

Table of Contents

1. Purpose	4
2. Compliance Table	4
3. Incident Response Team Compositions	4
3.1 24x7 Availability of IR Team Members	5
3.2 Purpose Response Plans	5
3.3 Confidential Data Exposure	5
3.4 Criminal Activity/Investigation	6
3.5 Denial of Service	7
3.6 Malicious Code Activity	7
3.7 Policy Violation	8
3.8 Reconnaissance Activity	8
3.9 Unauthorized Access	9
3.10 Un-Patched Vulnerability	9
3.11 Un-Authorized Network Access	9
4. Data Backup Strategy	10
5. Contact List	10
6. Incident Response Time	10
7. Security Incident Classification	11
8. Learnings	12
9. IR Plan Review and Modification Process	13
10. Periodic Training	13
11. Problem Management	14
11.1 Scope	14
11.2 Roles and Responsibilities	14
11.3 Problem Identification and Escalation Procedures	14
11.4 Audit and Compliance	14

12. Fraud Management	14
12.1 Objectives	14
12.2 Prevention and Reporting	15

DOCUMENT CONTROL

VERSION CONTROL

Document Control ID	EFR-Incident Management Plan-050
Issued Date	
Effective Date	
Owner	Information Security & Compliance Department

REVISION TABLE

Date	Version	Brief Description	Author

RELEASE AUTHORIZATION

Task	Author	Title	Date

REVIEWER AUTHORIZATION

Task	Author	Title	Date

APPROVAL AUTHORIZATION

Name	Title	Signature	Date

Important Note: This document is intended solely for the use of the individual or entity to whom it is transmitted to and others authorized to receive it. It may contain confidential or legally privileged information. If you are not the intended recipient you are hereby notified that any disclosure, copying, distribution or taking any action in reliance on the contents of this document is strictly prohibited and may be unlawful. If you have received this document in error, please notify us immediately.

1. Purpose

This document outlines the incident response plan for dealing with any incidents as per the Incident Management Policy document. All classifications of incidents and response best practices have been outlined in the policy document. This document acts as an incident response plan outlining the actual process of dealing with any incidents.

2. Compliance Table

Policy/Procedure Name	ISO 27001:2022 Control	UAE IA Control Policy/Procedure	UAE IA Control Number	Requirements
Incident Management Plan	A5.24, A5.25, A5.26, A5.27	Incident Response Plan, Classification, Training, Testing, Assistance & Learning	T8.2.1, T8.2.3, T8.2.4, T8.2.5, T8.2.6, T8.2.7, T8.2.8	NIST SP800-144 Guidelines

3. Incident Response Team Compositions

Note: Contact info of all these is in a separate matrix at the end of the document.

Team	Responsibilities	Members
Alert Monitoring Team (AMT)	Monitoring the alerts.	
Technical Operations Team (TechOps)	- Monitoring system components. - Identifying and logging the incident. - Escalating to the next level. - Taking immediate containment actions. - Working with other teams for restoration & eradication.	
Technical Assessment Team (TAT)	- Does a deeper analysis of the issue. - Confirms category and severity level. - Comes up with detailed plan to contain, eradicate and restore. - Escalating to the next level if required. - Ensuring a follow-up plan to prevent such incidents. - Signs off on the eradication & restoration.	
Information Security Team	- Acts as Incident Co-Ordinator. - Monitors the incident response. - Responsible for contacting external parties (acquirers). - Acts as a point of contact for forensic	

Team	Responsibilities	Members
	investigations, initiates forensic processes. Gets fresh scans, VAPT, etc. done to ensure the fix is proper.	
Executive Management (EM)	- Provide leadership during incident response. - Approves forensic investigation. - Work with law enforcement agencies for initial complaint logging. - Work with card associations, acquiring banks.	

3.1 24x7 Availability of IR Team Members

- IR Team members must acknowledge that they can be reached at any time of the day including nights.
- The team members must provide their contacts and alternate contacts to the monitoring team.
- Any travel plans are intimated in advance and a backup IR member is identified.
- Any Security-related incidents should be reported to the bank's Information Security team by IR team members.

3.2 Purpose Response Plans

Cyber Security Incidents are to be treated and reported based on the applicable legal and regulatory reporting requirements. Cyber Security Incidents must be reported immediately to the Stakeholders.

The Categories of Cyber Security Incidents to be reported to the stakeholders as defined in the section Contact List are given below but are not limited to:

- Denial of Service (DOS)
- Distributed Denial of Service (DDOS)
- Virus/Worm/Trojan/Malware
- Intrusion/Hack/Unauthorized access
- Website Defacement
- Misuse of Systems/Inappropriate usage
- APT/0-day attack
- Spear phishing/Whaling/Phishing/Wishing/Social engineering attack

3.3 Confidential Data Exposure

Any security incident should be reported to

Tech Ops:

- Immediately disconnect affected device(s) from the network.
- Call up Information Security team, call TAT.
- Immediately initiate scans in other devices to see if others are affected.
- If there is a threat of it spreading or existing in other devices, disconnect the full processing infra from firewall.
- Give all data, logs, alerts etc. to TAT for analysis. Conduct your own analysis.
- Plan for bringing up another clean instance to prevent service disruption. Never use any builds or files from infected device.

TAT:

- Review all data, logs, alerts, etc. from Tech Ops and do a thorough investigation.
- Plan for bringing up another clean instance with Tech Ops to prevent service disruption. Never use any builds or files from the infected device.
- Periodically update higher levels.
- Come up with a plan to prevent future incidents.

Information Security:

- Review the extent of damage and check if fraud has already been committed.
- Contact higher levels.
- Work with EM to immediately contact Forensic companies to initiate a forensic investigation.
- Provide leadership and ensure best practices are adhered to.
- Once eradication is done, ensure it is tested by initiating VAPT, scans, etc.

EM:

- Provide leadership and ensure best practices are adhered to.
- Sign off on a forensic investigation.
- Contact Cyber Cell and lodge a complaint.

3.4 Criminal Activity/Investigation

Tech Ops:

- Give all data, logs, alerts, etc. to TAT for analysis or as evidence. This includes login attempts, audit trail, etc.
- Disable the culprits' credentials and associated partners if any.

TAT:

- Come up with a plan to prevent future incidents with maybe additional authentication, tracking mechanisms, etc.

Information Security:

- Review the extent of damage and check if fraud has already been committed.
- Contact higher levels.
- Provide leadership and ensure best practices are adhered to.
- Once eradication is done, ensure it is tested by initiating VAPT, scans etc.

EM:

- Provide leadership and ensure best practices are adhered to.
- Contact Cyber Cell and lodge a complaint.

3.5 Denial of Service

Tech Ops:

- Blacklist the IP addresses from where DOS attacks originate.
- Make firewalls more stringent.
- Contact DNS providers to blacklist IP, update DNS entries to other IP addresses.

Information Security:

- Contact acquirer to blacklist IP.

EM:

- Contact Cyber Cell and lodge a complaint if attacks persist.

3.6 Malicious Code Activity

AMT:

- Immediately connect with the required teams to check if alerts received for unauthorized code are valid or not.
- If not valid, immediately escalate to Information Security team and IR team.

Tech Ops:

- Immediately disconnect affected device(s) from the network.
- Immediately initiate scans in other devices to see if others are affected.

- If there is a threat of it spreading or existing in other devices, disconnect the full processing infra from the firewall.
- Give all data, logs, alerts, etc. to TAT for analysis. Conduct your own analysis.
- Plan for bringing up another clean instance to prevent service disruption. Never use any builds or files from the infected device.

TAT:

- Review all data, logs, alerts, etc. from Tech Ops and do a thorough investigation.
- Plan for bringing up another clean instance with Tech Ops to prevent service disruption. Never use any builds or files from the infected device.
- Periodically update higher levels.
- Come up with a plan to prevent future incidents.

Information Security:

- Provide leadership and ensure best practices are adhered to.
- Review the extent of damage and check if fraud has already been committed.
- Contact higher levels.
- Work with EM to immediately contact Forensic companies to initiate forensic investigation.
- Once eradication is done, ensure it is tested by initiating VAPT, scans etc.

EM:

- Provide leadership and ensure best practices are adhered to.
- Sign off on forensic investigation if required.
- Contact Cyber Cell and lodge a complaint if required.

3.7 Policy Violation

Tech Ops:

- Put in place the process outlined by TAT/ Information Security team.
- Ensure proper re-training to adhere to policies.

Information Security:

- Identify processes to prevent future policy violations.

3.8 Reconnaissance Activity

Tech Ops:

- Blacklist the IP addresses from where port scans are happening.

- Make firewalls more stringent.
- Contact DNS providers to blacklist IP, update DNS entries to other IP addresses.

Information Security:

Contact acquirer to blacklist IP at card associations.

EM:

- Contact Cyber Cell and lodge a complaint if attacks persist.

3.9 Unauthorized Access

Tech Ops:

- Review access logs.
- Blacklist user, blacklist IP, blacklist device.

Information Security:

- Decide if the violation is criminal in nature or an accident or mischief. Accordingly, take disciplinary action and conduct a fresh review of access policies.

3.10 Un-Patched Vulnerability

Tech Ops:

- Temporarily disconnect the system from the network, review it, and plan to apply the patch.
- After applying the patch ensure it is tested again for vulnerabilities.
- Open the system after checking with the Information Security team.

Information Security:

- Once the patch is done, ensure it is tested by initiating VAPT, scans, etc.
- Come up with a process to prevent such incidents from happening.

3.11 Un-Authorized Network Access

Tech Ops:

- Blacklist the IP addresses from where access is initiated.
- Make firewalls more stringent.
- Disable credentials if any of the access points.

Information Security:

- Assess if any criminal proceedings are to be initiated.
- Identify processes to prevent this from happening again.

EM:

- Contact Cyber Cell and lodge a complaint if attacks persist.

4. Data Backup Strategy

- All data required for business continuity is stored only in the DB. DB is replicated in real-time, hence, no backup process is required as part of the incident response.
- However, the log files must be backed up during each incident, to ensure the latest activities are captured to analyze and review the RCA.
- As a best practice, instead of backing up specific logs during specific types of incidents, a general strategy of backing up all the logs during all incidents is used. This ensures that no logs are missed just in case those are required at a later stage of analysis and are missed being backed up.
- The log lists to be backed up during each incident are:
 - Server OS logs- security and audit logs
 - Application logs – all modules

5. Contact List

Alert Monitoring Team (Amt)	
Network Admin (Tech Ops)	
Tat	
Associate Vice President (IS)	
Exec Management	
Client Contacts	

6. Incident Response Time

Risk	Response Time
Critical	
High	
Medium	
Low	
Info	

7. Security Incident Classification

Incident Classification	Risk	Incident Examples	Description
Abusive Content	Medium	Spam	Spam or "Unsolicited Bulk Email", this means that the recipient has not granted verifiable permission for the message to be sent and that the message is sent as part of a larger.
	Medium	Harmful Speech	Discretization or discrimination of somebody (e.g., cyber stalking, racism and threats against one or more individuals).
	Medium	Child/Sexual/Violence/	Child pornography, glorification of violence...
Malicious Code	Critical	Virus	Software that is intentionally included or inserted in a system for a harmful purpose. User interaction is normally necessary to activate the code.
	Critical	Worm	
	Critical	Trojan	
	Critical	Spyware	
	Critical	Dialer	
	Critical	Rootkit	
Information Gathering	Low	Scanning	Attacks that send requests to a system to discover weak points. This also includes some kind of testing processes to gather information about hosts, services and accounts. Examples: fingered, DNS querying, ICMP, SMTP (EXPN, RCPT, ...), port scanning.
	Low	Sniffing	Observing and recording of network traffic (wiretapping).
	Low	Social engineering	Gathering information from a human being in a non-technical way (e.g., lies, tricks, bribes, or threats).
Intrusion Attempts	High	Exploiting known vulnerabilities	An attempt to compromise a system or to disrupt any service by exploiting vulnerabilities with a standardized identifier such as CVE name (e.g., buffer overflow, backdoor, cross site scripting, etc.).
	High	Login attempts	Multiple login attempts (Guessing / cracking of passwords, brute force).
	High	New attack signature	An attempt using an unknown exploit.
Intrusions	Critical	Privileged account compromise	A successful compromise of a system or application service). This can have been caused remotely by a known or new vulnerability, an unauthorized local access. Also includes being part of a botnet.
	Critical	Unprivileged account compromise	
	Critical	Application compromise	

Incident Classification	Risk	Incident Examples	Description
	Critical	Bot	
Availability	High	DoS	By this kind of an attack a system is bombarded with so many packets that the operations are delayed or the system crashes. DoS examples are ICMP and SYN floods, Teardrop attacks and mail-bombing. DDoS often is based on DoS attacks originating from botnets, but other scenarios exist like DNS Amplification attacks. However, the availability also can be affected by local actions (destruction, disruption of power supply, etc.) – or by Act of God, spontaneous failures or human error, without malice or gross neglect being involved.
	High	DDoS	
	High	Sabotage	
	High	Outage (no malice)	
Information Content Security	High	Unauthorized access to information	Besides a local abuse of data and systems, information security can be endangered by a successful account or application compromise. Furthermore, attacks are possible that intercept and access information during transmission (wiretapping, spoofing, or hijacking). Human/configuration/software errors can also be the cause.
	High	Unauthorized modification of information	
Fraud	Critical	Unauthorized use of resources	Using resources for unauthorized purposes including profit-making ventures (E.g., the use of e-mail to participate in illegal profit chain letters or pyramid schemes).
	Critical	Copyright	Offering or Installing copies of unlicensed commercial software or other copyright-protected materials.
	Critical	Masquerade	Type of attacks in which one entity illegitimately assumes the identity of another to benefit from it.
	Critical	Phishing	Masquerading as another entity to persuade the user to reveal a private credential.
Vulnerable	High	Open for abuse	Open resolvers, world-readable printers, vulnerability apparent from Nessus, etc scans, virus signatures not up to date, etc.
Other	Medium	All incidents which do not fit in one of the given categories should be put into this class	If the number of incidents in this category increases, it is an indicator that the classification scheme must be revised.

8. Learnings

- After any incident, even if there is no breach of data or any business impact, there must be a meeting conducted to review the learnings from the incident.
- The team responsible for this activity is Information Security.

- Outline the cause of the incident, study it carefully to understand why it happened.
- Discuss the cause, the solution, and the process improvements with all teams applicable – IT, Development, service provider, QA, etc.
- Study impact on policy & processes. Conduct risk assessment.
- Update the policy document if critical, else put it down for the periodic policy updates.
- Update the process document immediately if required.
- If critical, call for a re-training of the IR team.

9. IR Plan Review and Modification Process

- Review this plan once every six months at least.
- The Information Security team is responsible for this activity.
- Prior to reviewing, make a list of all the past incidents, if any, and learnings from them.
- All previous changes to policy and processes are collected for another round of review.
- Make a list of all similar or related incidents in the industry based on subscription newsletters (Cert-In), media articles, online resources.
- Make a list of any new requirements based on ISO, UAE IA or industry best practices.
- Call a meeting of the IR team and walk through all the learnings, the articles.
- Do a quick risk assessment.
- Discuss with various stakeholders – IT team, Dev, QA etc.
- Update all related policy docs with the changes as applicable.
- Update all the related process docs with the changes as applicable.
- Ensure the IR team is trained in the new policies and procedures.
- Publish the new documents to all employees.

10. Periodic Training

- Schedule training once every six months at a minimum for the IR team and monitoring team and if required related teams (IT, Dev, etc.).
- Training can be done immediately after an incident too to rectify the processes, or at any time as seen fit by the IR team.
- The Information Security team is responsible for this activity.
- During the training, a detailed analysis of past incidents is presented and causes, and remediation measures are explained.

- Any related incidents occurring in the industry are also studied.
- The gaps leading to the incidents are identified.
- The updated process and policies are discussed.
- The IR team is made to sign an affidavit confirming they have attended and understood the training material.

11. Problem Management

- Problem Management that outlines an organization's approach to identifying, managing, and resolving problems within its IT infrastructure, services, or business processes.
- Problem management is an essential part of IT service management (ITSM) and is closely related to incident management.

11.1 Scope

- This Problem Management covers all IT services, systems, and processes provided by EFR.

11.2 Roles and Responsibilities

- Problem Manager: The Information Security team is responsible for overseeing the problem management process, ensuring problems are identified, categorized, and prioritized correctly, and coordinating resolution efforts.
- Incident Resolution Teams: The Information Security Team is responsible for investigating and resolving problems within their respective areas of expertise.

11.3 Problem Identification and Escalation Procedures

- Problems may be identified through incident reports, or other sources. All incidents should be reviewed for potential problem identification.
- Periodic audits will be conducted to ensure compliance with this Problem Management Policy.
- Clear escalation paths for problems that cannot be resolved at lower support levels will be established.

11.4 Audit and Compliance

- Periodic audits will be conducted to ensure compliance with this Problem Management Policy.

12. Fraud Management

- Fraud is defined as any intentional act or omission, whether by an employee, contractor, vendor, customer, or other party, that results in a financial or non-financial loss to EFR.
- Fraud management outlines an organization's commitment to preventing, detecting, and responding to fraudulent activities. The specific content and structure of such a policy may vary depending on the organization's size, industry, and risk profile.

12.1 Objectives

The objectives of this Fraud Management Policy are to:

- Identify and mitigate fraud risks.

- Promote a culture of fraud awareness and prevention.
- Detect and investigate potentially fraudulent activities promptly.
- Take appropriate action against individuals or entities engaged in fraudulent activities.
- Safeguard the organization's assets, reputation, and stakeholders' interests.

12.2 Prevention and Reporting

The following measures to prevent fraud:

- Conduct regular risk assessments to identify and evaluate potential fraud risks.
- Promote a culture of ethical behavior, fraud awareness, and whistleblower protection.
- Provide training and education to employees on fraud prevention and reporting.
- Implement access controls, authorization processes, and segregation of duties.
- All employees, contractors, and stakeholders are encouraged to report suspect fraudulent activities promptly.
- Reports can be made through EFR's established reporting channels.
- EFR will adhere to all applicable laws and regulations related to fraud management, including industry-specific compliance requirements.
- Fraud Management will be communicated to all employees, contractors, vendors, and stakeholders.

--End of Document--