EPIMONEY PRIVATE LIMITED (FLEXILOANS)

INCIDENT MANAGEMENT POLICY (IMP)

Document version 1.2

Document Control

Item	Description
Document Title	INCIDENT MANAGEMENT POLICY (IMP)
Document Owner	Information Security Function (ISF)
Document Code	FL-IMP-v1.2
Document Classification	Internal
Document Author	Mr. Jigar Mehta

Document Revision Record (Change History - Created / Modified / Reviewed/ Approved)

Sr.No.	Page No.	Date	Created/Modified By	Reviewed By	Approved By	Version	Nature Of Change
1	01-06	22-06-2019	Jigar Mehta	Ashish Pawar	Ashish Pawar	1.0	Initial Version
2	01-13	20-09-2024	Aditya Shelar	Ashish Pawar	Ashish Pawar	1.1	Updated Incident Log Section
3	12	03-09-2025	Aditya Shelar	Anuj Jha	Board approved	1.2	Update communication of incident section 3.9 for customers

Table of Contents

1. Purpose

The purpose of this document is to ensure quick detection of security events and weaknesses, and quick reaction and response to security incidents EPIMONEY PRIVATE LIMITED ("**FlexiLoans**" or "the **Company**")

2. Scope

This document is applied to the entire Information Security Management System (ISMS) scope, i.e. to All Personnel (On-Roll and Third-Party Personnel), Information and Information Processing Facilities and Systems within the ISMS scope, as well as to suppliers and other persons outside the Company who come into contact with systems and information within the ISMS scope.

Users of this document are all employees of FlexiLoans as well as all the above-mentioned persons.

3. Policy Statement

An information security incident is 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" (ISO/IEC 27000:2022) and impacts on the Confidentiality, Integrity or Availability of Information Asset, Information Processing Facilities and systems.

Information Security and Information Technology Functions shall maintain a process for reporting and managing security incidents. This process should cover identification and documentation of Root Cause thereby incorporating the learning and reducing the recurrence of security incidents.

3.1. Receipt of incidents, weaknesses and events

All Personnel are expected to remain vigilant for possible fraudulent activities and are responsible for reporting an Incident or event which could lead to a possible incident in the following way:

- Incidents, weaknesses and events must be reported as soon as possible by call, email or in person.
- Information Technology related Incidents must be reported to the IT Service, InfoSec Team (ISF) / Support Desk.
- Information and cybersecurity-related Incidents must be reported to the InfoSec Team / Support Desk and ISG Function.
- Information security incidents must be reported to appropriate authorities whenever this is required to comply with legal requirements or regulations.
- Suspected violations of Information Security policies shall be reported to the CISO and CTO.
- Information relating to Information Security incidents may be released to outside entities, authorities and media only after authorization from the CTO/CISO/ ISSC.
- Review Security breaches which need to be investigated shall be approved by ISSC
- The Company shall ensure that all personnel are aware of their responsibility to report information security events.
- The information security incident management procedure shall include a mechanism to proactively notify CERT-In/RBI regarding cyber security incidents.

CERT-In (Indian Computer Emergency Response Team):

- **Email for Reporting Incidents:** incident@cert-in.org.in
- **Additional Contact:** You can also visit CERT-In's website for more detailed contact information.

RBI (Reserve Bank of India):

- **Email for Reporting Cybersecurity Incidents:** cybersecuritynbfc@rbi.org.in

3.1.1. Incident Management Role Map

Process Role	Role Map
Incident Reporter	▪ All Personnel's ▪ Internal Team/External Vendor ▪ Device, Sensor etc.
Incident details Receiver	▪ IT Support ▪ Information Security Function/CTO
Assign Severity to Incident	▪ Infrastructure Team Lead ▪ Application Team Lead ▪ Business Lead ▪ Information Security Function/CTO
Initiate Security Incident Report and Incident Register	▪ Information Security Function
Complete Security Incident Report and Incident Register	▪ Infrastructure Team Lead ▪ Application Team Lead ▪ Subject Matter Expert (SME)

3.1.2. Impact of Incidents (Definition)

Security Objective	Potential Impact			
	Low	**Medium**	**High**	**Critical**
Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and	The unauthorized disclosure of information could be expected to have a very low or no impact on the company's operations, or individuals.	The unauthorized disclosure of information could be expected to have a limited adverse effect on the company's operations, assets or individuals.	The unauthorized disclosure of information could be expected to have a serious adverse effect on the company's operations, assets or individuals.	The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on the company's operations,

proprietary information.				assets or individuals.
Integrity: Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity.	The unauthorized disclosure of information could be expected to have a very low or no impact on the company's operations or individuals.	The unauthorized disclosure of information could be expected to have a limited adverse effect on the company's operations, assets or individuals.	The unauthorized disclosure of information could be expected to have a serious adverse effect on the company's operations, assets or individuals.	The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on the company's operations, assets or individuals.
Availability: Ensuring timely and reliable access to and use of information.	The disruption of access to or use of information or an information system having limited or no impact on operations, assets or individuals.	The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on the company's operations, assets or individuals.	The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on the company's operations, assets or individuals.	The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on the company's operations, assets or individuals.

3.1.3. Categories of Incidents

This section identifies different categories of Incidents,

Category	Description
Unauthorized Access	▪ When an individual or entity gains logical or physical access without permission to the company's network, system, application, data or other resource.
Improper or Inappropriate Usage	▪ When a person violates acceptable computing policies.
Suspected PII Breach	▪ If an incident involves personally identifiable information (PII) a breach is reportable by being merely suspected.
Suspected Loss of Sensitive Information	▪ An incident that involves a suspected loss of sensitive information (not PII) that occurred as a result of unauthorized access, malicious code or improper handling of data.
Targeted Scanning, Probing and	▪ Publicly available reconnaissance techniques, including web and newsgroup searches, WHOIS querying, and Domain Name System (DNS) probing, are used to

Reconnaissance of Networks and IT Infrastructure:	collect data about the structure of the target network from the Internet without scanning the network or necessarily probing it directly.
Large scale defacement and semantic attacks on websites:	▪ A website defacement is when a Defacer breaks into a web server and alters the contents of the hosted website. Attackers change the content of a web page subtly, so that the alteration is not immediately apparent. As a result, false information is disseminated
Ransomware, Malicious Code attacks (virus/worm/ /Trojans/Botnets):	▪ Malicious code or malware is software designed to infiltrate or damage a computer system without the owner's informed consent. Malicious code is hostile, intrusive, or annoying software or program code. Commonly known malware is virus, worms, trojans, spyware, adware and Bots ▪ Agencies are NOT required to report malicious logic that has been successfully quarantined by Antivirus (AV) software.
Malware affecting Mobile devices:	▪ Malicious code and malicious applications (apps) affecting operating systems/platforms used for mobile devices such as Symbian, Android, iOS, Windows Mobile, Blackberry OS.
Large scale SPAM attacks:	▪ Spamming is the abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages. SPAM mails may also contain virus, worm and other types of malicious software and are used to infect Information Technology systems.
Large scale spoofing	▪ Spoofing is an attack aimed at 'Identity theft'. Spoofing is a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage
Phishing attacks	▪ Phishing is an attack aimed at stealing the 'sensitive personal data' that can lead to committing online economic frauds. Phishers attempt to fraudulently acquire sensitive information, such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication
Social Engineering:	▪ Art of manipulating people into performing disclosure actions or divulging confidential information
Denial of Service (DoS) attacks:	▪ DoS is an attempt to make a computer resource unavailable to its intended users or successfully prevents or impairs the normal authorized functionality of networks, systems or applications by exhausting resources.
Distributed Denial of Service (DDoS) attacks:	▪ A distributed denial of service attack (DDoS) occurs when multiple compromised computer systems flood the communication link (called bandwidth) or resources of a targeted system.
Application-Level Attacks:	▪ Exploitation of inherent vulnerabilities in the code of application software such as web/mail/databases
Infrastructure attacks:	▪ Attacks such as DoS, DDoS, corruption of software and control systems such as Supervisory Control and Data Acquisition (SCADA) and Centralized /Distributed Control System (DCS), Gateways of ISPs and Data Networks, Infection of Programmable Logic Control (PLC) systems by sophisticated malware.
Compound attacks:	▪ By combining different attack methods, hackers could launch an even more destructive attack. The Compound attacks magnify the destructiveness of a physical attack by launching coordinated cyber-attack.
Server level attacks:	▪ A critical function or service offered to customer is down due to Multiple Production Server Compromises or Production Server breaches, Data Breaches.
Router level attacks:	▪ Routers are the traffic controllers of the Internet to ensure the flow of information (data packets) from source to destination. Routing disruption could lead to massive routing errors resulting in disruption of Internet communication.

Attacks on Trusted infrastructure:	▪ Trust infrastructure components such as Digital certificates and cryptographic keys are used at various levels of cyber space ranging from products, applications and networks.
High Energy Radio Frequency Attacks:	▪ Use of physical devices like Antennas to direct focused beam which can be modulated from a distance to cause RF jamming of communication systems including Wireless networks leading to attacks such as Denial of Service
Cyber Espionage and Advanced Persistent Threats:	▪ Targeted attack resulting in compromise of computer systems through social engineering techniques and specially crafted malware.
Ransomware Attack	▪ A specialized targeted attack called ransomware attack is a type of cyberattack where malicious software encrypts a victim's data, rendering it inaccessible. The attacker then demands a ransom payment in exchange for the decryption key. Failure to pay often results in permanent data loss or the public release of sensitive information.

3.2. Incident Severities/ Impact

Below are some examples of incidents for different severities and the severity level may change during the lifecycle of the incident.

Severities / impact	Role Map
Security event or weakness	▪ No incident occurred, but the event related to a system, process or may trigger the occurrence of an incident in the near or further future
Low	▪ No effect to the company's ability to provide all services to all users
Medium	▪ The incident represents attempts that may lead to an attack in the future ▪ Minimal effect and can still provide all critical services to all users but has lost efficiency. ▪ Incident which cannot significantly impact confidentiality or integrity of information, and cannot cause long-term unavailability
High	▪ An incident which can incur significant damage due to loss of confidentiality or integrity of information or may cause an interruption in the availability of information and/or processes for an unacceptable period and lost the ability to provide a critical service to a subset of system users. ▪ The incident may have limited financial impact
Critical	▪ Confidentiality, Integrity compromised for data classified as Confidential ▪ The effect of the incident could be felt for an extended period ▪ The Company is no longer able to provide critical services to any users ▪ The incident may have significant financial and / or reputation impact ▪ The incident violates RBI regulations or IT Act 2000 or Digital Data Protection Act.

3.3. Classification of incidents

All reported incidents shall be logged and classified according to specific criteria relating to the criticality of the incident.

Below are some examples of incidents for different severities and some guidelines about how to treat each class of incident. The severity level may change during the lifecycle of the incident.

Severity	Impact	Examples	Reporting Details	Response
1	Low (CCMP=NA)	• No effect to the company's ability to provide all services to all users • Individuals Virus Incidents Affecting Individuals • Network Scanning Attempts	Internal	Containment/ Clean-up/ Preventive Steps/ Damage Assessment/
2	Medium (CCMP=NA)	• Minimal effect: The Company can still provide all critical services to all users but has lost efficiency. • Server compromise (Test or Dev or Non-production) • Virus or Ransomware in non-critical systems		
3	High **(CCMP=Yes)**	• The incident represents attempts that may lead to an attack in the future • Lost the ability to provide a critical service to a subset of system users • The incident may have limited financial impact • A critical function or service offered to customer is down • Production Server breaches • Ransomware, DDoS, Web Defacement	Internal / Management / Regulatory Bodies	Assess the situation and Invoke CCMP if required Damage Assessment/ Limit Damage/ Secure Evidence/ Regulatory Requirements
4	Critical **(CCMP=Yes)**	• Multiple Production Server Compromises and the effect of incident could be for an extended period • No longer able to provide some critical services to any users • Sensitive Customer Information Stolen. • Data Confidentiality, Integrity have been compromised (Data Breaches) • The incident may have significant financial and / or reputation impact • The incident violates RBI regulations or IT Act 2000 or DPDP Act		

3.4. Treatment process for security weaknesses or events

Incidents need to be analyzed, establish the cause and, if necessary, suggest preventive and corrective action and need to be handled according to the severity of the incident

3.4.1. Treating minor incidents (Low and Medium)

If a Low and Medium severity incident were reported, the person who received the information must take the following steps:

- Must log the incident manually, electronically or automated at Incident-response@flexiloans.com
- Take measures to contain the incident

- Analyze the cause of the incident
- Take corrective actions to eliminate the cause of the incident
- Inform persons who were involved in the incident, as well as CTO about the incident treatment process

3.4.2. Treating major incidents (High and Critical)

CCMP is invoked in the case of major incidents (high and critical).

Refer to Cyber Crisis Management Plan (CCMP).

3.5. Learning from incidents

ISG Function must review all minor incidents periodically, and enter recurring ones, or those which may turn into major incidents on the next occasion, in the Incident Log.

The Chief Technology Officer (CTO) along with IS Function or CISO must analyze each incident recorded in the Incident Log (identifying type, relatedness, and cost of the incident) and, if necessary, suggest preventive or corrective action.

3.6. Disciplinary actions

The HR Function, along with the CTO/ISSC, must initiate a disciplinary process for any violation of security rules by employees, consultants, or third parties. Disciplinary committee comprising members from HR, Legal, the CTO, CISO, and ISG, will be convened to evaluate the issue. This committee will assess whether the incident was the result of an unintentional error or a deliberate action. Based on their findings, the committee will collectively decide on the appropriate response, which may include termination, warning and recording the incident in the incident register.

3.7. Guidelines for Securing, Collection of evidence and Handling Incidents

IS Function will define the rules on how to identify, collect and preserve evidence and handle the incidents that will be accepted as evidence in legal and other proceedings. A few of them are given below:

- Employees should report suspicious incidents to the command IS Team or events to the CISO.
- IS Team will assign a unique Incident ID in the incident register
- IS Team shall evaluate the information contained on Incident ID to determine the potential for loss and the risk to the Company
- IS Team assigns the incident to the Incident Response Handling Team in consultation with CISO.
- The Incident Response Handling Team shall analyze the incident evidence, develop and test hypotheses regarding the incident, develop a set of findings and conclusions, and resolve the incident.
- The Incident Response Handling Team should perform a post-incident analysis after an incident has been fully handled, and all systems are restored to a normal mode of operation.
    - Analyzing what has transpired and what was done to intervene
        - Did detection occur promptly or, if not, why not?
        - Was the incident sufficiently contained?

- Was communication adequate, or could it have been better?
- What practical difficulties were encountered?
- Was the incident caused due to negligence or malicious intent of an employee?

- Analyzing the cost of the incident
  - How much is the associated monetary cost/time?
  - How much did the incident disrupt ongoing operations?
  - Were any data irrecoverably lost, and, if so, what was the value of the data?
  - Was any hardware damaged?
- If any employee is found guilty, HR should be informed to initiate disciplinary proceedings against the employee.

- The Incident Response Handling Team should discuss actions that were taken and shall be recorded for future references
  - Workarounds and measures adopted to mitigate incidents shall be updated in the knowledge base or ticketing system.
  - Lessons learned, recommendations, and deficiencies should be presented to the Senior Management for discussion related to security planning.

- The Team should report Incidents to the respective regulator in annual filings.
- Initiate tools for capturing data for further analysis
- Capture complete details of the incident
- Capture & secure logs and screenshots of the incident
- Use tools for forensic investigation or data containment if applicable
- In the case of the data or database in question make a copy of the contents of the database
- Take a backup of the servers/application/impacted system
- Inspect and inventory components of the impacted system, Service, and Vulnerability for possible cause
- Checking connectivity with other systems and possible compromise of other systems
- Seeking and finding the source of the attack
- Breaking the connection with the source of the attacker
- Document the tracing process for future incidents
- Erase - All of the content that may be infected or impacted, this also includes formatting of PCs to contain the ransomware attack or due to rootkit type of compromise.
- Restoring databases, applications or data from clean backup in a container for inspection
- Patching and updates: Operating System, Application or Database components
- Examine the susceptibility to see any gap that still exists
- Replacing all of the components/application code/DB versions
- Build the application or restore the service in a contained environment
- Renew all user authentications for any password compromised or exposed on the Dark web
- Renew all data and backup if the data was deleted or encrypted due to ransomware.

- Mapping and closing vulnerabilities identified
- Public release/statements related to the incident
- Perform Penetration Testing in Non-Production and Production environment before the release
- Creating activity reports along with the sequence of events.
- Creation of a new knowledge base on the attack
- Document Root Cause Analysis - Records evidence -Take note of the tools used
- Making evaluations and recommendation

3.8. Incident Prevention and Precautionary Measures

Incident prevention plans will enable the Company or business process to anticipate, and withstand cyber-attacks and the capability to contain, recover rapidly and evolve to improved capabilities from any disruptive impact of cyber-attacks. The Company should employ the following plans to prevent Cyber Incidents:

- Identification of key information and technology assets that support the services of the Company.
- Implementation of controls to sustain the ability of those assets to operate under disruptive events and recover rapidly from disruption.
- Development of processes to maintain and repeatedly carry out the protection and recovery activities.
- Identification, prioritization, assessment, remediation, and protection of the Company infrastructure and key resources based on the plan for the Company's Information Infrastructure.
- Ensure compliance with global security best practices, business continuity management and cyber crisis management plan by all entities within the domain of the Company/ department, to reduce the risk of disruption and improve the security posture.

3.9. Communication of Incidents

- The Company shall communicate the information security incident details to internal and external stakeholders including vendors and board members, as applicable.
- In the event of a major security incident, as classified under Section 3.3, the Company shall notify customers of any service disruption, through available communication channels.
- The Company shall ensure that Contact details of authorities, other relevant agencies that handle the issues related to incidents is documented and updated on a periodic basis

3.10. Escalation Matrix

Criticality Level	Escalation Matrix				Timeline for Closure
	1st Level	2nd Level	3rd Level	4th Level	
Critical	Time: Immediate To: Business Functional Head and Incident SPOC	Time: > 15 mins To: Dept Head	Time: > 30 mins To: CISO	Time: > 2 hours To: CTO & CIO	3 hours

High	Time: Immediate To: Business Functional Head and Incident SPOC	Time: > 1 hour To: Dept Head	Time: > 2 hours To: CISO	Time: > 6 hours To: CTO & CIO	24 hours
Medium/low	Time: Immediate To: Business Functional Head and Incident SPOC	Time: > 36 hours To: Dept Head			60 hours

4. Managing records kept based on this document

Record name	***Storage location***	***Person responsible for storage***	***Controls for record protection***	***Retention time***
Incident Log	intranet /Shared folder	IS / IT Function	IS / IT Function has the right to edit the log	1 year
Rules for identifying, collecting and preserving evidence	intranet /Shared folder	ISG Function	IS Function has the right to edit and publish the rules	1 year

IS / IT Function can grant other employees' access to the records.

5. Appendix 1 – Incident Log

Incidents are classified into the following types:

- information related (directly related to information or communications technology)
- non-information related (all other incidents)

Information about the incidents:

1. FL-IT Incident Tracker.xls

2. FL-Non- IT Incident tracker.xls