IT Security

Incident Response Procedure

DOCUMENT SUMMARY:

AUTHOR	INFORMATION SECURITY MANAGER
REVIEWED BY	CIO/CISO
CURRENT VERSION	1.2
DATE OF CURRENT VERSION	10-07-2020
DATE OF ORIGINAL VERSION	30-11-2018
DOCUMENT REFERENCE NO.	SFO-ISMS-POL-004
DOCUMENT TYPE	POLICY
DOCUMENT STATUS	FINAL
DOCUMENT CIRCULATION	NEED BASED CIRCULATION ONLY
OWNER	INFORMATION SECURITY MANAGER
APPROVED BY	MANAGING DIRECTOR

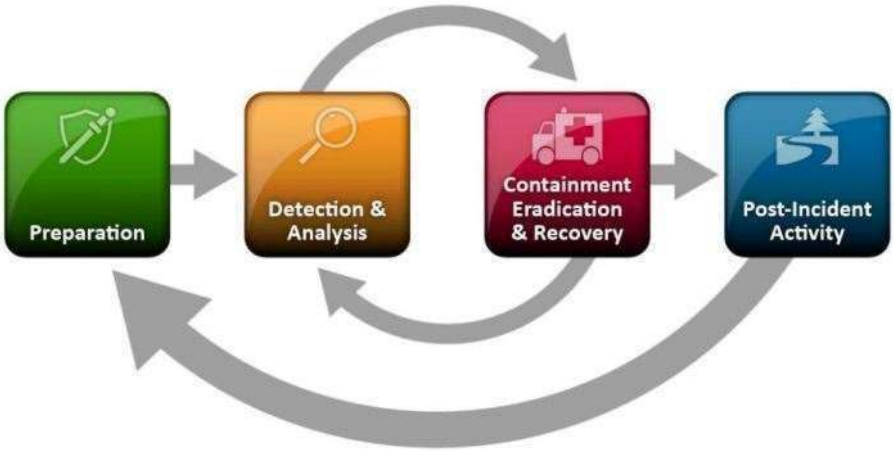
DOCUMENT AMENDMENT RECORD

CHANGE NO.	DATE	PREPARED BY	BRIEF EXPLANATION
0.1	30-11-2018	IT Security Incident Response	Version 1.0
1.0	15-12-2019	IT Security Incident Response	Version 1.1
1.1	10-07-2020	IT Security Incident Response	Version 1.2

IT Security Incident Response Procedure

The Security Incident Response Process is following the NeST best practice guideline as shown in Fig 1.

Fig 1.



1.0 Detect and Analysis Stage

Evaluate severity level. Any security incident involving an information system used to store, transmit or process SFO High Sensitive, Confidential/Personal or Open/ Non sensitive Data (Data classification as per the Data Classification and Data Protection Policy) or a security incident that results in degraded performance of a SFO IT asset, which represents more than a minor impact on operations , is considered a high-severity incident. Highseverity incidents should be reported immediately.

Typical ways of determining when there is an issue include but not limited to:

- Alerts from security monitoring tools, malfunctions within the systems, unusual behaviours, unexpected or unusual file modifications, copying, downloads etc.
- Reporting by users, network or system admins, security personnel, or external thirdparty partners or customers.
- Audit logs with signs of unusual user or systems behaviour, such as multiple failed login attempts, large file downloads high memory usage, and other anomalies.

1.1 Report high-severity incidents to the SFO Information Security Office by sending email to itsecurity@nestgroup.net. Include a brief description of the incident and who should be contacted for more information. See "How to Report a Security Incident" below for specific contact details.

2.0 Containment, threat elimination, and recovery

Protect the evidence

2.1 Do not access (logon) or alter the affected IT asset

2.2 Do not power off or logoff the affected IT asset

2.3 Unplug the network cable from the affected IT asset, network port or wall-jack

2.4 Physically label the IT asset, directing others to not touch or use the IT asset

2.5 Document the following; provide as much specificity as possible:

2.5.a When and how the incident was detected?

2.5.b What actions have been taken so far? Include the date/time, location, person(s) involved and actions taken for each step.

2.5.c The type of data the affected IT asset is used to store, transmit or process

2.5.d Anticipate that the SFO IT Security Team will collect all related system or service logs and ancillary electronic evidence

2.5.e Be prepared to assist the SFO IT Security Team as they investigate the incident

2.6 All reported high-severity security events and/or incidents shall be promptly investigated and documented by the SFO IT Security Team in accordance with SFO's Information Security Incident Response Plan. The SFO IT Security Team is authorized to direct all incident response activities including, when necessary, containment and remediation tasks necessary to protect SFO's IT resources.

3.0 Conduct a post-incident review

Resolving an incident also offers lessons learned, and teams can analyse their security solution and address the weak links to prevent a similar incident in the future. Some of the improvements include deploying better security and monitoring solutions for both internal and external threats, enlightening the staff and users on security threats such as phishing, spam, malware, and others that they should avoid.

Other protective measures are running the latest and effective security tools, patching the servers, addressing all vulnerabilities on client and server computers, etc.

Definitions:

- **High Severity Incidents** - are IT security incidents, which involve a confirmed or suspected restricted data breach or have more than a minor impact on operations.
- **Restricted Data** – Any classification of data as defined in SFO's Data Classification and Data Protection Policy.