IRIS BUSINESS SERVICES LIMITED



Incident Management Policy

Version 3.7

July 2023

This document contains sensitive & confidential information, and should not be disclosed, transmitted, duplicated, used in whole or part other than for its intended purpose and intended recipients.

Document Control

Document Name	Incident Management Policy
Version Number	v3.7
Prepared By	Akshay Rane
Reviewed By	Mahesh Tilave
Date of Review	25/04/2023
Approved By	P K X Thomas
Date of Release	
Summary of Changes	Updated Annexure B

Version Control:-

Version No.	Date	Prepared by / Modified by	Overview of Changes
V1.0	17/07/2011	Varinder Kumar	First Release
V2.0	20/11/2012	Ashwini Raskar	Reviewed document with Minor changes incorporated.
V3.0	20/11/2012	Rajesh Jadhav	Reviewed document with Minor changes incorporated.
V3.1	28/09/2017	Rajesh Jadhav	Point 5 – (Incident Management Procedure Changed, Incident classification added)
V3.2	28/12/2017	Nitin Salunke	Point 4.5 - Major Incident
V3.3	02/06/2020	Sabu Ouseph	Reviewed document with Minor changes incorporated
V3.4	21/09/2021	Rajendra Patil	Updated Annexure B
V3.5	18/09/2022	P K X Thomas	Annual Review
V3.6	25/04/2023	P K X Thomas	Annual Review/Change in Annexure B – MAJOR INCIDENTS COMMITTEE: Member name changed from Sabu O To Mahesh Tilave

V3.7	06/07/2023	P K X Thomas	Annual Review/Change in Annexure B – MAJOR INCIDENTS COMMITTEE: Member name changed from Prasad Shirke To Adesh Kumar & Priyanka Devarakonda

Table of Contents

1. POLICY STATEMENT 4
2. PURPOSE 4
3. SCOPE 4
4. PROCEDURE 4
4.1 SECURITY INCIDENT CLASSIFICATION SYSTEM 5
4.2 INCIDENT CATEGORIES 6
4.3 INCIDENT SEVERITY 6
4.4 TARGET TIMES 8
4.5 SECURITY WEAKNESS 8
4.6 MAJOR INCIDENT 8
5. PROCEDURE FOR DEALING WITH INFORMATION SECURITY INCIDENTS 9
5.1 REPORTING INFORMATION SECURITY WEAKNESSES 9
5.2 ASSESSMENT AND DECISION ON INFORMATION SECURITY EVENTS 10
5.3 RESPONSE TO INFORMATION SECURITY INCIDENTS. 10
5.4 INCIDENT RESOLUTION BY MAKING CHANGE 11
5.5 COLLECTION OF EVIDENCE 11
5.6 LEARNING FROM INFORMATION SECURITY INCIDENTS 11
6. ANNEXURES: 13
ANNEXURE A – SAMPLE INFORMATION SECURITY INCIDENT REPORT 13
ANNEXURE B – MAJOR INCIDENTS COMMITTEE 15

1. Policy Statement

The aim of this policy is to ensure that IRIS information systems and data are protected from any actual or suspected security incidents. The definition of an incident is an adverse even that has caused or has the potential to cause damage to an organizations assets, reputation and/or personnel. Incident management in IT is concerned with intrusion, compromise and misuse of information and information resources, and the continuity of critical information systems and processes. All IRIS employees, contractors and users who access IRIS equipment and information (in any format including electronic and paper records) are responsible for ensuring the safety and security of the IRIS systems and the information that they use or manipulate.

2. Purpose

This policy serves to minimize the negative consequences of incidents and to improve organization ability to promptly restore operations affected by such incidents. The policy also strives to ensure incidents are promptly reported to the appropriate authorities, that they are consistently and expertly responded to, and that significant incidents are properly monitored and mitigated.

3. Scope

This policy applies to all users of the IRIS facilities and equipment including staff and any third party suppliers and contractors. All users have a role to play and a contribution to make to the safe and secure use of technology and the information that it holds.

4. Procedure

Reporting of Security Events

- IT related incidents – ITSS & ISD
- Non-IT related incidents – HR & Admin

Employees can report incidents in one of the following two ways.

- Ticketing system through open project

- Send an e-mail to itsupport@irisbusiness.com

4.1 Security Incident Classification System

Security incidents will be classified according to incident categories and severity of incident in order to determine the appropriate response.

4.2 Incident Categories

An information security incident can happen for a number of reasons:

Violation of IS policy	System Crash
Criminal activity/investigation	Internet access misuse
Pornography	Email access misuse
Denial of Service	Single or distributed (DoS or DDoS)
Malicious code activity	Worm, virus, Trojan
Violation of code of conduct	Unauthorized monitoring
Phishing, Spamming	Unauthorized access
Inappropriate post to Internet	Redirected web site
Computer security intrusion	Compromised user account
Disruption to critical services	Social engineering

Some examples of Information Security incidents are as follows:

- Receiving and forwarding chain letters – including virus warnings, scam warnings and other emails which encourage the recipient to forward onto others
- Unknown people asking for information which could gain them access to council data (e.g. a password or details of a third party)
- Use of unapproved or unlicensed software within organization.
- Accessing a computer database using someone else's authorisation (e.g. someone else's user id and password)
- Writing down your password and leaving it on display / somewhere easy to find
- Printing or copying confidential information and not storing it correctly or confidentially
- Theft / loss of a hard copy file

4.3 Incident Severity

The severity of incident is a subjective measure of its impact or threat to the operation or integrity of its information. It determines the priority for handling the incident, who manages the incident, and the timing and extent of the response.

The following factors are considered in determining the severity of an incident:

- Scope of impact – how many people, departments, or systems does it affect?

- Criticality of the system or service – how important is it to the continuing operation of the organization? What would be the impact on the business, either functional or financial, if this system or service were unavailable or corrupted?

- Sensitivity of the information stored on or accessed through the system or service – does it contain confidential data, such as personal identity information or critical business information

- Probability of propagation – how likely is it that the malware or negative impact will spread or propagate to other systems, especially to other systems within organization?

Four levels of incident severity will be used to guide incident response: high, medium, low, and NA (“Not Applicable”).

High

The severity of a security incident will be considered “high” in any of the following conditions exist:

- Threatens to have a significant adverse impact on a large number of systems and/or people (for example, the entire organization is affected)
- Poses a potential large financial risk or legal liability to the University
- Threatens confidential data (for example, the compromise of a server that contains critical business information)
- Adversely impacts an system or service critical to the operation of a major portion of the organization (for example, e-mail, employee information , financial information system, human resources information system, learning management system, Internet service, or a major portion of the business network)
- Poses a significant and immediate threat to human safety, such as a death-threat to an individual or group.
- Has a high probability of propagating to many other systems within organization and causing significant damage or disruption

High severity incidents require an immediate response, focused and dedicated attention by the CTO, Delivery Head, higher Management (Directors and CEO) and other appropriate authorities until remediated.

Medium

The severity of a security incident will be considered “medium” if any of the following conditions exist:

- Adversely impacts a moderate number of systems and/or people, such as an individual department, unit, or building
- Adversely impacts a non-critical enterprise system or service
- Adversely impacts a departmental system or service, such as a departmental file server
- Disrupts a building or departmental network
- Has a moderate probability of propagating to other systems within organization and causing moderate damage or disruption

Medium severity incidents require a quick response by appropriate personnel (usually from the affected unit) who have primary responsibility for handling the incident.

Low

Low severity incidents have the following characteristics:

- impacts a very small number of systems or individuals
- Disrupts a very small number of network devices or segments
- Has little or no risk of propagation or causes only minimal disruption or damage in

their attempt to propagate

Since a single compromised system can “wake up” and negatively affect other systems at any time, appropriate personal (usually the technical support staff responsible for the system) must respond as quickly as soon possible as.

4.4 Target Times

Following are the current targets for response and resolution for incidents based upon priority.

Target Priority	Response	Resolution
Low	24 hours	7 days*
Medium	2 hours	4 hours
High	15 minutes	2 hours

4.5 Security Weakness

Weakness of an asset (resource) or a group of assets that can be exploited by one or more threats these shall be reported without any delay to be of any real use. Users should not, however, attempt to prove any security weakness.

Examples include:

Security weakness observed in a particular software / hardware being used in the organization.

- Network Security weakness.
- Security weakness observed in a practice / procedure / standard.
- Software Malfunctions:
- Apart from security incidents, day to day software malfunctions should be reported to the IT Help Desk

4.6 Major Incident

- Major incidents should be recorded in the ticketing system (Open Project) as problem record.
- Objective is to restore the service as quickly as possible(Permanent Resolution Or Temporary work around)
- If the incident is categorized as a major incident, the members defined in Annexure B needs to be contacted.

- The incident should be thoroughly investigated and a proper action plan for the resolution of the incident should be prepared.
- Major Resolution Incident Status should be communicated to the stake holder.at regular interval along with final closure sign off. All major incident should be reviewed half yearly.
- Root Cause Analysis of the entire major incident should be prepared and documented to avoid reoccurrence of the incident.

5. Procedure for Dealing with Information Security Incidents

Sr. No.	Activity	Responsible
1	Report / Notify any information security event in systems or services to IT Infra team. Security Incidents may be reported through telephone calls, voice mails, visit's, letters or e-mails.	Incident Notifier
2	Verify the notification to determine if it is a valid security incident or not. In case of invalid security incidents, inform the incident notifier.	IT Infra Team
3	For valid security incidents, provide confirmation to the notifying process/ incident notifier.	IT Infra Team

5.1 Reporting information security weaknesses

Sr. No.	Activity	Responsible
1	Report / Notify any information security event in systems or services to IT Infra team. Security Incidents may be reported through telephone calls, voice mails, visit's, letters or e-mails.	Incident Notifier
2	Verify the notification to determine if it is a valid security incident or not. In case of invalid security incidents, inform the incident notifier.	IT Infra Team

3	For valid security incidents, provide confirmation to the notifying process/ incident notifier.	IT Infra Team

5.2 Assessment and decision on information security events

Sr. No.	Activity	Responsible
1	Review all relevant information relating to the nature of the incident. Further details or clarification (if any) should be obtained from the incident notifier.	IT Head
2	Classify the security incident based upon the below defined priority criteria/guidelines. The details should be recorded in Open Projects. Multiple events may relate to one security incident. Such events should be recorded as a single security incident. Classification/Priority is as follows : 1) High Priority – High business impact 2) Medium Priority – Medium business impact 3) Low Priority – Low business impact	Requestor/ IT Infra Team

5.3 Response to information security incidents.

Sr. No.	Activity	Responsible
1	Security incidents should be responded promptly and the response should be in line with the classification of incident.	IT Infra Team

5.4 Incident resolution by making change

Sr. No.	Activity	Responsible
1	Follow change management procedure if change need to be done in any asset such as hardware, software this includes replace or upgrade, software version upgrade. Resolution of bugs is excluded in the change management procedure but the actions taken to rectify issue should be documented.	IT Infra Team Build Manager

5.5 Collection of Evidence

Sr. No.	Activity	Responsible
1	The below guideline should be followed while handling the evidences related to security incidents: ● Minimize handling of the original data to be used as evidence by duplicating / copying. ● Make copies of the original in a manner such that the original remains unchanged. ● Ensure that the original data is secured. ● Maintain record of all action steps performed as part of incident resolution.	IT Infra Team

5.6 Learning from information security incidents

Sr. No.	Activity	Responsible
1	Prepare six monthly service reports based on the data collected for the recorded security incidents. The service report should highlight the performance metrics to enable management review and should exhibit information on both the detailed status of incidents and the overall state of Security Incident Management.	IT Infra Team

2	Review the Incident Records and update the status of security incidents to the stakeholders.	IT Infra Team
3	Review learning's from the security incidents and identify actions for preventing the recurrence of similar incidents on a regular basis. Updates from Professional Associations and Security Forums should be obtained and considered in determining the preventive actions.	IT Infra Team / IT Head

6. Annexures:

Annexure A – Sample Information Security Incident Report

[To be completed & returned within 2 working days] [Complete electronically]

Report Number	

1. Notification

Reported by	Division	Phone ext	Date Reported

2. Incident Details

Type of Incident [Tick All That Apply]:	
System Related Issue	
Application Related	
Unauthorized Disclosure	
Unauthorized Access	
Equipment Loss	
Data Loss	
Breach of Policy	
Other (expand)	

Date Incident occurred	
Date Incident detected	
Incident Location	
Person(s) responsible for incident (Originator)	
Please describe the incident in as much detail as possible:	
Identify potential risks to the subject /owner of the information? E.G potential for identity theft / Phishing aid / Commercial detriment / Reputational damage	
What steps have been taken to mitigate the risks associated with the incident? For example has the information been retrieved? Has it been returned or destroyed? Has the subject/owner been informed of the incident?	
What remedial action has been taken to mitigate against future similar incidents occurring at an individual / team /organizational level?	
Identify any potential impact this incident may have on IRIS's reputation or relationship with Customer / Stakeholder.	

I confirm that the above is a complete and accurate account of the incident, information involved & potential impact:

Title	NAME	Date
Originator		
IT Manager		

Please return completed form to Information Management & Governance team ASAP but no later than 2 working days from the date of incident being reported: itsuppport@irisbusiness.com

Annexure B – MAJOR INCIDENTS COMMITTEE

Sr.no	**Name**	**Designation**
1	Deepta Rangarajan	Director
2	K.Balachandran	CFO
3	P K X Thomas	CTO
4	Mahesh Tilave	IT Lead
5	Adesh Kumar & Priyanka Devarakonda	Product Manager- Carbon
6	Mayank Sharma	Product Manager- GST
7	Hemant Karale	Product Manager- iDeal
8	Nisha Rai	HR Head