Definitions

Clear text: Unencrypted data

Full disk encryption: Technique that encrypts an entire hard drive, including operating system and data.

Key: Phrase used to encrypt or decrypt data

Overview

Acceptable use of {COMPANY-NAME} owned mobile devices must be managed to ensure that employees, Board of Directors, and related constituents who use mobile devices to access {COMPANY-NAME}'s resources for business do so in a safe and secure manner.

This policy is designed to maximize the degree to which private and confidential data is protected from both deliberate and inadvertent exposure and/or breach.

OWNED MOBILE DEVICE ACCEPTABLE USE AND SECURITY /R

Purpose

This policy defines the standards, procedures, and restrictions for end users who have legitimate business requirements to access corporate data from a mobile device connected to an unmanaged network outside of {COMPANY-NAME}'s direct control.

This mobile device policy applies to, but is not limed to, any mobile device issued by {COMPANY-NAME} that contains stored data owned by {COMPANY-NAME} and all devices and accompanying media that fit the following device classifications:

- Laptops. Notebooks, and hybrid devices
- Tablets
- Mobile/cellular phones including smartphones
- Any {COMPANY-NAME} owned mobile device capable of storing corporate data and connecting to an unmanaged network

This policy addresses a range of threats to, or related to, the use of {COMPANY-NAME} data:

Threat	Description
Loss	Devices used to transfer, or transport work files could be lost or stolen
Theft	Sensitive corporate data is deliberately stolen and sold by an employee
Copyright	Software copied onto a mobile device could violate licensing
Malware	Virus, Trojans, Worms, Spyware and other threats could be introduced via a mobile device
Compliance	Loss or theft of financial and/or personal and confidential data could expose {COMPANY-NAME} to the risk of non-compliance with various identity theft and privacy laws

Addition of new hardware, software, and/or related components to provide additional mobile device connectivity will be managed at the sole discretion of IT.

Non-sanctioned use of mobile devices to backup, store, and otherwise access any enterprise-related data is strictly forbidden.

This policy is complementary to any other implemented policies dealing specifically with data access, data storage, data movement, and connectivity of mobile devices to any element of the {COMPANY-NAME} network.

Audience

This policy applies to all {COMPANY-NAME} employees, including full and part-time staff, and the Board of Directors who utilize company-owned mobile devices to access, store, back up, relocate, or access any organization or member-specific data.

Such access to this confidential data is a privilege, not a right, and forms the basis of the trust {COMPANY-NAME} has built with its members, suppliers, and other constituents.

Consequently, employment at {COMPANY-NAME} does not automatically guarantee the initial and ongoing ability to use these devices to gain access to corporate networks and information.

Policy Detail

This policy applies to any corporate owned hardware and related software that could be used to access corporate resources.

The overriding goal of this policy is to protect the integrity of the private and confidential member and business data that resides within {COMPANY-NAME}'s technology infrastructure.

This policy intends to prevent this data from being deliberately or inadvertently stored insecurely on a mobile device or carried over an insecure network where it can potentially be accessed by unsanctioned resources.

A breach of this type could result in loss of information, damage to critical applications, loss of revenue, and damage to {COMPANY-NAME}'s public image.

Therefore, all users employing a {COMPANY-NAME} owned mobile device, connected to an unmanaged network outside of {COMPANY-NAME}'s direct control, to backup, store, and otherwise access corporate data of any type must adhere to company-defined processes for doing so.

Affected Technology

Connectivity of all mobile devices will be centrally managed by {COMPANY-NAME}'s IT Department and will utilize authentication and strong encryption measures. To protect {COMPANY-NAME}'s infrastructure, failure to adhere to these security protocols will result in immediate suspension of all network access privileges.

Responsibilities /R

It is the responsibility of any employee or Board Member of {COMPANY-NAME}, who uses a {COMPANY-NAME} owned mobile device to access corporate resources, to ensure that all security protocols normally used in the management of data on conventional storage infrastructure are also applied here.

OWNED MOBILE DEVICE ACCEPTABLE USE AND SECURITY /R

It is imperative that any {COMPANY-NAME} owned mobile device that is used to conduct {COMPANY-NAME} business be utilized appropriately, responsibly, and ethically. Failure to do so will result in immediate suspension of that user's account. Based on this, the following rules must be observed:

- **Access Control**
  - IT reserves the right to refuse, by physical and non-physical means, the ability to connect mobile devices to {COMPANY-NAME} and {COMPANY-NAME}-connected infrastructure. IT will engage in such action if it feels such equipment is being used in such a way that puts {COMPANY-NAME}'s systems, data, users, and members at risk.
  - Prior to initial use on the {COMPANY-NAME} network or related infrastructure, **all mobile devices must be registered with IT**. {COMPANY-NAME} will maintain a list of approved mobile devices and related software applications and utilities, and it will be stored in the IT Document Storage location. Devices that are not on this list may not be connected to the {COMPANY-NAME} infrastructure. To find out if a preferred device is on this list, an individual should contact the {COMPANY-NAME} IT Department Service Desk.
  - Although IT currently allows only listed devices to be connected to the {COMPANY-NAME} infrastructure, it reserves the right to update this list in the future.
  - **End users** who wish to connect such devices to non-corporate network infrastructure to gain access to {COMPANY-NAME} data **must employ**, for their devices and related infrastructure, **a company-approved personal firewall** and any other security measure deemed necessary by the IT Department. {COMPANY-NAME} data is not to be accessed on any hardware that fails to meet {COMPANY-NAME}'s established enterprise IT security standards.
  - All mobile devices attempting to connect to the {COMPANY-NAME} network through an unmanaged network (i.e. the Internet) will be inspected using technology centrally managed by {COMPANY-NAME}'s IT Department. Devices that are not corporate issued are not in compliance with IT's security policies and will not be allowed to connect except by provision of the Personal Device Acceptable Use and Security Policy. {COMPANY-NAME} owned laptop computers may only access the corporate network and data using a Secure Socket Layer (SSL) Virtual Private Network (VPN) or Internet Protocol Security (IPSec) VPN connection. The SSL or IPSec VPN portal Web address will be provided to users as required. Smart mobile devices such as Smartphones, PDAs, and UMPCs will access the {COMPANY-NAME} network and data using Mobile VPN software installed on the device by IT.

- **Security /R**
  - **Employees** using mobile devices and related software for network and data access **will**, without exception, **use secure data management procedures**. All mobile devices containing stored data owned by {COMPANY-NAME} **must use an approved method of encryption** to protect data. Laptops must employ full drive encryption with an approved software encryption package. No {COMPANY-NAME} data may exist on a laptop in clear text. All mobile devices must be protected by a **strong password**. Refer to the {COMPANY-NAME} password policy for additional information. **Employees agree to never disclose their passwords to anyone**, particularly to family members, if business work is conducted from home.
  - All keys used for encryption and decryption must meet complexity requirements described in {COMPANY-NAME}'s Password Policy.
  - All users of corporate owned mobile devices must employ reasonable physical security measures. End users are expected to secure all such devices used for this activity whether they are actually in use and/or being carried. This includes, but is not limited to, passwords, encryption, and physical control of such devices whenever they contain {COMPANY-NAME} data. Users with devices that are not issued by {COMPANY-NAME} must adhere to the Personal Device Acceptable Use and Security Policy.
  - To ensure the security of {COMPANY-NAME} equipment, mobile devices will be transported and stored as specified in the "Mobile Device Transport and Storage" procedure.
  - Passwords and confidential data should not be stored on unapproved or unauthorized non-{COMPANY-NAME} devices.
  - Any corporate owned mobile device that is being used to store {COMPANY-NAME} data must adhere to the authentication requirements of {COMPANY-NAME}'s IT Department. In addition, all hardware security configurations must be pre- approved by {COMPANY-NAME}'s IT Department before any enterprise data-carrying device can be connected to it.

- IT will manage security policies, network, application, and data access centrally using whatever technology solutions it deems suitable. Any attempt to contravene or bypass said security implementation will be deemed an intrusion attempt and will be dealt with in accordance with {COMPANY-NAME}'s overarching security policy.
- Employees, Board of Directors, and temporary staff will follow all enterprise- sanctioned data removal procedures to permanently erase company- specific data from such devices once their use is no longer required. For assistance with detailed data wipe procedures for mobile devices, an individual should contact the {COMPANY-NAME} IT Department Service Desk. This information is found in the IT Document Storage location.
- In the event of a lost or stolen mobile device, it is incumbent on the user to report this to IT immediately. {COMPANY-NAME} shall employ remote wipe technology to remotely disable and delete any data stored on a {COMPANY-NAME} PDA or cell phone that is reported lost or stolen. If the device is recovered, it can be submitted to IT for re-provisioning.
- Usage of location-based services and mobile check-in services, which leverage device GPS capabilities to share real-time user location with external parties, is prohibited within the workplace. This applies to both {COMPANY-NAME}-owned and personal mobile devices being used within {COMPANY-NAME}'s premises.
- IT maintains the process for patching and updating mobile devices. A device's firmware/operating system must be up-to-date in order to prevent vulnerabilities and make the device more stable. The patching and updating processes are the responsibility of IT for computing platforms (i.e. laptops). /R
- IT maintains the process for security audits on mobile devices. Since handheld devices are not completely under the control of {COMPANY-NAME}, a periodic audit will be performed to ensure the devices are not a potential threat to {COMPANY-NAME}.

- **Help and Support**
  - {COMPANY-NAME}'s IT Department will support its sanctioned hardware and software but is not accountable for conflicts or problems caused by the use of unsanctioned media, hardware, or software. This applies even to devices already known to the IT Department.
  - Employees, Board of Directors, and temporary staff will not make modifications of any kind to {COMPANY-NAME} owned and installed hardware or software without the express approval of {COMPANY-NAME}'s IT Department. This includes, but is not limited to, any reconfiguration of the mobile device.
  - IT reserves the right, through policy enforcement and any other means it deems necessary, to limit the ability of end users to transfer data to and from specific resources on the {COMPANY-NAME} network.
- **Organizational Protocol**
  - IT can and will establish audit trails and these will be accessed, published, and used without notice. Such trails will be able to track the attachment of an external device to a PC, and the resulting reports may be used for investigation of possible breaches and/or misuse. To identify unusual usage patterns or other suspicious activity, the end user agrees to and accepts that his or her access and/or connection to {COMPANY-NAME}'s networks may be monitored to record dates, times, duration of access, etc. This is done to identify accounts/computers that may have been compromised by external parties. In all cases, data protection remains {COMPANY-NAME}'s highest priority.
  - The end user agrees to immediately report, to his/her manager and {COMPANY-NAME}'s IT Department, any incident or suspected incidents of unauthorized data access, data loss, and/or disclosure of {COMPANY-NAME} resources, databases, networks, etc.
  - {COMPANY-NAME} will not reimburse employees if they choose to purchase their own mobile devices except in accordance with the Personal Device Acceptable Use and Security Policy. Users will not

be allowed to expense mobile network usage costs.

- {COMPANY-NAME} prohibits the unsafe and unlawful use of mobile devices, including but not limited to, texting, emailing, or any distracting activity while driving, and requires this audience to comply with all state laws in which one is currently operating, regarding same, hands-free requirements, etc.
- Before being granted a device and access to {COMPANY-NAME} resources, a mobile device user must understand and accept the terms and conditions of this policy.

EXHIBIT A

{COMPANY-NAME} Owned Mobile Device Agreement

This {COMPANY-NAME} Owned Mobile Device Agreement is entered into between the User and {COMPANY-NAME} LLC ({COMPANY-NAME}), effective the date this agreement is executed by {COMPANY-NAME}'s Information Technology Department (IT). The parties agree as follows:

ELIGIBILITY

The use of a {COMPANY-NAME} supported mobile device by the User for {COMPANY-NAME} business is a privilege granted to the User, by management approval, per the {COMPANY-NAME} Owned Mobile Device Acceptable Use and Security Policy. If the User does not abide by the terms, IT Management reserves the right to revoke the privilege granted herein. The policies referenced herein are aimed to protect the integrity of data belonging to {COMPANY-NAME} and to ensure the data remains secure.

In the event of a security breach or threat, {COMPANY-NAME} reserves the right, without prior notice to the User, to disable or disconnect some or all {COMPANY-NAME} services related to connection of a {COMPANY-NAME} owned mobile device to the {COMPANY-NAME} network.

SECURITY CONSIDERATIONS AND ACCEPTABLE USE

Compliance by the User with the following {COMPANY-NAME} policies, published elsewhere and made available, is mandatory: Acceptable Use of Information Systems, {COMPANY-NAME} Owned Mobile Device Acceptable Use and Security, and other related policies including, but not limited to, Anti- Virus, E-Mail, Network Security, Password, Safeguarding Member Information, Telecommuting.

The User of the {COMPANY-NAME} owned mobile device shall not remove sensitive information from the {COMPANY-NAME} network, attack {COMPANY-NAME} assets, or violate any of the security policies related to the subject matter of this Agreement.

SUPPORT

{COMPANY-NAME} will offer the following support for the {COMPANY-NAME} owned mobile device: connectivity to {COMPANY-NAME} servers, including email and calendar, and security services, including policy management, password management, and decommissioning and/or remote wiping in case of loss, theft, device failure, device degradation, upgrade (trade-in), and carrier network or system outages that result in a failure of connectivity to the {COMPANY-NAME} network.

The User assumes full liability including, but not limited to, an outage or crash of any or all of the {COMPANY-NAME} network, programming and other errors, bugs, viruses, and other software or hardware failures resulting in the partial or complete loss of data or which render the mobile device inoperable.

_____

Device Make/Model

_____ _____

User Date

_____ _____

IT Department Management Date