Cogent E Services Private Limited

Mobile Device Security Policy

Based on ISO/IEC 27001:2013

Version: 3.2

Corporate Information Security Guidelines

Preface

The Cogent E Services Private Limited (hereafter referred to as "Cogent") Information Security Management System (ISMS) Team assumes responsibility for this document and updates it as required to meet the needs of users. The Cogent ISMS Team welcomes and solicits feedback from users of this document and its reference artifacts so that future revisions of this document will reflect improvements, based on new technology, organizational best practices, and lessons learned. It will be maintained by the Information Security Manager (ISM) and is subjected to review at a minimum on a yearly basis.

This document forms part of Cogent's ISMS Policy framework and as such, must be fully complied with.

Document Revision History

Version	Prepared by		Reviewed by		Approved by		Implementation Date	Summary of Changes
	By	Date	By	Date	By	Date		
0.1	ISM	03rd Dec'14	CISO	05th Dec'14	ISSC	--------	---------	Initial Draft
1	ISM	30th Dec'14	CISO	30th Dec'14	ISSC	30th Dec'14	1st Jan'15	First Revision
1.0	ISM	30th Dec'14	CISO	30th Dec'14	ISSC	30th Dec'14	1st Jan'15	New Template and updated document
1.1	ISM	13th Nov'15	CISO	13th Nov'15	ISSC	13th Nov'15	2nd Jan'16	
1.2	ISM	15th Oct'16	CISO	15th Oct'16	ISSC	15th Oct'16	31st Dec'16	
2.0	ISM	15th dec'17	CISO	15th dec'17	ISSC	15th dec'17	1st Jan'18	
2.1	ISM	22nd dec'18	CISO	22nd dec'18	ISSC	22nd dec'18	3rd Jan'19	
3.0	ISM	07th Dec'19	CISO	07th Dec'19	ISSC	07th Dec'19	10th Dec'19	
3.1	ISM	07 Jul'21	CISO	07 Jul'21	ISSC	07 Jul'21	11th Jul'21	
3.2	ISM	07 Apr'22	CISO	07 Apr'22	ISSC	07 Apr'22	11th Apr'22	

Document Distribution

The Cogent Chief Information Security Officer (CISO) shall distribute this document to members of Information Security Steering Committee (hereafter referred to as ISSC) and

Information Security Implementation Committee (hereafter referred to as ISIC).

The softcopy of the manual and related documents will be accessible to all employees in read-only mode through intranet server at location http://*********

The CISO will ensure that any update to the Cogent ISMS is incorporated on the intranet server and is communicated to all employees of Cogent through an appropriate mode such as e-mail.

Distribution List

Name	Acronym
Information Security Steering Committee	ISSC
Information Security Implementation Committee	ISIC
Chief Information Security Officer	CISO
All employees and relevant external parties.	-

Conventions

The statements containing the words 'shall' and 'required to' in the document are mandatory rules. Failure to observe these rules may be construed as non-compliance to the policy.
The statements containing the words 'should' and 'recommended' imply a desirable requirement. Failure to adhere to these rules may not be a direct non-compliance.

Contents

1. Introduction

The use of handheld devices is increasing in corporate environments, providing mobile services and constant connectivity to mobile workers. Due to the fact that handheld devices are recent and not yet properly managed, they present new threats to corporate assets. Handheld devices combine security challenges posed by laptops, removable storage (e.g. USB keys), and cameras.

Every member of Cogent E Services Private Limited (hereafter referred to as "Cogent") community who utilizes a laptop computer or Mobile Device (e.g. portable hard drives, USB flash drives, smart phones, tablets) is responsible for Cogent data stored, processed or transmitted via that computer or Mobile Device and for following the security requirements set forth in this policy and in the Information Security Policy.

.

2. Objective

The objective of this policy document is to establish the criteria governing the authorized use of personal or corporate owned smart phone and tablet (mobile) devices where the owner has established access to Cogent Systems enabling them to send and receive work related email messages and conduct other company business.

3. Scope

The Mobile Device Security Policy applies to

a) All mobile devices, whether owned by or owned by employees, inclusive of smart phones and tablet computers that have access to corporate networks, data and systems are governed by this mobile device security policy.

b) all employees, consultants, temporaries, and others not mentioned who access Cogent information assets and information processing facilities

c) to all Cogent sites in the scope of its Information Security Management System

Exemptions:

3.1.1 The scope of this policy does not include corporate IT-managed laptops.

3.1.2 Where there is a business need to be exempted from this policy (too costly, too complex, adversely impacting other business requirements) a risk authorized by security management must be conducted.

3.1.3 Applications used by employees on their own personal devices which store or access corporate data, such as cloud storage applications, are also subject to this policy.

4. Mobile Device Security Program

This security policy establishes rules for the proper use of handheld devices in corporate environments in order to protect the confidentiality of sensitive data, the integrity of data and applications, and the availability of services at, protecting both handheld devices and their users, as well as corporate assets (confidentiality and integrity) and continuity of the business (availability).

The policy and supporting security measures should be adopted to manage the risks introduced by using mobile devices.

This policy applies to all employees, consultants, vendors, contractors, students, and others using business or private mobile handheld devices on any premises occupied by Cogent .

Adherence to these requirements and the security policies derived from them and implementation of provisions is binding across the whole of Cogent , its subsidiaries and majority holdings.

Willful or negligent infringement of the policies jeopardizes the interests of Cogent and will result in disciplinary, employment, and/or legal sanctions. In the case of the latter the relevant line managers and where applicable legal services shall bear responsibility.

These requirements and the security policies derived from them and implementation provisions also apply to all suppliers of Cogent . They shall be contractually bound to adhere to the security directives. If a contractual partner is not prepared to adhere to the provisions, he must be bound in writing to assume any resulting consequential damage

How to Protect Non-Public Information

Every user of laptop computers or other Mobile Devices must use reasonable care, as outlined in Cogent Information Security Policy, to protect Cogent non-public information. The Information Security Policy details examples of non-public information and the requirements for securing this data during transmission and at rest. Protection of non-public information against physical theft or loss, electronic invasion, or unintentional exposure is provided through a variety of means, which include user care and a combination of technical protections such as authentication and encryption that work together to secure electronic data Mobile Devices against unauthorized access.. The use of unprotected Mobile Devices to access or store non-public information is prohibited regardless of whether or not such equipment is owned or managed by Cogent. The IT Support Center (ITSC) should be contacted to determine if appropriate protections are already in place and to assist with enabling the security measures for laptops or other Mobile Devices. The Information Security Policy details requirements for securing this data during transmission and at rest.

Technical Requirements

1. Devices must use the following Operating Systems: Android 2.2 or later, iOS 4.x or later.
2. Devices must store all user-saved passwords in an encrypted password store.
3. Devices must be configured with a secure password that complies with's password policy. This password must not be the same as any other credentials used within the organization.
4. Only devices managed by IT will be allowed to connect directly to the internal corporate network.
5. These devices will be subject to the valid compliance rules on security features such as encryption, password, key lock, etc. These policies will be enforced by the IT department using Mobile Device Management software.

User Requirements

1. Users may only load corporate data that is essential to their role onto their mobile device(s).
2. Users must report all lost or stolen devices to IT immediately.
3. If a user suspects that unauthorized access to company data has taken place via a mobile device, they must report the incident in alignment with ’s incident handling process.
4. Devices must not be “jailbroken” or “rooted”* or have any software/firmware installed which is designed to gain access to functionality not intended to be exposed to the user.
5. Users must not load pirated software or illegal content onto their devices.
6. Applications must only be installed from official platform-owner approved sources. Installation of code from untrusted sources is forbidden. If you are unsure if an application is from an approved source contact IT.
7. Devices must be kept up to date with manufacturer or network provided patches. As a minimum patches should be checked for weekly and applied at least once a month.
8. Devices must not be connected to a PC which does not have up to date and enabled anti-malware protection and which does not comply with corporate policy.
9. Devices must be encrypted in line with compliance standards.
10. Users may must be cautious about the merging of personal and work email accounts on their devices. They must take particular care to ensure that company data is only sent through the corporate email system. If a user suspects that company data has been sent from a personal email account, either in body text or as an attachment, they must notify IT immediately.
11. The above requirements will be checked regularly and should a device be noncompliant that may result in the loss of access to email, a device lock, or in particularly severe cases, a device wipe.
12. The user is responsible for the backup of their own personal data and the company will accept no responsibility for the loss of files due to a non compliant device being wiped for security reasons.
13. Users must not use corporate workstations to backup or synchronize device content such as media files, unless such content is required for legitimate business purposes.

**To jailbreak/root a mobile device is to remove the limitations imposed by the manufacturer. This gives access to the operating system, thereby unlocking all its features and enabling the installation of unauthorized software.*

Actions which may result in a full or partial wipe of the device, or other interaction by IT

1. A device is jail broken/rooted
2. A device contains an app known to contain a security vulnerability (if not removed within a given time-frame after informing the user)
3. A device is lost or stolen
4. A user has exceeded the maximum number of failed password attempts

Reporting Loss/Theft of Equipment or Data

Cogent employees who possess Cogent owned laptop computers and Mobile Devices are expected to secure them whenever they are left unattended. Accordingly, Cogent will not reimburse for the loss of a laptop computer or other Mobile Device unless it is burglarized (e.g., taken from a locked desk, cabinet, closet, or office, the item was secured by using a locking cable and there are signs of forced entry thereto).

In the event an Cogent -owned or managed laptop computer or Mobile Device is lost or stolen, the theft or loss must be reported immediately to the Police Department in accordance with **Cogent Policy for Theft.**

In the event Cogent non-public information is contained on any Mobile Device that is lost or stolen, the ITSC must be contacted immediately.

Requirements When Traveling Overseas

Cogent personnel carrying Cogent issued laptops or Mobile Devices while traveling abroad, whether on business or for pleasure, must comply with the applicable trade control laws.

Before traveling abroad with a laptop or other Mobile Device, Cogent staff must understand the restrictions described here. The Office of the Chief Information Security Officer can provide further guidance and information on these limitations.

5. Roles & responsibilities

1. All employees are responsible for adhering to the information security provisions.

Specific tasks are documented in the definition of roles.

2. For each role a person must be defined by name and made known to the IT security department.

3. Individuals may assume several roles.

4. Definition of roles applies to all the security policies and implementation provisions

Derived from this policy.

5. IT security ensures that the roles are documented consistently in corporate quality management.

The following table represents roles and responsibilities at the management level:

Name	Responsibilities
Business owner	Ensures the necessary resources are provided to IT Department
IT governance	Maintains security policies: - Creation, adaptation to existing policies in place – Maintenance up-to-date - Guidelines and procedures to implement this policy exist and are communicated to the intended people Policy and procedures are documented - Policies and procedures are well communicated Is responsible for policy enforcement: Ensures that users are properly trained
IT department, IT staff, security administrator, devices manager	Are responsible of managing mobile handheld devices Manage the inventory Ensure that the necessary services are available to users Provide the necessary resources for the use of services Are responsible for policy enforcement: - Via the appropriate working controls - Make requests for changes/adaptations in this policy to IT governance
Users, Employees	Must read, understand and agree to security policies - Must conform to security policies - Must inform IT staff of exceptions to security policies

The IT department is responsible of the application of this policy in a practical sense. It is in charge of mobile devices management and is responsible for providing the necessary complementary documentation and information for the best application of this policy

User Responsibility

General

User agrees to a general code of conduct that recognizes the need to protect confidential data that is stored on, or accessed using, a mobile device. This code of conduct includes but is not limited to:

- Doing what is necessary to ensure the adequate physical security of the device
- Maintaining the software configuration of the device – both the operating system and the applications installed.
- Preventing the storage of sensitive company data in unapproved applications on the device
- Ensuring the device's security controls are not subverted via hacks, jailbreaks, security software changes and/or security setting changes
- Reporting a lost or stolen device immediately

Personally Owned Devices

The personal smart phone and tablet devices are not centrally managed by Corporate IT Services. For this reason, a support need or issue related to a personally owned device is the responsibility of the device owner. Specifically, the user is responsible for:

- Settling any service or billing disputes with the carrier o Purchasing any required software not provided by the manufacturer or wireless carrier
- Device registration with the vendor and/or service provider
- Maintaining any necessary warranty information
- Battery replacement due to failure or loss of ability to hold a charge
- Backing up all data, settings, media, and applications
- Installation of software updates/patches
- Device Registration with Corporate IT Services Corporate Owned Devices Corporate owned smart phone and tablet devices are centrally managed by Corporate IT Services.

Specifically, the user is responsible for:

- Installation of software updates
- Reporting lost or stolen device immediately

Corporate IT Services Support Responsibility

The following services related to the use of a personal smart phone or tablet are provided by Corporate IT Services:

- Enabling the device to access the web-based interface of the email system. This is a default capability. Personal device registration is not required.
- Enabling the device to access the web-based application system. This is a default capability. Personal device registration is not required. »
- Email, Calendar and Contact Sync service configuration. Personal device registration is required.
- Wi-Fi Internet Access configuration. This service is limited to the facility. Personal device registration is required. Personal email will not sync when connected to Cogent network
- Devices not compliant with secure configuration standards will be unsubscribed from Mobile Device services.
- Security Policy Requirements
- The user is responsible for securing their device to prevent sensitive data from being lost or compromised and to prevent viruses from being spread. Removal of security controls is prohibited.
- User is forbidden from copying sensitive data from email, calendar and contact
- applications to other applications on the device or to an unregistered personally owned device

Security and configuration requirements:

- Sensitive data will not be sent from the mobile device. Secure Mail services will be utilized in such cases.
- The device operating system software will be kept current.
- The data on the device will be removed after 10 failed logon attempts.
- The device will be configured to encrypt the content.
- The device will be configured to segregate corporate data from personal data.
- User agrees to random spot checks of device configuration to ensure compliance with all applicable Corporate information security policy

Loss, Theft or Compromise

- If the device is lost or stolen, or if it is believed to have been compromised in some way, the incident must be reported immediately by contacting Physical Security, the Technology Service Center or a member of the user's management team.

Company's Right to Monitor and Protect

- The Company has the right to, at will:
- Monitor Corporate messaging systems and data including data residing on the user's mobile device
- Modify, including remote wipe or reset to factory default, the registered mobile device configuration remotely

Device Reset and Data Deletion

- Device user understands and accepts Cogent data on the device will be removed remotely under the following circumstances:
    - Device is lost, stolen or believed to be compromised
    - Device is found to be non-compliant with this policy
    - Device inspection is not granted in accordance with this policy
    - Device belongs to a user that no longer has a working relationship with the Company.
    - Note: the "selective" wipe capability is available for IOS based devices only. BlackBerry OS based devices will be reset to the factory default.
    - User decides to un-enroll from the Mobile Device Policy and Management solution

Enforcement

- Any user found to have violated this policy may be subject to disciplinary action, including but not limited to:
  - Account suspension
  - Revocation of device access to Cogent System
  - Data removal from the device
  - Employee termination

[END OF DOCUMENT]