Information Security Incident Management Policy

DOCUMENT SUMMARY:

AUTHOR	INFORMATION SECURITY MANAGER
REVIEWED BY	CIO/CISO
CURRENT VERSION	2.1
DATE OF CURRENT VERSION	04-03-2016
DATE OF ORIGINAL VERSION	30-11-2013
DOCUMENT REFERENCE NO.	SFO-ISMS-POL-003
DOCUMENT TYPE	POLICY
DOCUMENT STATUS	FINAL
DOCUMENT CIRCULATION	NEED BASED CIRCULATION ONLY
OWNER	INFORMATION SECURITY MANAGER
APPROVED BY	MANAGING DIRECTOR

DOCUMENT AMENDMENT RECORD

CHANGE NO.	DATE	PREPARED BY	BRIEF EXPLANATION
0.1	30-11-2018	Information Security Manager	Draft Version
1.0	15-12-2019	Information Security Manager	Version 1.0
1.1	10-07-2020	Information Security Manager	Version 1.1

TABLE OF CONTENTS

1 Introduction

The Incident Management policy helps SFO to develop, communicate and implement formal methods and procedures for detecting and reporting incidents relating to exceptional situations in day-to-day administration of IT and information security related areas. It shall be ensured that the incidents are reported in time to the appropriate authorities and corrective actions are taken immediately to avoid the recurrence of such events in future.

1.1 Policy Statement

"All Incidents and suspected actions must be reported without any delay to the Incident coordinator to speed the identification of any damage caused, any restoration, and repair and to facilitate the gathering of any associated evidence."

There shall be an implemented procedure and other controls capable of enabling prompt detection of security events and response to security incidents to execute, monitor and review the following

1) Promptly detect errors in the results of processing

2) Promptly identify attempted and successful security breaches and incidents

3) Enable management to determine whether the security activities delegated to people or implemented by information technology are performing as expected

4) Help detect security events and thereby prevent security incidents by the use of indicators

5) Determine whether the actions taken to resolve a breach of security were effective.

2 What is 'Information Security Incident'?

'Information security Incident' is a term related to exceptional situations or a situation that warrants intervention of specialist help or senior management. An incident is detected in day-to-day operations and management of the IT function. This may be result of unusual circumstances as well as the violations of existing policies and procedures of the company. An incident may relate to any of the following:

- Malfunctions of software and hardware
- Virus incidents regarding e-mail, Internet, USB, CD, diskette and other media
- Malware, Ramsomware , similar attacks
- Power problems
- Natural calamity or disaster
- Loss of service, equipment or facilities
- System malfunctions or overloads
- Human errors
- Non-compliance issues with policies or procedures

- Breaches of physical security arrangements
- Uncontrolled system changes
- Access violations
- Suspected hacking attempts
- Successful hacking attempts
- Hardware resources and components lost / stolen

3 Reporting Information Security Events

An information security event may be detected by anybody in the organization. The concerned personnel shall immediately bring it to the notice of the Incident coordinator within IT Security either by logging information security event to Incident module in IT-Helpdesk tool and also intimate it to their Line Managers concerned. The Incident coordinator will allocate the responsibility of handling the incident to the concerned member of staff.

- All contractors and external parties shall also follow this policy.
- Reporting security events and weaknesses and the methodology can be explained in user awareness training programs.
- Critical and Major System alerts , event logs and messages should be auto converted into Security Incident Tickets.

4 Reporting Information Security Weaknesses

In addition to reporting security incidents, employees, contractors and third parties are also required to report security weaknesses. Employees, contractors and third parties should not attempt to prove suspected security weaknesses, in the sense users should refrain from exploiting the weaknesses found. Testing weaknesses is construed as a potential misuse of the system and could cause damage to the system & services.

5 Incident Categorization

An incident should be categorized into various severity levels. These severity levels are based on the impact to SFO and can be expressed in terms of financial impact, credibility impact, impact to sales and marketing, impact to the organization's image or impact to trust by SFO's customers.

5.1 Level One Type Incident

A small-scale response, involving one of the support services within the organization and external intervention is not required. Respective Line Manager or System Administrator is required to manage the immediate response. E.g. could be small software, hardware related problems, Human error.

5.2 Level Two Type Incident

A significant response is required by multiple services within the organization and external emergency services are also involved. E.g. Human errors, non-compliance with policies or guidelines, software & Hardware related problems which require external intervention.

5.3 Level Three Type Incident

A major community response is required, where the external emergency services assume the overall management of the incident, in conjunction with Organization services. E.g. Fire, physical security breaches.

Incident coordinator has to declare the level of the incident. It should be remembered that the level of the incidents could increase based on the time delay and when an asset that is part of a critical process has got affected. In case the Maximum Tolerable Downtime threshold is reached, then the Incident coordinator should inform the IT Team.

5.4 Incident Response prioritizing

SFO should respond effectively whenever incident occurs, in order to minimize the effect of critical incident, and to have a coordinated response. Incident coordinator should respond to the incidents based on the scale and severity that is caused by the incident. Information Security Manager should prioritize the actions to be taken during the incident. The following are the priorities that the team should consider for responding to the incident:

- **Priority one** - protection of human life and people's safety
- **Priority two** - protection of classified and/or sensitive data of systems, networks or sites. Information sharing of affected classified and/or sensitive systems, networks or sites
- **Priority three** - protection of other data, including proprietary, scientific, managerial
- **Priority four** - prevention of damage to systems (e.g., loss or alteration of system files, damage to disk drives, etc.)
- **Priority five** - minimize disruption of computing resources

6 Procedures for handling Information Security incidents

Procedures should be established to handle different types of information security incidents such as malicious code, information system failures, and application and software errors, misuse of information systems. Procedures should include root cause analysis, corrective actions, and communication to those who are affected or involved, the action taken. Refer Incident Management Procedures.

6.1 Incident Recovery Action Plan

The Incident coordinator in consultation with respective section/department manager(s) shall prepare the corrective action plan for the incident. The action plan, though specific to each case, shall typically cover the following:

- Particulars about the operating unit, location, date and time, etc
- Facts and explanation / reasons for the incident
- Other business units affected
- Corrective action to be taken
- Estimated cost of implementing the corrective action
- Estimated time frame, start date and end date
- Personnel responsible for taking the action
- Documentation of emergency action taken.

A management report about emergency action taken through an appropriate ATR (Action Taken Report).

6.1 Monitoring

All the major assets, Operations, IT Equipment, Facilities shall be reviewed and monitored by the Incident coordinator; the findings will be discussed in the Information Security Management Forum (ISMF) meeting every quarter. The magnitude and criticality of the incidents may prompt the Incident coordinator to discuss and take actions on the incidents immediately instead of at fixed intervals with Information Security Task Force. All Level 3 incidents shall be taken-up with ISMF also.

6.2 Documentation and Reporting

The Incident coordinator will analyze the impact of the incident, then prepare a detailed report and update in the database. The Incident coordinator shall maintain the central database of all such incidents. The Incident coordinator after analyzing the extent of exception and facts of the incident shall appraise the ISMF (for level 3 type incidents).

The same shall be formally documented along with relevant evidence collected or observations.

6.3 Incidences due to violation of Security Policies

Incidence arising out of violation of organizational security policies and procedures by employees shall be dealt with through a formal disciplinary process. The disciplinary actions will be as envisaged by SFO's rules and regulations as framed by HR-Manager.

7 Learning from Information Security Incidents

In addition to creating log of all incidents reported, type, volume and costs involved as a result of the incident will have to be quantified. Each procedure defined for handling different types of information security incident should cover this and the information gained from the evaluation shall be used to identify recurring or high impact incidents. Such evaluation indicates the need for enhanced or additional controls to limit the frequency, damage and cost of future occurrences.

8 Collection of Evidence

Incident coordinator must identify the cause for Incident, collect evidences and appraise its impact on SFO's Systems and data. Incident coordinator considers the following while identifying the causes of Incidents:

- Evidences for security breaches are collected if Incident causes a breach with statutory, regulatory or contractual obligations, criminal or civil law
- Evidences collected have to be evaluated according to their particular circumstances, and this may, or may not, require various departments to be involved
- Paper document evidences – keep original securely with records of who found it, where it was found and when it was found
- Electronic evidences – take backup and trace logs.
- Information on computer media – Mirror images or copies of any removable media. Information on hard disks or in memory

9 Enforcement Zone

This policy is applicable to all the incidents happening at SFO.

10 Responsibilities

The responsibility of enforcing incident management would rest with IT team.

11 Review

11.1 Scheduled, periodic review

The policy, with its supporting guidelines and procedures will be reviewed by the Incident coordinator once in a year to ensure its completeness, effectiveness and usability.

11.2 Unscheduled review

The Incident coordinator will also review and evaluate the policy in response to any changes affecting the basis of the original risk assessment such as organizational changes, technological changes, significant security incidents, new vulnerabilities, etc.

12 Disciplinary process

This policy has to be adhered to by all employees of SFO. Deliberate breach or circumvention of the principles of this policy, or of the guidelines and procedures that implement it, will lead to appropriate disciplinary action.

13 Recommendations and guidelines

Follow the Information Security Incident Management Procedure document.

14 ISO 27001 References

- A.16.1.1 Responsibilities and procedures
- A.16.1.2 Reporting information security events
- A.16.1.3 Reporting information security weaknesses
- A.16.1.5 Response to information security incidents
- A.16.1.7 Collection of evidence