Cogent E Services Private Limited

Human Resource 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.

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	

Copyright

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://172.19.197.214/Policies

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

Contents

1. INTRODUCTION 5
2. OBJECTIVE 5
3. SCOPE 5
4. APPLICABILITY 6
5. ROLES RESPONSIBILITIES AND AUTHORITIES 6
6. POLICY 6
7. EXECUTION RESPONSIBILITY 12
8. RELATED DOCUMENTS 12

1. Introduction

Overview

The objective of Human Resources Security is to ensure that all employees (including contractors and any user of sensitive data) are qualified for and understand their roles and responsibilities of their job duties and that access is removed once employment is terminated.

The three areas of Human Resources Security are:

- **Pre-Employment:** This topic includes defining roles and responsibilities of the job, defining appropriate access to sensitive information for the job, and determining depth of candidate's screening levels - all in accordance with the company's information security policy. During the phase, contract terms should also be established.
- **During Employment:** Employees with access to sensitive information in an organization should receive periodic reminders of their responsibilities and receive ongoing, updated security awareness training to ensure their understanding of current threats and corresponding security practices to mitigate such threats.
- **Termination or Change of Employment:** To prevent unauthorized access to sensitive information, access must be revoked immediate upon termination/separation of an employee with access to such information. This also includes the return of any assets of the organization that was held by the employee.

Human resources policies and practices should reduce the risk of theft, fraud or misuse of information facilities by employees, contractors and third-party users.

2. Objective

The objective of this document is to govern the human resources aspect of information security for employees of Cogent to be able to protect information assets from theft, fraud and misuse, and to provide a sense of security in the day to day operations of Cogent personnel and users of Cogent information assets.

The purpose of this policy is to ensure that employees, contractors and third party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities.

Non-compliance with this policy could have a significant effect on the efficient operation of Cogent and may result in financial loss and an inability to provide necessary services to our customers

3. Scope

This document addresses policies related to security of information assets of Cogent from human aspects. The organization’s human resources policies, taken as a whole, should extend to all the persons within and external to the organization that do (or may) use information or information processing facilities.

This could include:

- tailoring requirements to be suitable for particular roles within the organization for which persons are considered;
- ensuring that persons fully understand the security responsibilities and liabilities of their role(s);
- ensuring awareness of information security threats and concerns, and the necessary steps to mitigate those threats; and

- equipping all persons to support organizational privacy and security policies in the course of their normal work, through appropriate training and awareness programs that reduce human error; and
- ensuring that persons exit the organization, or change employment responsibilities within the organization, in an orderly manner

To support this policy Cogent will establish guidelines, procedures, and requirements to ensure the appropriate protection to Cogent information and information systems.

4. Applicability

The policies detailed in this document are applicable to personnel and users of Cogent information assets.

This policy applies to all employees, consultants, temporaries, and others not mentioned who access Cogent information assets and information processing facilities. This policy applies at all times and should be adhered to whenever accessing Cogent information in any format, and on any device.

5. Roles Responsibilities and Authorities

Security roles responsibilities and authorities of employees, contractors and third-party users should be defined and documented in accordance with the organization's information privacy and security policies.
This could include:

- requirements to act in accordance with the organization's policies, including execution of all processes or activities particular to the individual's role(s);
- requirements to protect all information assets from unauthorized access, use, modification, disclosure, destruction or interference;
- requirements to report security events, potential events, or other risks to the organization and its assets; and
- assignment of responsibility to individuals for actions taken or, where appropriate, responsibility for actions not taken, along with appropriate sanctions for mal-, mis- or nonfeasance

6. Policy

6.1. Security prior to employment

6.1.1. Roles and responsibilities

6.1.1.1. For all the jobs the security roles and responsibilities of employees, contractors and third party users must be documented and must include general as well as specific responsibilities for implementing or maintaining security in Cogent .

6.2. Screening

Pre-employment screening

6.2.1. Appropriate background verification checks (“screening”) for all candidates for employment, contractor status, or third party user status, should be carried out by the organization or appropriate third parties.

6.2.2. This could include screening that:

6.2.2.1. is commensurate with the organization's business needs, and with relevant legal-regulatory-certificatory requirements;
6.2.2.2. takes into account the classification(s)/sensitivity(ies) of the information or information processing facilities to be accessed, and the perceived risks;
6.2.2.3. takes into account all privacy, protection of personal data and other relevant employment legislation; and
6.2.2.4. includes, where appropriate, components such as identity verification, character references, CV verification, criminal and credit checks

6.3. Background/reference checks must be performed on all personnel performing sensitive or critical job roles. Also, personnel who are third party service providers must have undergone a background /reference check by their respective organizations and the assurance of their background /reference should be provided to Cogent. Information provided by personnel at the time of recruiting must be subjected to verification procedures.

6.4. Appropriate background verification checks -- also known as "screening" or "clearance" -- for all candidates for employment, contractor status, or third party user status, should be carried out. Control includes checks that are:

6.4.1. commensurate with the organization's business needs, and with relevant legal-regulatory-certificatory requirements;

6.4.2. take into account the classification(s)/sensitivity(ies) of the information to be accessed, and the perceived risks;

6.4.3. take into account all privacy, protection of personal data and other relevant employment legislation; and

6.4.4. Include, where appropriate, components such as identity verification, character references, CV verification, criminal and credit checks.

6.5. Background verification checks must be carried out on all potential users, in accordance with all relevant laws, regulations and ethics. The level of such checks must be appropriate to the business requirements, the classification of the information to be accessed, and the risks involved. The basic requirements for Cogent employment must be:

6.5.1. Minimum of two satisfactory references.

6.5.2. Completeness and accuracy check of employee’s application form.

6.5.3. Confirmation of claimed academic and professional qualifications.

6.5.4. Identity check against a passport or equivalent document that contains a photograph.

6.6. **Terms and Conditions of employment**

6.6.1. All supervisors are responsible for the performance and conduct of staff reporting to them. Project Leaders are required to monitor performance and conduct of each of their staff, as well as to assess their impact on the security of the Information Assets to which the staff has access.

6.6.2. All users of Cogent Information Assets must accept and sign non-disclosure obligations. All employees of Cogent must sign the terms and conditions of employment as an indication of acceptance.

6.6.3. Employees, contractors, and third party users should agree to and sign a statement of rights and responsibilities for their affiliation with the organization, including rights and responsibilities with respect to information privacy and security.

6.6.4. This statement could include specification of:

6.6.4.1. the scope of access and other privileges the person will have, with respect to the organization's information and information processing facilities;

6.6.4.2. the person's responsibilities, under legal-regulatory-certificatory requirements and organizational policies, specified in that or other signed agreements (see Additional pre-employment agreements);

6.6.4.3. responsibilities for classification of information and management of organizational information facilities that the person may use;

6.6.4.4. procedures for handling sensitive information, both internal to the organization and that received from or transferred to outside parties;

6.6.4.5. responsibilities that extend outside the organization's boundaries (e.g., for mobile devices and tele-working);

6.6.4.6. the organization's responsibilities for handing of information related to the person him/herself, generated in the course of an employment, contractor or other third party relationship;

6.6.4.7. an organizational code of conduct or code of ethics to the employee, contractor or third party; and

6.6.4.8. actions that can be anticipated, under the organization's disciplinary process, as a consequence of failure to observe security requirements

6.6.5. **Additional pre-employment agreements** :Where appropriate, employees, contractors and third-party users should be required to sign, prior to being given access or other privileges to information or information processing facilities, additional:

6.6.5.1. confidentiality or non-disclosure agreements ; and/or

6.6.5.2. acceptable use of assets agreements

6.7. Security during employment

6.7.1. Management responsibilities

Management should require employees, contractors and third party users to apply security controls in accordance with established policies and procedures of the organization. This could include:

6.7.1.1. appropriately informing all employees, contractors and third party users of their information security roles and responsibilities, prior to granting access to sensitive information or information systems (see Terms and conditions of employment);

6.7.1.2. providing all employees, contractors and third parties with guidelines/rules that state the security expectations of their roles within the organization;

6.7.1.3. achieving an appropriate level of awareness of security controls among all employees, contractors and third parties, relevant to their roles and responsibilities,

6.7.1.4. achieving an appropriate level of skills and qualifications, sufficient to execute those security controls;

6.7.1.5. assuring conformity to the terms and conditions of employment related to privacy and security;

6.7.1.6. motivating adherence to the privacy and security policies of the organization, such as with an appropriate sanctions policy; and

6.7.1.7. mitigating the risks of a failure to adhere to policies, by ensuring that all persons have appropriately-limited access to the organization's information and information facilities

Employees joining Cogent, at the time of induction training, are briefed on security roles and responsibilities prior to granted access to sensitive information.

All employees, contractors and third party users using the information processing facilities of Cogent are provided with an awareness session on Do's and Don'ts that needs to be adhered by them.

6.7.2. Information security awareness, education and training

All employees of the organization, and, where relevant, contractors and third party users, should receive appropriate awareness training in and regular updates of organizational policies and procedures relevant to their job functions. Training and Awareness Programs are provided to all the employees of Cogent during induction as well on an ongoing basis to reinforce the security awareness among all its employees.

This could include:

6.7.2.1. a formal induction process that includes information privacy and security training, prior to being granted access to information or information systems; and

6.7.2.2. ongoing training in security control requirements, legal-regulatory-certificatory responsibilities, and generally accepted security procedures, suitable to the person's rules and Training requirements of all the employees must be reviewed regularly and training calendar must be prepared for each department

6.7.3. **Disciplinary process**

There should be a formal disciplinary process for employees who have committed a security breach. This could include requirements for:

6.7.3.1. appropriate evidentiary standards to initiate investigations (e.g., "reasonable suspicion" that a breach has occurred);

6.7.3.2. appropriate investigatory processes, including specification of roles and responsibilities, standards for collection of evidence and chain of custody of evidence;

6.7.3.3. disciplinary proceedings that observe reasonable requirements for due process and quality of evidence;

6.7.3.4. reasonable evidentiary and burden-of-proof standards to determine fault, that ensure correct and fair treatment for persons suspected of a breach; and

6.7.3.5. sanctions that appropriately take into consideration factors such as the nature and gravity of the breach, its impact on operations, whether it is a first or repeat offense, whether or not the violator was appropriately trained, whether or not the violator exercised due care or exhibited negligence.

6.7.4. A formal disciplinary process for employees who have violated the organizational security policies and procedures must be defined and implemented.

6.7.5. Any employee who absents himself from work for three days is considered to be absconding. For such employees HR department takes all steps as are required in case of an employee who has been terminated.

6.8. **Security on termination or change of employment**

6.8.1. **Termination responsibilities**

Prior to relieving an employee, the HR ensures that all assets and information with the employee is retrieved to a rightful owner of Cogent .

Once the employee is able to furnish the proper handing over of the charge and return of company property such as access card, keys, project artifacts, and other information processing facilities, the HR shall complete the employee's full & final settlement.

Responsibilities and practices for performing employment termination or change of employment should be clearly defined and assigned. This could include:

1. termination processes that ensure removal of access to all information resources (see also Removal of access rights);

2. changes of responsibilities and duties within the organization processed as a termination (of the old position) and re-hire (to the new position), using standard controls for those processes unless otherwise indicated;

3. processes ensuring that other employees, contractors and third parties are appropriately informed of a person's changed status; and

4. any post-employment responsibilities are specified in the terms and conditions of employment, or a contractor's or third party's contract.

6.8.2. Return of assets

Employee shall return all assets of Cogent , which includes software, data, manual, access cards, etc. and any information processing facilities viz., laptop, etc.

All employees, contractors and third parties should return all of the organization's information and physical assets in their possession upon termination of the employment relationship or contract. This could include:

1. a formal process for return (e.g., checklists against inventory) of the organization's hardware, software and data media;

2. a formal process for return or destruction of organizational data of any kind; and

3. where the employee, contractor or third party uses personal equipment, requirements for secure erasure of software and data belonging to the organization

6.8.3. Removal of access rights

Access rights to information and information processing facilities should be removed upon termination of the employment or contractual relationship. This could include:

6.8.3.1. changes of employment or contractual status include removal of all rights associated with prior roles and duties, and creation of rights appropriate to the new roles and duties;

6.8.3.2. removal or reduction of access rights in a timely fashion; and

6.8.3.3. removal or reduction of access rights prior to the termination, where risks indicate this step to be appropriate (e.g., where termination is initiated by the organization, or the access rights involve highly sensitive information or facilities)

6.8.3.4. Before leaving the organization, every employee shall have to obtain clearance from every department and complete a clearance form.

HR shall inform all relevant teams, including the IT and Admin teams, whenever an employee is about the leave the organization, usually on the last working day of the employee.

Once IT receives information from HR about an employee leaving the organization, all access to electronic information, including emails and system access, shall be immediately revoked.

Once Admin received information from HR about an employee leaving the organization, all physical access to Cogent 's offices is immediately revoked.

7. Execution Responsibility

1.1. The Head – HR is responsible for ensuring adherence to policies stated in this document.

Termination Responsibilities Line managers must notify the ICT Helpdesk in a timely manner of the impending termination or suspension of employment so that their access can be suspended. ICT Helpdesk must notify the appropriate system owners who must suspend access for that user at an appropriate time, taking into account the nature of the termination. Responsibilities for notifying changes, performing employment termination or change of employment must be clearly defined and assigned

8. Related Documents

1.2. Human Resource Security Procedure (ISMS-L3-A7)