Go-Cort, Inc. Mobile Device Management Policy

Last Update Status: Updated January 2021

1. Overview

This policy defines standards, procedures, and restrictions for any and all end users with legitimate business uses connecting mobile devices to Go-Cort, Inc's (DBA Apptoto) corporate network, digital resources, and data. The mobile device policy applies, but is not limited to, all devices and accompanying media that fit the following classifications:

- Smartphones
- Other mobile/cellular phones
- Tablets
- E-readers
- Portable media devices
- Portable gaming devices
- Laptop/notebook/ultrabook computers
- Wearable computing devices
- Any other mobile device capable of storing corporate data and connecting to a network

In order to enforce security and remote device management, only devices that meet the following criteria are allowed to access corporate resources:

- Smartphones, tablets, and other devices running Android version 2.3 (Gingerbread) and higher.
- Smartphones and tablets running iOS 5.0 and higher.
- Laptops running Windows 7 and higher
- Laptops running Mac OS X Cheetah (10.0) and higher

The policy applies to any mobile device that is used to access corporate resources, whether the device is owned by the user or by the organization.

2. Purpose

The primary goal of this policy is to protect the integrity of the confidential client and business data that resides within Go-Cort, Inc.'s technology infrastructure, including internal and external cloud services. 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 could potentially be accessed by unauthorized resources. A breach of this type may result in loss of information, damage to critical applications, loss of revenue, damage the company's public image, breach our data privacy requirements, and violate data privacy laws. Therefore, all employees, contractors, or personnel using a mobile device connected to Go-Cort, Inc.'s corporate network, and/or capable of backing up, storing, or otherwise accessing corporate data of any type, must adhere to company-defined processes and policies in doing so.

3. Scope

This policy applies to all Go-Cort, Inc. employees, including full and part-time staff, contractors, freelancers, and other agents who use any mobile device to access, store, backup, or relocate any organization or client-specific data. Such access to this confidential data is a privilege, not a right, and forms the basis of the trust Go-Cort, Inc. has built with its clients, supply chain partners, and other constituents. Consequently, employment at Go-Cort, Inc. does not automatically guarantee the initial or ongoing ability to use these devices to gain access to corporate networks and information.

The policy addresses a range of threats to enterprise data, or related to its use, such as:

Threat	**Description**
Device Loss	Devices used to transfer or transport work files could be lost or stolen.
Data Theft	Sensitive data is deliberately stolen and sold by an employee or unauthorized third party.
Malware	Viruses, Trojans, worms, spyware, malware, and other threats could be introduced to or via a mobile device.
Compliance	Loss or theft of financial and/or personal and confidential data could expose the enterprise 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 the Go-Cort, Inc. IT group. Unauthorized use of mobile devices to back up, store, and otherwise access any company-related data is strictly forbidden.

This policy is complementary to any previously implemented policies dealing specifically with data access, data storage, data movement, and connectivity of devices to any element of the company network and resources.

4. Responsibilities

4.1. The Owner of Go-Cort, Inc. has the overall responsibility for the confidentiality, integrity, and availability of corporate data as well as the execution and maintenance of information technology and information systems.

4.2. Other staff under the direction of the Owner are responsible for following the procedures and policies within information technology and information systems.

4.3. All Go-Cort, Inc. employees are responsible to act in accordance with company policies and procedures.

5. Affected Technology

5.1. Connectivity of all mobile devices will be centrally managed by Go-Cort, Inc.'s IT department and will use authentication and strong encryption measures. Although IT will not directly manage personal devices purchased by employees, end users are expected to adhere to the same security protocols when connected to non-corporate equipment. Failure to do so will result in immediate suspension of all network access privileges so as to protect the company's infrastructure.

6. Policy & Appropriate Use

6.1. It is the responsibility of any Go-Cort, Inc. employee using a 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. It is imperative that any mobile device that is used to conduct company business be used appropriately, responsibly, and ethically. Failure to do so will result in immediate suspension of that user's account. Based on this requirement, the following rules must be observed:

6.2. Access Control

6.2.1. IT reserves the right to refuse, by physical and non-physical means, the ability to connect mobile devices to corporate and corporate-connected infrastructure. IT will engage in such action if such equipment is being used in a way that puts the company's systems, data, users, and clients at risk.

6.2.2. Prior to initial use on the corporate network or related infrastructure, all mobile devices must be approved by IT. Go-Cort, Inc. will maintain a list of approved mobile devices and related software applications and utilities, and it will be stored in a company Google Drive. Devices that are not on this list may not be connected to corporate infrastructure. Employees may contact IT regarding the possible addition of new devices. Although IT currently only allows listed devices to be connected to enterprise infrastructure, it reserves the right to update this list in the future.

6.2.3. End users who wish to connect such devices to non-corporate network infrastructure to gain access to enterprise data must employ, for their devices and related infrastructure, security measures deemed necessary by the IT department. Enterprise data is not to be accessed on any hardware that fails to meet Go-Cort, Inc.'s established enterprise IT security standards.

6.2.4. All personal mobile devices attempting to connect to the corporate network through the Internet will be inspected by Go-Cort, Inc.'s IT department. Devices that are not approved by IT, are not in compliance with IT's security policies, or represent any threat to the corporate network or data will not be allowed to connect. Devices may only access the corporate network and data through the Internet using a Secure Socket Layer (SSL) Virtual Private Network (VPN) connection. The SSL VPN portal web address will be provided to users as required. Smart mobile devices such as smartphones, tablets, and laptops will access the corporate network and data using mobile VPN software installed on the device by IT.

6.3. Mobile Device Management

6.3.1. Go-Cort, Inc.'s IT department uses a mobile device management solution to secure mobile devices and enforce policies remotely. Before connecting a mobile device to corporate resources, the device must be set to be manageable by the Company’s solution.

6.3.2. The mobile device management solution’s client application must be installed on any mobile devices connecting to corporate resources. Even personal devices owned by employees must have the mobile device management system installed. The application can be installed by contacting the IT department.

6.3.3. The mobile device management solution enables IT to take the following actions on mobile devices: [remote wipe, location tracking, remote lock].

6.3.4. Any attempt to contravene or bypass the mobile device management implementation will result in immediate disconnection from all corporate resources, and there may be additional consequences in accordance with Go-Cort, Inc.’s overarching security policy.

6.4. Security

6.4.1. Employees using mobile devices and related software for network and data access will, without exception, use secure data management procedures. All mobile devices must be protected by a strong password; a PIN is not sufficient. All data stored on the device must be encrypted using strong encryption. See Go-Cort, Inc.’s password and encryption policies in the Clean Desk, Acceptable Use, and Bring Your Own Device Policies for additional background. Employees agree never to disclose their passwords to anyone.

6.4.2. All users of mobile devices must employ reasonable physical security measures. End users are expected to secure all such devices against being lost or stolen, whether or not they are actually in use and/or being carried.

6.4.3. Any non-corporate computers used to synchronize or backup data on mobile devices will have installed up-to-date anti-virus and anti-malware software deemed necessary by Go-Cort, Inc.'s IT department.

6.4.4. Passwords and other confidential data, as defined by Go-Cort, Inc.’s IT department, are not to be stored unencrypted on mobile devices.

6.4.5. Any mobile device that is being used to store or access Company data must adhere to the authentication requirements of the IT department. In addition, all hardware security configurations must be pre-approved by Company’s IT department before any enterprise data-carrying device can be connected to the corporate network.

6.4.6. IT will manage security policies, network, application, and data access centrally using whatever technology solutions it deems suitable. Any attempt to contravene or bypass that security implementation will be deemed an intrusion attempt and will be dealt with in accordance with Go-Cort, Inc.’s overarching security policy.

6.4.7. Employees, contractors, and temporary staff accessing Go-Cort, Inc. internet resources from a smartphone or tablet will NOT save their user credentials or internet sessions when logging in or accessing company resources of any kind.

6.4.8. Employees, contractors, and temporary staff will follow all enterprise-sanctioned data removal procedures to permanently erase company-specific data from such devices once its use is no longer required.

6.4.9. In the event of a lost or stolen mobile device, the user is required to report the incident to IT immediately. The device will be remotely wiped of all data and locked to prevent access by anyone other than IT. If the device is recovered, it can be submitted to IT for re-provisioning. The remote wipe will destroy all data on the device, whether it is related to company business or personal. The Go-Cort, Inc. Remote Wipe Waiver, which ensures that the user understands that personal data may be erased in the rare event of a security breach, must be agreed to before connecting the device to corporate resources.

6.4.10. Usage of location-based services and mobile check-in services, which use GPS capabilities to share real-time user location with external parties, is prohibited within the workplace.

6.4.11. Usage of a mobile device to capture images, video, or audio, whether native to the device or through third-party applications, is prohibited within the workplace.

6.4.12. Applications that are not approved by IT are not to be used within the workplace or in conjunction with corporate data.

6.5. Hardware & Support

6.5.1. 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 enterprise network.

6.5.2. Users will make no modifications to the hardware or software that change the nature of the device in a significant way (e.g. replacing or overriding the operating system, jail-breaking, rooting) without the express approval of Go-Cort, Inc.'s IT department.

6.5.3. IT will support the connection of mobile devices to corporate resources. On personally owned devices, IT will not support hardware issues or non-corporate applications.

6.6. Organizational Protocol

6.6.1. IT can and will establish audit trails, which will be accessed, published, and used without notice. Such trails will be able to track the attachment of an external device to the corporate network, and the resulting reports may be used for investigation of possible breaches and/or misuse. 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. in order to identify unusual usage patterns or other suspicious activity. The status of the device, including location, IP address, Serial Number, IMEI, may also be monitored. This monitoring is necessary in order to identify accounts/computers that may have been compromised by external parties or users who are not complying with Go-Cort, Inc.'s policies.

6.6.2. The end user agrees to immediately report to his/her manager and Company's IT department any incident or suspected incidents of unauthorized data access, data loss, and/or disclosure of company resources, databases, networks, etc.

6.6.3. Go-Cort, Inc. will not reimburse employees if they choose to purchase their own mobile devices. Users will not be allowed to expense mobile network usage costs.

6.6.4. Every mobile device user will be entitled and expected to attend a training session about this policy. While a mobile device user will not be granted access to corporate resources using a mobile device without accepting the terms and conditions of this policy, employees are entitled to decline signing this policy if they do not understand the policy or are uncomfortable with its contents.

6.6.5. Any questions relating to this policy should be directed to Go-Cort, Inc. Human Resources Department.

7. Policy Compliance

7.1. Compliance Measurement

Go-Cort, Inc. will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback from employees.

7.2. Exceptions

Any exception to the policy must be approved by Go-Cort, Inc. in advance.

7.3. Non-Compliance

Failure to comply with the Mobile Device Acceptable Use Policy may, at the full discretion of the organization, result in the suspension of any or all technology use and connectivity privileges, disciplinary action, and possibly termination of employment. Human Resources will be advised of breaches of this policy and will be responsible for appropriate remedial action.

8. Revision History

Date of Change	Responsible	Summary of Change
November 2020	Frank Cort	Adopted and customized to apptoto.com
January 2021	Frank Cort	Customized to Go-Cort, Inc. (DBA Apptoto)