Cyber-Incident Escalation Playbook

Applies to: All employees, consultants, and interns with system or data access.

1. Purpose
To preserve the confidentiality, integrity, and availability of client and firm information by defining the lawful actions to be taken in the event of an information-security or data-handling incident.

This Playbook operationalizes AWS Legal Group's duty of care under UAE law and internal compliance standards.

2. Legal Foundation
This Playbook is issued pursuant to:

- **Federal Decree-Law No. 33 of 2021 (UAE Labour Law)** Articles 16 and 44 impose employee obligations to protect employer property and information and outline dismissal grounds for breach.
- **Cabinet Resolution No. 1 of 2022 (Executive Regulations of the Labour Law)** Articles 38 to 44 govern disciplinary procedures, warnings, suspension, and termination arising from professional or security misconduct.
- **Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data** requires controllers and processors to adopt organisational and technical measures ensuring lawful handling of personal and client data.

Together these instruments establish the legal basis for AWS Legal Group's HR–IT governance and disciplinary authority.

3. Scope
Applies to all AWS Legal Group entities, subsidiaries, and remote work arrangements.

Covers all forms of information digital, printed, verbal, or visual related to clients, cases, or operations.

4. Definition of an Incident
Any act or event that compromises or could compromise the confidentiality, integrity, or availability of data, including:

- Phishing or social-engineering attempts targeting staff or clients.
- Malicious attachments masquerading as legal documents.
- Lost or stolen laptops, phones, or storage devices.
- Unauthorized access to DMS, email, or cloud accounts.
- Accidental disclosure or mis-sending of client materials.
- Modification or deletion of case records or evidence.

5. Golden Rule Report Within 15 Minutes

Uncertainty is acceptable; delay is not.

If a security event is suspected, pause work and report within 15 minutes through the official portal or alternate channels below.

6. Immediate Actions by Employee

a. **Stop activity** and close the suspicious window or email.
b. **Disconnect the device** from Wi-Fi or network cables.
c. **Preserve evidence** do not delete files or clear history.
d. **Record** key details (time, sender, filename, screenshot).
e. **Report using one of these methods:**

- **HR Portal → "Report a Security Incident"** (primary channel).
- **Email:** wecare@aws-legalgroup.com
- **Telephone:** inform Department Head or IT if systems are offline.

7. Handling Client Files and External Documents

- Open attachments only from verified sources.
- Never enable macros or open compressed files without IT confirmation.
- Store all client data solely in approved repositories (Onedrive / DMS / Legal Portal).
- Redirect clients who attempt to send materials through personal channels to secure portals.
- Report corrupted or encrypted files immediately to IT.

8. Information to Provide When Reporting

- Description of the incident
- Source (email, file, device type)
- Time of detection
- Device and location (if remote)
- Supporting screenshots or filenames

9. Roles and Responsibilities

Role	Key Responsibility
Employee	Detect → Pause → Report → Co-operate fully
IT Department	Validate and contain incident; preserve evidence; Log report
HR Department	Enforce disciplinary procedure
Department Head	Coordinate containment and operational response
Chairman / Legal Director	Approve external communications and regulatory disclosure

10. Containment and Recovery

- IT isolates affected devices and disables compromised accounts.
- Credentials are reset and MFA re-enforced firm-wide.
- Systems are restored from verified backups only.
- A clearance certificate is issued before system re-connection.

11. Communication Control

- Only IT or Management may issue statements about incidents.
- Client notifications are handled exclusively by authorized partners.
- Employees must not discuss any incident on WhatsApp, Threads, or social media.

12. Escalation Model

Detect → Pause → Report → Contain → Recover

This five-step model is displayed inside the HR Portal and reviewed during induction.

13. Post-Incident Review

Within five (5) working days of closure:

- IT issues an Incident Summary Report to Management.
- HR records disciplinary or training outcomes pursuant to Cabinet Resolution 1 of 2022 (Arts. 38 - 44).

14. Training and Accountability

- All employees must complete the annual **Security Awareness Assessment**, in accordance with preventive-training obligations under **Cabinet Resolution No. 1 of 2022, Article 11**.
- Acknowledgment is recorded in the HR file and auditable by MOHRE.
- Negligence or failure to report is subject to disciplinary action under Articles 38 - 44 of the Executive Regulations and Article 44 of the Labour Law.

15. Language and Jurisdiction

This document is issued in English; Arabic translation available upon request.

In case of discrepancy, the English version prevails.

Governed by the laws of the United Arab Emirates.