|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Information Security Policies | | | | | |
| Mobile Computing 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](#_Toc457461083)

[Scope 1](#_Toc457461084)

[Policy 1](#_Toc457461085)

[Configuration and Issuing of Mobile Devices 1](#_Toc457461086)

[Mobile Data Management 2](#_Toc457461087)

[Configuration Management 2](#_Toc457461088)

[Physical Security Protection 2](#_Toc457461089)

[Authentication and Network Access 3](#_Toc457461090)

[Foreign Travel Considerations 3](#_Toc457461091)

[Lost or Stolen Mobile Devices 3](#_Toc457461092)

[Teleworking 3](#_Toc457461093)

[Violations 4](#_Toc457461094)

[Definitions 4](#_Toc457461095)

[References 4](#_Toc457461096)

[Related Documents 5](#_Toc457461097)

[Approval and Ownership 5](#_Toc457461098)

[Revision History 5](#_Toc457461099)

Purpose

This policy defines the minimum requirements for the protection of Company X information stored, processed or transported on mobile computing devices or in remote locations.

Scope

This policy applies to all Company X computer systems and facilities, including those managed for Company X by third-parties. This policy applies to all employees, partners and third-parties with access to Company X information assets. .

Policy

### Configuration and Issuing of Mobile Devices

**Only Company Owner Mobile Devices** – Employees must not use personal mobile devices to store or process Company X information. All mobile devices used for Company X business purposes must be issued by the Information Security Department.

**Mobile Device Management** – If mobile phones are used to store or process Company X information, these devices must be controlled by a mobile device management system approved by the Information Security Department.

### Mobile Data Management

**Sensitive Data Approval - All mobile computing devices used to conduct any Company X business must be approved by the Information Security Department for use with the information appropriate for the normal business activities of the individual user.**

**Sensitive Information Encryption - All mobile computing devices, including laptops, notebooks, and their peripherals containing sensitive Company X information must consistently employ both hard-disk encryption for all such files, and wherever possible, startup and screen-saver-based password\boot protection.**

Information Ownership In Mobile Devices **- The information stored in Company X portable computer equipment is Company X property, can be inspected or used in any manner at any time by Company X and, like the equipment, it must be returned to Company X or wiped clean at the time workers are no longer employed by Company X.**

**Storage and Labeling of Portable Media - When sensitive information is written to portable storage device such as a portable disk, magnetic tape, smart card, or other storage media, the media must be suitably marked with the highest relevant sensitivity classification. When not in use, this media should be stored in locked bag or furniture.**

### Configuration Management

**Changes to Configurations And Software - On Company X-supplied computer hardware, workers must not change the operating system configuration or install new software unless the software is approved in advance by the Information Security Department.**

**Accepting SMS Messages – Company X workers must not accept text messages on mobile devices from unknown senders due to the risk of malicious software. Any messages or contacts received on a mobile phone from an unknown number or device should be treated with suspicion. Messages should be destroyed without opening and connections denied.**

### ****Physical Security Protection****

**Personnel Responsibility** - All mobile devices in the possession of company personnel must be protected from physical threats such as loss due to theft or vandalism.

**Locking Personal Offices or Conference Rooms** - All workers with separate personal offices should lock the doors when these offices are not in use or otherwise unattended.

**Leaving Mobile Devices Unattended** - Workers must keep Company X portable computers containing Company X information in their possession at all times unless they have been deposited in a secure location such as a locked closet or a hotel safe.

**Mobile Devices Stored Out of Site** – All portable devices in the possession of Company X personnel must be stored in a secure location, such as a locked file cabinet or drawer, when not in use. Under no circumstances should portable devices be left in open view on desks or in public areas.

**Checked Luggage** - Workers in the possession of portable, laptop, notebook, palmtop, handheld, smart phones, personal digital assistants, and other transportable computers containing sensitive Company X information must not check these computers in airline luggage systems. These computers must remain in the possession of the traveler as hand luggage.

**Locks for Laptops and Mobile Devices** – All Company X issues mobile devices much have physical cable locks issues by the Information Security Department.

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

**Automatic Wireless Network Connections** – Company X mobile devices capable of making wireless network connections must be configured to that automatic network connection is disabled. Mobile devices must only connect to wireless networks approved by the Information Security Department.

**Strong Passwords Required** – All portable devices used for Company X business purposes must have passwords enabled. These passwords must be at least eight (8) characters in length.

### **Foreign Travel Considerations**

**Foreign Transport of Sensitive Information** - Whenever Confidential information is carried by a Company X worker into a foreign country, the information must either be stored in some inaccessible form, such as an encrypted external storage media, or must remain in the worker’s possession at all times.

**Special Laptops for International Travel** - All Company X employees traveling with Secret information must only use special “travel” laptops issued by the Information Technology department. These special devices are stripped of all non-essential information and must employ both full-disk encryption and two-factor authentication.

**Inspection of Machines for International Travel** - All Company X personnel returning from overseas travel must have their laptops and other portable devices inspected by the Information Security department before connecting to the Company X network. This inspection is required to check for malicious software or other security vulnerabilities that may have been introduced during inspection by authorities.

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

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

### Teleworking

**Alternative Work-Site Requirements** - Before a telecommuting arrangement can begin, the worker’s supervisor or manager must be satisfied that an alternative work-site is appropriate for the Company X work performed by the involved worker.

**Telecommuter Information Security Procedures** - Telecommuters must follow all remote system security policies and procedures including, but not limited to, compliance with software license agreements, performance of regular backups, hard disk encryption packages, locking file cabinets, and use of shredders to dispose of sensitive paper-resident information.

**Lockable, Burglar-Resistant Furniture** - All workers who must keep sensitive Company X information and mobile devices at their homes to perform their work, must receive from Company X – or otherwise provide – approved lockable cabinets or desks for the proper storage of this information.

**Remote Workspace Environmental Controls** – Equipment should be located and/or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.

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.

**Information Asset –** Any Company X data in any form, and the equipment used to manage, process, or store Company X data, that is used in the course of executing business. This includes, but is not limited to, corporate, customer, and partner data.

Mobile Computing Devices - Mobile computing assets include, but are not limited to: laptop, notebook, tablet, desktop computers, all personal wireless-enabled devices, including pagers, cellular phones, mobile email devices, PDAs and other hybrid devices, and all portable storage media, including flash drives, smart cards, tokens, etc.

**Password** **–** An arbitrary string of characters chosen by a user that is used to authenticate the user when he attempts to log on, in order to prevent unauthorized access to his account.

**Third-Party –** Any non-employee of Company X who is contractually bound to provide some form of service to Company X.

**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 |  |
|  |  |  |  |  |