INCIDENT RESPONSE & BREACH NOTIFICATION POLICY

of

Cosmix LLP

DOCUMENT INFORMATION

Document:	INCIDENT RESPONSE & BREACH NOTIFICATION POLICY
Document Number:	COS/POL/10
Version:	1.0
Document Date:	17-06-2026
Prepared By:	HOD-IT
Reviewed By:	CISO
Approved By:	CEO
Classification Level:	Internal

Modification History

Sl. No.	Description of Change	Review Date	Version No.
1	Initial Basic Release	**17-06-2026**	1.0

Contents

1. PURPOSE

The purpose of this policy is to establish a consistent and structured approach for identifying, reporting, assessing, responding to, recovering from, and reviewing information security incidents that may affect LLP's information assets, systems, services, or business operations. The Policy seeks to minimize the impact of security incidents, ensure timely restoration of normal operations, protect organizational information, and facilitate continual improvement of the Information Security Management. It also supports compliance with applicable legal, regulatory, contractual and business requirements.

2. SCOPE

- This Policy applies to all information assets, applications, networks, cloud services, business processes, and supporting infrastructure operated or managed by LLP.
- The Policy is applicable to all Partners, employees, consultants, contractual personnel, interns, third-party service providers, and any individual authorized to access organizational information or technology resources.
- The Policy covers both information technology (IT) and non-information technology (Non-IT) incidents that may impact confidentiality, integrity, availability, regulatory compliance, business continuity or organizational reputation.

3. POLICY STATEMENT

- LLP shall ensure that every actual or suspected information security incident is promptly reported, appropriately assessed, effectively managed and documented throughout its lifecycle.
- All personnel shall immediately report any event that may compromise organizational information, systems, or business operations. Every reported incident shall be evaluated based on its impact, urgency, and associated business risk to determine the appropriate response and escalation requirements.
- The organization shall implement suitable containment, investigation, recovery, and corrective actions to minimize disruption and prevent recurrence. Records of all incidents shall be maintained to support audit requirements, regulatory compliance, root cause analysis and continual improvement.

4. INCIDENT CLASSIFICATION AND PRIORITIZATION

- Security incidents shall be categorized according to their nature, severity, urgency, and business impact. Examples include unauthorized access, malware infections, phishing attacks, ransomware, data leakage, network or system failures, cloud service disruptions, loss or theft of organizational devices, physical security breaches, privacy incidents, and violations of applicable security policies.

- Incident priority shall be determined using a combination of business impact and urgency.

Priority	Severity	Target Response	Target Resolution
P1	Critical	Immediate	Within 1 Hour*
P2	High	Within 15 Minutes	Within 4 Hours
P3	Medium	Within 1 Hour	Within 8 Business Hours
P4	Low	Within 4 Business Hours	Within 1 Business Day
P5	Minor	Within 1 Business Day	Within 5 Business Days

*Timelines are indicative and may vary depending upon incident complexity and business requirements.

5. INCIDENT REPORTING AND RESPONSE

- Every employee and authorized user shall report suspected or confirmed security incidents immediately through approved reporting channels such as the IT function, Information Security Team, reporting manager, or other designated incident reporting mechanisms.
- Reported incidents shall be acknowledged, logged, assessed, and assigned an appropriate priority. Initial assessment shall determine the nature of the incident, affected assets, business impact, urgency, and immediate containment requirements.
- The designated response team shall implement suitable containment measures, which may include isolating affected systems, disabling compromised accounts, restricting unauthorized access, blocking malicious activity, or activating business continuity procedures where necessary.
- Recovery activities shall focus on restoring affected services securely through approved procedures, validating system integrity, and ensuring that normal business operations resume with minimal disruption.

6. INVESTIGATION, EVIDENCE PRESERVATION & COMMUNICATION

- Significant incidents shall be investigated to determine the root cause, assess business impact, identify security weaknesses, and recommend corrective and preventive actions.
- Where legal, contractual, regulatory, or disciplinary proceedings may arise, relevant evidence including system logs, audit trails, emails, network records, screenshots, backup data, and other supporting information shall be collected, preserved, and protected to maintain integrity and admissibility.
- Throughout the incident lifecycle, appropriate communication shall be maintained with management, affected business units, technical teams, clients, regulators, or external service providers, as applicable. External communications regarding security incidents shall only be made by authorized personnel.

7. INCIDENT ESCALATION

Incidents shall be escalated whenever predefined response timelines cannot be achieved, business-critical services are affected, sensitive information has been compromised, specialized technical expertise is required, or significant legal, financial, operational, or reputational risks are identified.

Escalation Level	Responsible Function	Typical Trigger
Level 1	IT Support / Service Desk	Initial reporting and assessment
Level 2	Information Security Team / System Administrator	Technical investigation and containment
Level 3	Application Owner / Specialist / External Vendor	Critical or complex incidents
Level 4	Designated Partners / Senior Management	Major incidents requiring executive oversight

Management may initiate immediate escalation whenever business circumstances require urgent intervention.

8. INCIDENT CLOSURE AND CONTINUAL IMPROVEMENT

- Incidents shall be formally closed only after confirming that recovery activities have been completed, affected services have been restored, documentation has been finalized, and corrective actions have been identified.
- Major incidents shall undergo a post-incident review to evaluate the effectiveness of the response process, identify root causes, assess control weaknesses, and capture lessons learned. Recommendations arising from incident reviews shall be incorporated into organizational policies, risk assessments, security awareness programmes, technical controls, and business continuity planning to strengthen the overall security posture.

9. ROLES AND RESPONSIBILITIES

- Management shall provide oversight, allocate necessary resources, approve major response decisions, and monitor implementation of corrective actions.
- The Information Security or designated IT function shall coordinate incident response, perform investigations, preserve evidence, maintain incident records, and communicate significant incidents to management.
- Department Heads shall ensure timely reporting of incidents within their functional areas, support investigations, and implement corrective measures.
- All employees, contractors, and third parties shall immediately report suspected incidents, cooperate during investigations, safeguard organizational information, and comply with this Policy.

10. POLICY REVIEW & EXCEPTIONS

- This Policy shall be reviewed at least annually or whenever significant changes occur in business operations, technology, regulatory requirements, or information security risks.
- Compliance with this Policy is mandatory. Any violation may result in disciplinary action, suspension of access privileges, contractual remedies, legal proceedings, or other actions considered appropriate by LLP in accordance with applicable laws and organizational procedures.