usage of PODs. Not all devices can be configured to adequately protect the stored information. The organization can use a device limitation policy to ensure that only those devices that are deemed acceptable to their enterprise are used and supported. The tables below are examples of devices that can be configured with acceptable password encryption controls. The tables are presented as examples only, not as an exhaustive or definitive list of acceptable devices. Additional tables may be added for other hardware should the organization choose to place limitation of personally-owned laptops, printers, storage devices, etc.

**Device Limitation – Employees and partners must not use any** smartphone or tablet computer to access Company X information other than those listed in the following tables:

|  |  |  |
| --- | --- | --- |
| **Smartphones** | | |
| Manufacturer | **Operating System** | **Version** |
| Apple iPhone | iOS | 3GS and above |
| All | Android | Any version with encryption continuously active as part of the operating system |
| All | Blackberry | All, provided that they connect through the Company X Blackberry Enterprise Server (BES). |

|  |  |  |
| --- | --- | --- |
| **Tablet Computers** | | |
| Manufacturer | **Operating System** | **Version** |
| Apple iPad | iOS | All |
| All | Android | Any version with encryption continuously active as part of the operating system |
| All | Blackberry | All, provided that they connect through the Company X Blackberry Enterprise Server (BES). |

### Mobile Computing Configuration and Data Management

**Mobile Devices Containing Sensitive Information – All PODs containing sensitive Company X information must consistently employ both encryption for all such files, and wherever possible, startup and screen-saver-based password/boot protection.**

**Information Transfer – Company X information residing on a POD, including but not limited to electronic mail messages and attachments must not be transferred to any non Company X device without approval from the Information Security Department.**

**Information Separation – All personal information stored on a POD must be kept in a location on the device that does not also contain Company X information.**

**Personal Information Restriction – Personal information stored on a POD must not be transferred or backed up to any Company X computer or communications system.**

Ownership of Information Stored In Mobile Devices **– All company information stored in a POD is Company X property, can be inspected or used in any manner at any time by Company X and must wiped clean at the time workers are no longer employed by Company X.**

**Storage Of Remote Access Information In Portable Computers - Users must not store remote access information, e.g., fixed passwords, user IDs, in their POD, or in the device case in which their POD is stored or used for transport.**

**Lending Computing Equipment Containing Sensitive Information - A POD used for business activities that contains Company X sensitive information must not be lent to anyone.**

**Accepting SMS Messages – Company X workers must not accept text messages on PODs from unknown senders. Any messages or contacts received on a POD from an unknown number or device should be treated with suspicion. Messages should be destroyed without opening and connections denied.**

### Video and Still Camera Features

**Image Capture - Information –** Employees and partners must not use the video or still camera features on any PODs, including smartphones and tablet computers to capture images that may depict confidential Company X information, including but not limited to customers, documents, computer displays and output.

**Image Capture - Facilities –** Employees and partners must not use the video or still camera features on any PODs, including smartphones and tablet computers to capture images within any Company X secure area, including but not limited to areas where proprietary procedures are performed, proprietary devices or equipment are used, or non-public information is processed, stored, or transmitted.

### ****Maintenance and Support****

This section is applicable for any organization that has not implemented a comprehensive program, i.e., one that provides an annual stipend for the purchase and maintenance of PODs. If a program of this type has been implemented the following policy statements should be modified and augmented to reflect the requirements of the program.

**Hardware** – Each POD must be fully maintained by the owner of the POD, i.e., Company X provides no assistance or services for PODs, which includes but is not limited to repairs, upgrades and replacements.

**Software** – All POD software, including but not limited to the operating system and communication applications, must be maintained with the most recent release, patches, and updates by the POD owner, not Company X.

**Malware Protection** – Each POD owner must ensure that their device is equipped with Company X-approved malware protection software and that this software is maintained with the most recent release, patches, and updates.

**Support** – POD owners must direct all hardware and software support issues to commercial sources, e.g., hardware vendor, telecommunications carrier, software vendors, not to the Company X Help Desk.

### ****Authentication and Access****

**Strong Passwords Required** – All PODs used for Company X business purposes must have passwords enabled and enforce all Company X password parameters.

**Separate Password for Portable Devices** – Company X workers must not use the same password for a POD that is used for network access or access to other devices and applications.

**Network Access** – All POD access to the Company X production network must be restricted to known and authorized devices.

**Electronic Mail Access** – Electronic mail access by PODS must be accomplished only through Microsoft ActiveSync.

Microsoft ActiveSync is one of a number of protocols that can be used to control access to electronic mail. The Microsoft ActiveSync Configuration policy does not present an exhaustive list of control settings. The organization should review and implement all relevant parameters that are configurable within the protocol in use.

**Microsoft ActiveSync Configuration** – Microsoft ActiveSync must be must be configured to require all devices to:

* Continually enable the password feature
* Enforce all of Company X password requirements
* Timeout the device after 15 minutes of in activity
* Encrypt all Company X information including any that is stored on a storage card
* Wipe all Company X information after 10 invalid password attempts
* Retain messages for no more than seven days

**Application Access** – Access to all applications from a mobile device must be properly authorized and managed through a central application server.

### ****Lost or Stolen Mobile Devices****

**Immediate Reporting Lost Devices** – All Company X personnel must immediately report lost or stolen PODs to their immediate supervisor and the Information Security Department.

**Mobile Device Wipe** – All devices that are reported lost or stolen immediately must have all Company X information remotely deleted or wiped.

### ****Mobile Device Management System****

This section is applicable for any organization using a mobile device management system to control the usage of PODs. The MDM Configuration policy does not present an exhaustive list of control settings. The organization should review and implement all relevant parameters that are configurable within the mobile device management system in use.

**Mobile Device Management (MDM) System** - All PODs in use at Company X must be controlled through the [enter MDM system name here].

**MDM Configuration** – The MDM system must be configured to require all devices to:

* Continually enable the password feature
* Enforce all of Company X password requirements
* Timeout the device after 15 minutes of in activity
* Encrypt all Company X information including any that is stored on a storage card
* Wipe all Company X information after 10 invalid password attempts
* Install or execute only those applications that do not negatively affect employee productivity or are in conflict with Company X or regulatory compliance.
* Limit data transfer to non-confidential Company X information to prevent data leakage.

### ****Device Monitoring****

**Activity Logging** – All security relevant user activity that is initiated from a POD must be logged and reviewed on a routine basis.

**Compliance Audit** – All PODs must be audited on a quarterly basis to ensure that each device is in compliance with Company X policies.

**Device Quarantine** – Any POD found to be out of compliance with Company X policies must be quarantined from the network until al deviations are corrected and validated by the Information Security Department.

Violations

Any violation of this policy may result in disciplinary action, up to and including termination of employment. Company X reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. Company X does not consider willful and deliberate conduct that is in violation of this policy to be within an employee’s or partner’s course and scope of employment, or the direct consequence of the discharge of the employee’s or partner’s duties. Accordingly, to the extent permitted by law, Company X reserves the right not to defend or pay any damages awarded against employees or partners that result from violation of this policy.

Definitions

Confidential Information (Sensitive Information) – Any Company X information that is not publicly known and includes tangible and intangible information in all forms, such as information that is observed or orally delivered, or is in electronic form, or is written or in other tangible form. Confidential Information may include, but is not limited to, source code, product designs and plans, beta and benchmarking results, patent applications, production methods, product roadmaps, customer lists and information, prospect lists and information, promotional plans, competitive information, names, salaries, skills, positions, pre-public financial results, product costs, and pricing, and employee information and lists including organizational charts. Confidential Information also includes any confidential information received by Company X from a third party under a non-disclosure agreement.

E-reader – A device for reading content, such as e-books, newspapers and documents, which typically has wireless connectivity for downloading content and conducting other Web-based tasks.

Jailbroken Device – An iOS smartphone or tablet computer which has been reconfigured to permit user access to the root level of the operating system.

Mobile Device – Any portable computing device used to access, process, transmit, or store information, e.g., laptops, smartphones, e-readers, tablet computers, which is used for Company X business purposes.

Mobile Device Management (MDM) System – Software that secures, monitors, manages and supports mobile devices deployed across mobile operators, service providers and enterprises. This functionality typically includes over-the-air distribution of applications, data and configuration settings for all types of mobile devices, including [mobile phones](http://en.wikipedia.org/wiki/Mobile_phone), smartphones, [tablet computers](http://en.wikipedia.org/wiki/Tablet_computer), mobile computers, mobile printers, mobile POS devices, etc.

**Personally-Owned Device (POD)** – Any device not owned by Company X used to access, process, transmit, or store information, e.g., smartphone, e-reader, tablet computer, notebook computer, which is used for Company X business purposes.

**Rooted Device** – An Android smartphone or tablet computer which has been reconfigured to permit user access to the root level of the operating system.

**Short Message Service (SMS)** – A [text messaging](http://en.wikipedia.org/wiki/Text_messaging) service component of phone, web, or mobile communication systems, using standardized [communications protocols](http://en.wikipedia.org/wiki/Communications_protocols) that allow the exchange of short text messages between [fixed line](http://en.wikipedia.org/wiki/Fixed_line) or [mobile phone](http://en.wikipedia.org/wiki/Mobile_phone) devices.

**Smartphone** –A cellular telephone with built-in applications and Internet access. Smartphones provide digital voice service as well as text messaging, e-mail, Web browsing, still and video cameras, MP3 player, video viewing and video calling. In addition to their built-in functions, smartphones can run a myriad of applications, which in effect classifies the device as a computer.

**Tablet Computer** – A complete computer contained in a touch screen, e.g., Apple iPad, Samsung Galaxy, Motorola Xoom, Blackberry Playbook. Tablet computers can be specialized for Internet use only or be full-blown, general-purpose PCs. The distinguishing characteristic is the use of the screen as an input device using a stylus or finger.

**Text Messaging** – Also known as "texting", refers to the exchange of brief written messages between mobile phones over cellular networks.

User – Any Company X employee or partner who has been authorized to access any Company X electronic information resource.

References

CPL: 4.5 Mobile Computing

ISO/IEC 27002: 6.2 Mobile devices and teleworking

HIPAA: Device and Media Controls 164.310(d)(1)

NIST: AC-19 Access Control for Mobile Devices

PCI: 12.3.9 Remote Access Technology

Related Documents

Approval and Ownership

|  |  |  |  |
| --- | --- | --- | --- |
| Owner | Title | Date | Signature |
| Policy Author | Title | MM/DD/YYYY |  |
| Approved By | Title | Date | Signature |
| Executive Sponsor | Title | MM/DD/YYYY |  |

Revision History

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Description | Revision Date | Review  Date | Reviewer/Approver Name |
| 1.0 | Initial Version | MM/DD/YYYY | MM/DD/YYY |  |
|  |  |  |  |  |