Cogent E Services Private Limited

Incident Management Procedure

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. It states the steps Cogent will take to limit the opportunity for information leakage by implementation of best practice, processes and procedures.

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 to adhere to these rules may not be a direct non-compliance.

Table of Contents

1. Objective

To detect, respond to and manage security incidents effectively to ensure minimum damages; and to learn from the incidents to avoid repetition in future at Cogent E Services Private Limited (hereafter referred to as "Cogent").

2. Scope

This document covers procedures related to defining and implementing an Incident Management Process in order to effectively respond to security incidents.

3. Applicability

These procedures apply to staff, related third parties and vendors, applications, information and information resources of Cogent

4. Roles and Responsibilities

4.1 Incident Management Team (IMT)

4.1.1 The Incident Management Team should comprise of the following:

4.1.1.1 Incident Management Leader

4.1.1.2 Incident Management Coordinator

4.1.1.3 Heads of Support Teams

4.1.1.4 Heads of Business Units

4.2 Incident Management Leader (IML)

4.2.1 Managing Director is the IML and should be responsible for the overall management of the Incident, and taking critical decisions related to business operations.

4.2.2 He would also be responsible for assisting the CISO of Cogent in interfacing with the media for public communications such as press releases, media briefings, etc.

4.3 Incident Management Coordinator (IMC)

4.3.1 The CISO is the IMC for all security related incidents. He should be the 'single point of contact' for all members of the Incident Management Team and other Cogent employees. He should collate as much information as possible about the Incident, and evaluate the Incident so as to classify it as per the defined criteria. He is also responsible for escalating the incident to the right team.

4.3.2 The responsibilities of the IMC will also include coordinating with the Incident Management Leader for managing and resolving the Incidents.

4.3.3 Post resolution of the incident, the IMC should be responsible for documenting the detailed Incident Report and identifying corrective actions. He must follow-up on the corrective actions to ensure that these are thoroughly implemented.

4.4 Heads of Support Teams

4.4.1 Head of Support Teams such as Technology, Administration, Human Resources, Finance, etc. form a vital component of the Incident Management Team. They are responsible for acting upon the Incidents as per the procedures detailed in this document.

4.4.2 Head Technology will primarily look after IT security related incidents such as virus outbreaks, unplanned network outage, disk failures, etc.

4.4.3 Head Administration will primarily look after physical security related incidents such as fire, health hazards, bomb threats, intruders, access control failures, flooding, etc.

4.4.4 Head – Human Resources will primarily look into incidents involving employees, such as injuries, casualties, workplace harassment, etc. The Head – HR will also be involved in any case involving a breach of security policy by any staff member leading to a disciplinary action.

4.5 Heads of Business Units

4.5.1 Heads of affected business units will also form a part of the Incident Management Team. The primary role of business unit heads would be to coordinate with their clients and keep them notified in case the incident is likely to materially affect the confidentiality, integrity or availability of information.

4.5.2 Business unit heads will also actively coordinate with the Incident Management Leader (IML) to quantify the damage caused by the incident to the unit's operations and ability to handle workflow.

5. Handling information security events

5.1 Pre Incident

5.1.1 Vulnerability Assessment

5.1.1.1 The objective of this assessment is to identify threats/vulnerabilities to the information assets of Cogent and to assess the risks and its impact on business.

5.1.2 Vulnerability Treatment Plan

5.1.2.1 To incorporate appropriate controls through policy and/or procedure so as to prevent, eliminate, transfer or minimize the identified risks.

5.1.3 Pre plan procedures

5.1.3.1 Incident management policies and procedures are in place to prevent the situation of incidents and disruptions in the work. These plans need to be regularly updated after having regular discussions with all the support and project heads.

5.1.4 Cooperation with Local Responders

5.1.4.1 First step would be to determine the potential responders. Potential responders would include Fire, Law enforcement, emergency medical services, hospitals etc. Then the employees needs to be trained regarding building maps, access protocols, emergency procedures and understanding their individual responsibilities during incident.

5.1.5 Training & Drills

5.1.5.1 Employees need to be trained on a regular basis on all the aspects of incidents. Cogent has a dedicated email ID to report any incident. The trainings would include awareness on emergency evacuation of the building, knowing individual roles and responsibilities etc. The testing will also include exercises such as call tree testing, fire drills, BCP testing etc.

5.2 During Incident

5.2.1 Identification, Detection and Initial Reporting

5.2.2 A security incident or weakness may be detected by anybody in the organization. The Incidents can be classified as detailed below.

5.2.2.1 **Type A: IT incidents** are detected and reported by the tools like IDSs, Firewalls, etc. The Network Management and monitoring Systems would be programmed with the desired thresholds for each defined Incident and would immediately generate a log or email to the Compliance / Systems/Network Engineers. IT helpdesk issues Incident tickets and escalations are reported to Incident team leader.

5.2.2.2 **Type B: Non - IT Incidents** may be detected by anybody in the organization. The concerned employee must immediately bring it to the notice of Compliance Team, who shall issue an Incident Ticket (Incident Reference Number). The Incident can be reported verbally or through email. It is the responsibility of the IMC to log and maintain all Incident details in soft form or in papers.

5.2.3 The IMC shall delegate all IT related incidents to System/Network Engineers for further action. The engineers must collect the reported facts (symptoms of problem) of the reported Incident and document (Refer: **ISMS–L4–26 Incident Report**) these findings. It should at least cover the following:

5.2.3.1 Time of the Incident

5.2.3.2 Nature of the Incident

5.2.3.3 Detailed facts of the Incident

5.2.3.4 Activity/error log(s) in the system.

5.3 Classification and Escalation

5.3.1 Classification

5.3.1.1 The IMC should classify the incident based on the matrix given below. One should assign the classification based on the information collected from the person reporting the incident. Based on the criteria outlined below, IMC shall inform relevant members of the Incident Management Team.

5.3.1.2 Incidents are classified based on the following:

a. Operational Impact

b. Information classification

c. Legal / Regulatory Impact

d. Contractual Impact

e. Availability

f. Propagation

Severity **Lowest** ◄·····► **Highest**

Impact Type	Level 0	Level 1	Level 2	Level 3
Operational	No or negligible Loss Affects <= 5 resources[1]	Minor Impact on operations Affects > 5 resources[1]	Significant Impact on Operations Affects > 30 resources[1]	Major Impact on operations Affects > 100 resources[1]
Information	Data classified as "Public": • Availability affected or lost • Integrity violated • Confidentiality suspect or compromised	Data classified as "Internal": • Availability affected or lost • Integrity violated • Confidentiality suspect or compromised	Data classified as "Confidential" or Personally Identifiable Information (PII): • Availability affected or lost • Integrity violated • Confidentiality suspect or compromised	Data classified as "Highly Confidential": • Availability affected or lost • Integrity violated • Confidentiality suspect or compromised
Legal / Regulatory	No or negligible Impact	Minor Impact - can be remedied immediately with negligible fines	Significant Impact - can be remedied but results in minor financial loss	Major Impact - cannot be remedied without substantial financial loss
Contractual	No or negligible breach of SLA	Minor breach of SLA - can be remedied immediately with negligible financial / operational impact to client	Significant breach of SLA - can be remedied but results in minor financial / operational impact to client	Major breach of SLA - cannot be remedied without substantial financial / operational loss to client
Availability	No or negligible Impact Outage <= 5 resources[1] Individual level outage	Minor Impact Outage > 5 resources[1] Team level outage	Significant Impact Outage > 30 resources[1] Project level outage	Major Impact Outage > 100 resources[1] Facility level outage
Propagation	No or negligible propagation One-off remote occurrence	Minor Impact Local occurrence and unlikely to spread further	Significant Impact Local occurrence but likely to spread and affect to a larger group	Major Impact Likely to propagate or has already propagated across groups

[1] The term “resources” includes people, technology, or infrastructure resources

Any incident where RCA is Integrity, Shall be considered as level 3-refereed to ISC to action.

5.3.2 **Escalation**

5.3.2.1 The IMC is the first point of notification for all security incidents.

5.3.2.2 Depending upon the nature and severity of the incident, IMC shall escalate it to the relevant member(s) of the IMT.

5.3.2.3 In case the incident results in a suspected or actual security breach or data leakage, appropriate client security and vendor governance teams must be informed immediately, or within 24 hours of the incident.

5.3.2.4 In certain cases, an incident may need to be reported to the law enforcement agencies or regulators. In such cases, evidence collection and investigation procedures need to be followed.

5.4 **Containment and Analysis**

5.4.1 Relevant member(s) of the IMT must visit the location (place, computer, server, etc.) to collect further details immediately and make appropriate steps to isolate and contain the incident if it is capable of spreading to other assets. If the IMT, by itself, is unable to identify the probable cause and the probable resolution, it must contact specialist vendors or any other appropriate personnel.

5.4.2 The IML shall convene a special committee to liaise with the law enforcement agencies to address the following issues:

5.4.2.1 Establishing a prior liaison with law enforcement agencies

5.4.2.2 Deciding when and if to involve these agencies

5.4.2.3 Setting up means of reporting such crimes

5.4.2.4 Establishing procedures for handling and processing reports of computer crime

5.4.2.5 Planning for and conducting investigations

5.4.2.6 Consulting the legal department and internal Incident Management Team

5.4.2.7 Involving senior management and the appropriate departments, such as legal, internal audit, and human resources

5.4.2.8 Ensuring the proper collection of evidence, which includes identification and protection of the various storage media

5.5 **Post Incident**

5.5.1 **Collection of Evidence**

5.5.1.1 The gathering, control, storage, and preservation of evidence are extremely critical in any legal investigation. Because the evidence may be intangible and subject to easy modification without a trace, evidence must be carefully handled and controlled in its life-cycle.

5.5.1.2 **Evidence Life cycle**

a. The evidence life cycle covers the evidence gathering and application process. It has the following components:

b. Discovery and recognition – Possible evidences are discovered, and discovered information is recognized as an evidence for an Incident

c. Protection – The discovered evidence should be protected at its source and location till it is recorded and collected

d. Recording - Evidence must be recorded in a logbook detailing the particular price of evidence, who found it, where it was found, when it was found.

e. Collection – Evidence is collected from the source carefully without changing the integrity of the Incident.

f. Identification (tagging and marking) – Collected evidence is tagged and marked

g. Preservation – Protect the evidence from getting damage during storage prior to court and transportation to court

h. Transportation – Transport of evidence from source to storage location and from storage location to court

i. Presentation in a court of law – Every piece collected should be presented to the court

j. Return of evidence to owner – Once the trial is over the evidence must be presented to the owner / court / law enforcement agencies.

5.5.1.3 Good sources of evidence are Telephone records, CCTV Tapes, Audit trails, System logs, System backups, Witnesses, Results of surveillance, Emails, etc.

5.5.2 **Remedial action and recovery**

5.5.2.1 Relevant member(s) of the IMT must prepare the corrective action plan for the Incident. The action plan, though specific to each case, should typically cover the following:

a. Facts and explanation/reasons for the Incident

b. Corrective action to be taken

c. Estimated cost of implementing the corrective action (if applicable)

d. Estimated time frame, start date and end date

e. Personnel responsible for taking the action

5.5.2.2 Based on the plan, relevant members of the IMT shall take action to correct and recover the systems.

5.5.3 **Corrective / Follow-up action**

5.5.3.1 After each Incident, a lessons-learned exercise must be conducted by the IMC in conjunction with relevant member(s) of the IMT and should be documented as part of a detailed Incident Report (Refer: ISMS-L4-26 Incident Report).

5.5.3.2 The Incident Report must specifically identify root cause(s) leading to the incident and required measures to prevent the incident from recurring (corrective actions).

5.5.3.3 The IMC must follow-up on corrective actions listed in the Incident Report and ensure that these are closed in a timely and satisfactory manner.

5.5.4 **Periodic reporting and trend analysis**

5.5.4.1 Members of the IMT shall review the Incidents on a monthly basis. The IMC would collate and prepare a single MIS of security incidents across locations and types and then circulate it amongst members of the IMT. The MIS must present an overview of incidents across types and severity levels. It must also present a trend analysis of security incidents over time. (Refer: ISMS-L4-32 Incident Management MIS Template).

5.5.4.2 A brief discussion on incidents must also be included as part of the agenda of periodic Information Security Forum meetings.

5.5.5 **Conference Bridge Facility in Case of Emergency**

5.5.5.1 Conference Bridge Facility has been implemented in Cogent to facilitate the decision making process in the event of an incident affecting the operations. This will also help in having clear, rapid escalation procedure of actual or potential incidents.

5.5.5.2 In the event of disaster the IMC would Dial-in and IMT members requiring latest update can dial-in and have an update on the situation.

5.5.5.3 Security Codes would be distributed to members of the IMT through emergency notification process or emails.

5.5.5.4 Conference Dial-in Number (local):

5.5.5.5 Conference Code:

6. Examples of Security Incidents

A security incident can be defined as any event that has resulted or could result in:

- The disclosure of confidential information to an unauthorized individual
- The integrity of a system or data being put at risk
- The availability of the system or information being put at risk

Examples of logical security incidents include:

- Unauthorized disclosure of sensitive information

- Extensive virus or malware outbreak and/or traffic
- Attempts (either failed or successful) to gain unauthorized access to a system or it's data
- Responding to a phishing email which results in the compromise of any Cogent user account
- Extensive disruption of Cogent information services
- Compromise of privileged accounts on computer systems
- Denial-of-service attacks on networking infrastructure and critical systems
- Attacks launched on others from within Cogent network
- Compromise of individual user accounts or desktop (single-user) systems
- Scans of Cogent systems originating from the Internet
- Spam and mail forgery that originates from, or is relayed through Cogent systems
- Viruses, Worms and Trojan Horses
- Disclosure of protected data, including paper disclosure, e-mail release or inadvertent posting of data on a web site
- Suspected information technology policy violation

Examples of physical security incidents include:

- Using another user's login id/swipe card
- Unauthorized disclosure of information
- Leaving confidential / sensitive files out
- Theft or loss of equipment that contains private or potentially sensitive information
- Theft or loss of computer media, i.e. floppy disc or memory stick
- Theft or loss of Secure ID tokens
- Writing passwords down and not locking them away
- Inadequate disposal of confidential material
- Positioning of pc screens where information could be viewed by the public
- Giving out or overhearing personally identifiable information over the telephone

7. Related Documents

7.1 ISMS-L1-A16.1: Incident Management Policy

7.2 ISMS-L4-A16.1 F1: Incident Report Form

7.3 ISMS-L4- A16.1 F2: Incident Management MIS Template