Safex Group

Incident Management Policy

SURAS
01/04/23

Safex Group

Incident Management Policy

1. Document Control

S. No.	Type of Information	Document Data
1.	Document Title	Incident Management Policy
2.	Document Code	ITIMP01
3.	Date of Release	01-04-2023
4.	Document Version No.	1.0
5.	Document Owner	Safex Group
6.	Document Author(s)	Suresh Yadav (AVP. IT)
7.	Document Approver	Piyush Jindal (Group Director)

Document Update Summary

Version No.	Revision Date	Nature of Changes	Date Approval
1	-		
2			
3			

Suresh
01/04/23

2. Purpose

Information Security Incident is any violation or imminent threat of violation of information security policies, standards, procedures or practices or any information security event that may compromise operations or threaten the security of an information system or business process inside Safex Group. Incident management is concerned with intrusion, compromise and misuse of information and information resources, and the continuity of critical information systems and processes.

Implementing solid security policies, blocking unnecessary access to networks and computers, improving user security awareness, and early detection and mitigation of security incidents, are some of the actions that can be taken to reduce the risk and drive down the cost of security incidents.

3. Terms & Definition

Information System	Asset/Systems in the context of this policy includes all allied assets including but not limited to: a) Computer equipment, e.g., servers, desktop, laptops, mobile phones, tablets, printers. b) Storage Media, e.g., hard drives, USB storage devices, network attached storage. c) Connectivity including network infrastructure, e.g., routers, firewall, telecommunications (landline and mobile networks). d) Software and related services including but not limited to on premise and cloud services. Data resident or processed on such information systems.
Information Media	Any device being used to store, process, or transmit Safex Group or client data and/or information.
Information	Data that is (1) accurate and timely, (2) specific and organized for a purpose, (3) presented within a context that gives it meaning and relevance, and (4) can lead to an increase in understanding and decrease in uncertainty or formation of an informed opinion.
Information security event	An identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant.
Information security incident	A single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security

Abbreviation

HR	Human Resources
SPOC	Single Point of Contact
CIO	Chief Information Officer
SIRT	Security Incident Response Team

4. Scope

This policy is applicable across all Safex Group facilities for all employees, contractors and third parties working with Safex Group information and/or information systems.

5. Objective

This policy aims to mitigate the following risks:

a. To reduce the impact of information security breaches by ensuring incidents are followed up correctly.

b. To help identify areas for improvement to decrease the risk and impact of future incidents.

6. Roles and Responsibilities

User	a) Report security incidents to SIRT b) Report any weakness observed in the system, which could lead to data leakage. c) Facilitate SIRT investigations by providing correct and complete inputs and evidence as requested
IT	d) Initiate the investigation of the reported information security incidents. e) Initiate an investigation based on the category of the known or suspected security incident. f) Prepare corrective action plan. g) Initiate disciplinary actions. h) Record all incidents and maintain evidence. i) Prepare and share the root cause analysis. j) Conduct analysis of all the records to identify concern areas. k) Perform periodic review of SIRT process and database. l) Monitor SIRT operations

Security Incident Response Team (SIRT)	m) Dedicated team responsible for addressing information security incidents. n) Review and track the flow and closure of incidents raised. o) Facilitate the investigation of the incident. p) Assist in implementation of corrective and disciplinary actions. q) The team shall respond to the security event identified as per the defined steps in the proceeding document.
Management review	r) Review performance and concern areas identified by the SIRT.
Admin	s) Maintain contacts with relevant authorities (law enforcement fire departments etc.) and initiate communication with them when necessary.
Legal	t) Providing a communication channel between Safex Group and law enforcement authorities and regulatory bodies u) Initiate any legal action required as per corrective or v) disciplinary process requirement
HR	w) Aid in investigation of incidents x) Initiate disciplinary action against the violator as per severity of incident/violation

7. Roles and Responsibilities of SIRT

Designation	Responsibilities	Authorities
AVP IT	a) Decide on the disciplinary actions (if required) to be taken for habitual incident creators / repeated breaches of information security. b) Review of security incidents status with Asst. Manager IT or as per the seriousness of open major / critical incidents whichever earlier.	a) Approve this procedure. b) Provide resources required for incident resolution.
Sr. Manager IT	a) Review this procedure and provide useful comments if any. b) Provide guidance on information security for the appropriate management of security incidents.	Edit this procedure.
Asst. Manager IT	a) Ensure the Incident Management Procedure is latest updated and complied with by all in the team. b) Overall responsibility of handling & resolving incidents. c) Analyze incidents with the IT Team. d) Take appropriate corrections & corrective actions to ensure the risk of occurrence of	a) The critical incidents that have an immediate and severe impact on the Safex Group business should be escalated to Group Director within one hour of the IT Team's

	such incidents is minimized.	cognizance of the incident. b) Incident Log and its sharing with team members.
Safex Group team members/ Assistant Manager IT	Help analyze the incidents and Weakness alerts and work closely to resolve the issue or to take the appropriate correction / corrective actions.	
All Safex Group personnel	It is the responsibility of Safex Group personnel not to be involved in committing security breaches or attempting to prove the suspected security incidents.	Report the information security incidents and Weakness alerts to IT Team.

8. Policy

The Information security incident management policy has been established to ensure that Safex Group reacts appropriately to any actual or suspected incidents relating to information systems and information. The policy ensures standard process is followed for reporting, recording, and resolving information security incidents and weakness within Safex Group. The learning from these incidents shall be captured and the evidence maintained for audit purpose.

a) An incident can be the result of unusual circumstances and/or violations of existing policies and procedures of Safex Group Systems. An incident may relate, but not limit to, to any of the following:
   I. Loss or theft of data, information, or information assets.
   II. Transfer of data or information to those who are not entitled to receive that information.
   III. Attempts (either failed or successful) to gain unauthorized access to data or information storage or a computer system.
   IV. Changes to information or data or system hardware, firmware, or software characteristics without the Council's knowledge, instruction, or consent.
   V. Unwanted disruption or denial of service to a system.
   VI. Unauthorized use of a system for the processing or storage of data by any person.
   VII. Loss of information due to unknown reasons (in hard or soft form).
   VIII. Virus incidents regarding e-mail, Internet and others.
   IX. Failure / crash of IT equipment.
   X. Power problems and loss of data.
   XI. Natural calamity or disaster.
   XII. Hardware, Software, and Operational errors that result in erroneous data.
   XIII. Unauthorized Physical Access to Safex Group Systems premises.
   XIV. Data loss or leakage of personal information, Data privacy.

b) All employees, contractors and third-party users of Safex Group information, information systems

and/or services shall be reported.

I. Any observed or suspected security weaknesses in the systems through Lifnr Bug Tracker application. The same can be reported via email to AVP IT as well.

II. A quarterly awareness session shall be held for reporting any observed and suspected security incident.

c) The reporter shall under no circumstance attempt to prove suspected security weakness by violating or testing it. Testing weaknesses shall be interpreted as a potential misuse of the system as it can cause damage to the information system or service and shall result in legal liability for the individual performing the testing.

d) Management shall appoint a SPOC from the IT (Assistant Manager IT) for management of information security incidents and database.

e) The SIRT alias shall also consist of the following:

I. HR representative
II. Legal team representative
III. Admin team representative
IV. IT representative

f) IT shall ensure timely root cause analysis (investigation), corrective and disciplinary actions implementation to minimize the damage to Safex Group information and information assets.

g) IT shall delegate the corrective action implementation to the concerned person/team for resolution of the incident and minimizing the damage. Respective person/team shall update IT for formal closure of the incidents in records.

h) Disciplinary action shall be initiated against an employee, contractor and/or third-party user in the following cases:

I. He/she is identified to have violated any Safex Group information security policy.
II. He/she is found involved in an act which jeopardizes the security of Safex Group information assets.
III. His/her credentials, email ID or system is identified as the source of violation or Information security breach.

i) Learning from incidents shall be captured in a centralized database by the IT team and shall be reviewed periodically.

j) The information gained from the evaluation of information security incidents shall be used to identify recurring or high impact incidents. This information shall be accessed by only authorized employees.

k) The logs, audit trails and similar evidence shall be collected and secured, as appropriate for:

I. Internal problem analysis
II. Use as an evidence in relation to a potential breach of contract, breach of regulatory requirement or in the event of civil or criminal proceedings e.g., under computer misuse or data protection legislation.
III. Negotiating for compensation from software and service providers

l) Evidence shall be collected, retained, and presented where a follow-up action against a person or organization after an information security incident involves disciplinary or legal action (either civil or criminal).

m) The contact lists for law and enforcement authorities, regulatory bodies, and fire brigade, information

and telecommunication service providers shall be readily available with SIRT Team. Legal department shall provide the communication channel between Safex Group systems and law enforcement authorities & regulatory bodies.

Contact List:

	Function	Name	e-mail id	Phone
Control s	**Online Portal, SAP Server Host**		esupport@ctrls.in	
PoweBi		**Anuj**	anuj.agarwal.ak@gmail.com	9711126440
Computer Peripherals	**Laptop Requirements**	**Sagar**	khuranasumit1986@gmail.com	9910894566, 9910895566
	Laptop and Repair	**Rohan Jain**	jainrohan@gmail.com	9812706910
Airtel	**Contact & Internet**	**Umesh**	umeshprajapat@gmail.com	9873235415
Tata	**Internet & PRI**	**Nisha Saxena**	Nisha.Saxena@tatatel.co.in	9250001171
Simplifii	**TA/DA Automation App with Inventory, tracking, Sales-Collection report, MDA Addition & Payment, HQ APP, Attendence Operations,**	**Munish**	munish@simplifii.com	9873778077
Spectra	**Online SAP Connectivity, Power bi Server and Domain Level Issues**	**Harbir**	hg@spectracloud.com	9212000234

n) The IT team shall conduct a monthly incident analysis and share it with the SIRT team.
o) The IT team shall continuously monitor the SIRT operations and reported incidents.
p) The punitive action will be decided on a case-to-case basis depending on the nature, gravity, occurrence, severity of violation / breach and its impact on the business.
q) Breaches or violations to Safex Group Systems Information Security policies shall be categorized into three levels.
   I. Low Severity
   II. Medium Severity

III. High Severity

r) Guidelines for classification of security violation

I. The below table lists common information security breaches / violations and its severity level.

S.no.	Severity Category	Possible Punitive Action	Remarks
1.	HIGH	Suspension of Service / Termination of Employment / Cancellation of Contract / Severe Warning.	
2.	MEDIUM	Counseling / Severe Warning/ Performance diary entry by manager and performance pay cut for not less than 1 month. Confiscate laptop and removal of admin rights	For installing unauthorized software laptop will be confiscated along with the admin rights removal
3.	LOW	Warning / Counseling/admin rights removal in case of software non- compliance.	For installing unauthorized software, admin rights will be removed.
4.	Counseling	Discussion with user	-

II. The Business Code of Conduct of Safex Group Systems (applicable to all matters concerning general conduct, performance and disciplinary control of employees, trainees, Associates) shall be referred while taking decision for punitive action.

III. The record of violations and the punitive action taken shall be maintained and updated by HR team in the employee personnel file.

s) Cloud Services

I. Safex Group will request information from the Cloud Service Provider ('CSP') about the mechanisms for: reporting, detection and tracking of security incidents.

II. Procedures will be agreed with CSP to respond to requests for potential digital evidence or other information from within the cloud computing environment.

9. Enforcement

Policy violations

- Violation of the Policy will result in corrective action from the management. Disciplinary action will be initiated consistent with the severity of the incident as determined by the investigation, and may include, but not limited to:

a. Loss of access privileges to information assets

b. Termination of employment or contract

c. Other actions deemed appropriate by Management

- Violation of the policy shall be reported to the IT Head.

10. Document Reference

Document/ Form No.	Title

SURESH
01/04/23