Cyber Security Incident Management Policy

Approved by the Management

This is a summary version of Probi's internal policy. This document only presents the main objectives of the policy.

Purpose:
Establishes a structured approach for handling cybersecurity incidents to minimize impact and restore operations. It defines roles, responsibilities, and response procedures for effective incident management.

Key Sections:

1. Scope:
Applies to all employees, contractors, and third-party vendors with access to Probi Group's information systems and data.

2. Incident Management:

- **Identification & Reporting:**
    - Report incidents immediately to IT Servicedesk, Incident Response Team (IRT), or supervisors.
    - IRT includes the CEO, CFO, and IT Manager.
    - Confidential reporting channels ensure no reprisal.
- **Categorization & Prioritization:**
    - IRT prioritizes incidents based on severity and impact.
- **Response Plan:**
    - Incident Response Plan (IRP) covers containment, eradication, and recovery.
    - External experts or law enforcement may be involved if needed.

3. Communication:

- IRT maintains communication with stakeholders throughout incident handling.
- Annual updates to employee contact details ensure readiness.

4. Documentation:

- Detailed records of incidents and actions are securely stored as sensitive information.

5. Policy Review:

- Annual review and updates by IRT ensure relevance and effectiveness.

6. Reporting:

- IRT reports incidents related to regulations (e.g., NIS2, DORA, GDPR) to management and authorities.

Attachments:

1. Incident Report Form:

- Captures details like incident type, actions taken, and impact assessments.

2. Checklist for Incident Response Plan:

- Outlines steps for preparation, detection, containment, eradication, recovery, and lessons learned.

Key Actions:

1. Report incidents promptly.
2. Activate Incident Response Team.
3. Follow the detailed Incident Response Plan.
4. Maintain communication and documentation.
5. Conduct post-incident reviews and updates.

This policy ensures compliance with legal standards and readiness to address cybersecurity threats effectively.