Leapmile - Security Incident Notification Process

Effective Date: May 1, 2025

Purpose & Scope

To ensure that all significant information security incidents, including any suspected or confirmed internal or external cyber attacks, are promptly reported to the Designated Security Contact (DSC) and managed in accordance with organizational protocols. This process applies to all employees, contractors, and third parties who use or manage company IT resources, systems, or data.

Definitions

Security Incident: Any attempted or actual unauthorized access, use, disclosure, modification, or destruction of information, or interference with system operations in an information system.
DSC (Designated Security Contact): The authorized individual or team responsible for handling information security issues.
Cyber Attack: A malicious attempt to access or damage a computer system or network.

Incident Notification Process

Step 1: Identification

Any user who observes or suspects a security incident must immediately report the issue.
Incidents may include:

- Unusual system activity
- Unauthorized access attempts
- Malware infection
- Phishing attempts
- Data leakage or loss
- Denial of service (DoS) attacks

Step 2: Initial Containment

If safe and appropriate, take immediate steps to contain the incident (e.g., disconnect affected device from the network). Do not delete logs or data related to the incident.

Step 3: Notification

Notify the DSC without undue delay via:

- Email: devops@leapmile.com
- Subject: Security Incident Notification

Provide the following details (if known):

Date and time of incident discovery
Description of the incident
Systems and data potentially affected
Actions already taken

Step 4: Documentation
Submit notification to the DSC. Maintain a record of all actions taken in response to the incident by emailing details of actions taken to the DSC email address.

Step 5: Escalation
The DSC will evaluate the incident severity and determine if escalation to executive management, legal, or external authorities is necessary.

Roles and Responsibilities

Role	Responsibility
All Users	Promptly report any suspected or confirmed security incidents.
DSC	Investigate incidents, coordinate response, maintain incident records, escalate when necessary.
IT/Admin Team	Provide technical support for investigation and containment.

Review and Maintenance
This process document will be reviewed annually or after any significant security incident.