**COMPANY Logo**

**Information Security Policies:** Mobile Device Management

Effective Date:

**COMPANY Logo**

Revised:

Approved by: CISO (or equivalent) Approved on: 00/00/20

Approved by: COO Approved on: 00/00/20

Approved by: Board of Directors Approved on: 00/00/20

# Purpose

The purpose of the Mobile Device Management Policy is to describe the process requirements to ensure adequate protection of COMPANY (“COMPANY”) information assets when using mobile computing devices and teleworking facilities and that the devices are securely managed. This policy:

* Defines the requirements for these devices necessary to ensure effective, efficient and reliable management of mobile devices
* Assures that the devices are maintained with adequate protection when used in an unprotected environment such as telecommuting and teleworking

# Scope

This policy applies to Users (employees, contractors, vendors, consultants, or other persons) who use or access mobile computing devices (e.g., laptops, smartphones, and mobile phones, etc.) used to conduct COMPANY business. It covers all telecommuting and teleworking facilities which are in public places, meeting rooms and any other unprotected areas outside of COMPANY’s physical premises.

# Roles and Responsibilities

## The RACI Chart below shows the assignment of functional and cross-functional activities. The roles are as follows:

| R - Responsible is the organizational title responsible for doing the work.A - Accountable is the organizational title for who is accountable for the work being done.C - Consulted is the organizational title that provides necessary information.I - Informed is the organizational title that receives information. **Milestone or Task** | Governance / Risk Management | Chief Information Security Officer (or equivalent) | Information Security Organization / IT | Corporate (Physical) Security | Users |
| --- | --- | --- | --- | --- | --- |
| Physical Security | C | A | R | C | R |
| Logical Security | C | A | R | I | R |
| Malware Protection | C | A | R | I | R |
| Performing Back-ups | C | A | R | I | R |
| Mobile Computing & Communications | C | A | R | C | R |
| Telecommuting / Teleworking | C | A | R | C | R |

# Policy Statements

The Mobile Device Management Policy is implemented to ensure that mobile devices containing COMPANY information are adequately protected and the security of mobile computing devices and teleworking facilities are maintained. The portability of the mobile computing device lends them to be more easily stolen and lost, adding additional risks to the information contained within.

This is accomplished via the following:

## Physical Security

* + 1. IT must maintain an inventory of COMPANY mobile computing devices.
    2. IT must issue all laptops with cable locking devices.
    3. Users must keep any mobile computing device (whether a COMPANY-owned device or not) containing COMPANY information (e.g., corporate information, Non-Public Information, intellectual property, etc.) physically secure.
    4. Users must not leave mobile computing devices unattended in cars, airports or other public places.
    5. Users must lock up mobile computing devices when not in use in hotel rooms, offices or other potentially insecure environments.

## Logical Security

* + 1. IT must implement logical access controls (e.g., passwords) to limit access to mobile computing devices, software programs and data.
    2. Users must encrypt valuable COMPANY information stored on mobile computing devices.
    3. Users must not download untrusted software onto mobile computing devices.

## Malware Protection

* + 1. IT must manage anti-malware software on laptops to ensure programs and information are protected from computer malware (e.g., viruses).
    2. IT must manage anti-malware software (where available) on each mobile computing device that has the ability to accept emails and has Internet access.
    3. IT must implement at a minimum the same anti-malware requirements for laptops (and other mobile computing devices where appropriate and available) as desktop computers.
    4. Users must follow the same anti-malware procedures and processes for laptops (and other mobile computing devices where anti-malware software is implemented) as desktop computers.

## Performing Backups

* + 1. IT must provide capabilities to ensure that valuable COMPANY information stored on mobile computing devices is properly backed-up or replicated.
    2. Users must back-up valuable COMPANY information stored on mobile computing devices.

## Mobile Computing and Communications

* + 1. The Information Security Organization must ensure that appropriate security measures (access controls, encryption, anti-malware, back-ups, etc.) are adopted to protect against the risks of using mobile computing devices and communication facilities.
    2. The Information Security Organization must arrange security awareness training for Users of mobile computing devices to raise their awareness of the additional risks and the controls that are in place.
    3. Users must protect mobile computing devices from unauthorized access or disclosure of COMPANY information stored and processed by these devices.
    4. Users must not use Instant Messaging (IM) to transmit files. COMPANY blocks transmission of attached files via IM to protect against viruses and to protect IP addresses.
    5. Users must take precautions to prevent overlooking by unauthorized persons when using mobile computing devices in public places.

## Telecommuting / Teleworking

* + 1. The Information Security Organization must develop and establish procedures for telecommuting and teleworking activities.
    2. IT must only authorize telecommuting and teleworking activities when satisfied that appropriate security arrangements and controls are in place, and that these comply with COMPANY’s Information Security Policies.
    3. IT must ensure that access to and activities for telecommuting and teleworking are authorized.
    4. IT must ensure appropriate protection measures are active before allowing telecommuting or teleworking connections access to the COMPANY network. Remote access to the COMPANY network from public networks using mobile computing devices must only take place after appropriate identification, authentication, and access controls are used.
    5. IT must implement appropriate controls for mobile network wireless connections.
    6. Users must protect telecommuting and teleworking sites against the theft of equipment and COMPANY information, unauthorized disclosure of information, and unauthorized remote access to COMPANY’s internal systems or misuse of resources.

# Compliance with Policies

# Use of COMPANY’s network, systems, hardware and applications represents the User’s consent to the terms of the policies described here, including consent for COMPANY to monitor and audit content and/or use. A User’s failure to comply with Information Security Policies may lead to disciplinary action to include one or more of the following:

* Oral and/or written warning or notification of violation to User(s) involved and supervisor(s)
* Suspension of network, system or application access or electronic communications privileges permanently or for a set period
* Repossession of electronic devices or hardware permanently or for a set period
* Electronic messages may be blocked or rejected if the message contains inappropriate content
* Written warning to the User’s HR file
* Suspension from work
* Education course related to the infraction paid for by the User
* Regulatory discipline or censure
* Termination of employment

Users consent by reading this policy at time of hiring and at each annual evaluation by signing an *Information Security Policy Acknowledgement* form.

# Questions

Users are encouraged to contact the Chief Information Security Officer (CISO) or the Information Security Organization with any questions or concerns. It is critical for all Users to consult supervisors and/or the Information Security Organization about “red flags” (any suspicious activities giving rise to concerns about whether such activities meet or potentially violate Information Security Policies). All Users are encouraged to raise questions or concerns if they believe an information-security risk or leak is present.

# Disclaimers

COMPANY retains the right to:

* Restrict or revoke any User’s privileges to information, equipment or systems
* Inspect, copy, remove or otherwise alter any information, program, or other system resource that may undermine these objectives
* Take any other steps deemed necessary to protect COMPANY information or information systems

This right may be exercised with or without notice to the involved users. COMPANY disclaims any responsibility for loss or damage to information or software that results from COMPANY exercising its rights under Information Security Policies.

All documents, computing assets, and communications systems assets, including the email and phone systems, physically located at or pertaining to COMPANY are the property of COMPANY. COMPANY reserves the right to examine all information stored in or transmitted by these systems, subject to applicable law. Users should have no expectation of privacy associated with personal information and information stored in, created on, or sent through the COMPANY computer and communication systems.

# Definitions

The following terms are related to this Information Security Policy:

* **Authentication**: To verify the identity of a user, device, or other entity in a computer system, often as a prerequisite to allowing access to resources in a system. To verify the integrity of data that have been stored, transmitted, or otherwise exposed to possible unauthorized modification. Security measures designed to protect a communications system against acceptance of fraudulent transmission or simulation by establishing the validity of a transmission, message, or originator.
* **Authorization / Access Control**: The granting of access rights to a user, program, process, or system.
* **Authorization**: The granting of access to an individual.
* **Confidentiality**: The concept of holding sensitive data in confidence, limited to an appropriate set of individuals or organizations.
* **Encrypt**: Generic term encompassing: encipher and encode (convert plain text to its equivalent cipher text by means of a code).
* **Identification**: The process that enables recognition of an entity by a system, generally by the use of unique machine-readable user names.