Incident Response Policies and Procedures at Blickfeld GmbH

Document revision v1.1 / 18.02.2025

Revision history

Rev.	Date	Authors	Reviewed by	Approved by
1.0	14.03.2024	R. Wojtech	W. Rosenfeld	M. Müller
1.1	18.02.2025 #55183	R. Wojtech	W. Rosenfeld	M. Müller

1. Purpose

The purpose of this document is to establish a standardized approach to managing security incidents to minimize impact and ensure the continuous protection of Blickfeld's assets, data, and reputation.

This document outlines the policies and procedures for the timely management of security incidents within Blickfeld. It ensures that all incidents are handled efficiently and effectively, in accordance with best practices and regulatory requirements. The document addresses the establishment, documentation, approval, communication, application, evaluation, and maintenance of these policies and procedures.

2. Scope

This policy applies to all employees, contractors, and third-party entities involved in the operation, support, and maintenance of Blickfeld's information systems.

3. Definitions

- **Security Event:** Any change in the normal behavior of the information system.
- **Security Incident**: Any security event that threatens the confidentiality, integrity, or availability of information or information systems.
- **Incident Response Team (IRT)**: A designated group responsible for responding to security incidents.

4. Incident Response Policy

Blickfeld is committed to:

- Promptly detecting and reporting security incidents.
- Assessing and prioritizing incidents based on impact and urgency.
- Responding to incidents in a timely and effective manner.
- Recovering from incidents to restore normal operations.
- Documenting all actions taken during incident response.
- Communicating effectively with stakeholders.
- Continuously reviewing and improving incident response processes.

5. Incident Response Procedures

5.1 Detection

- Foster a culture of awareness for suspicious behaviour.
- Implement continuous monitoring tools to detect potential security incidents.
- Regularly review logs and alerts for unusual activities.

5.2 Reporting

- Immediate reporting of suspected incidents to the Incident Response Team (IRT).
- Use the **Incident Report Form** to document and report incidents.

5.3 Assessment

- Assess the reported incident to determine its scope, severity, and impact.
- Prioritize the incident based on its criticality and urgency.

5.4 Response

- Contain the incident to prevent further damage.
- Eradicate the root cause of the incident.
- Notify affected stakeholders according to the communication plan.

5.5 Recovery

- Restore affected systems and data from clean backups.
- Verify the integrity of restored systems.

5.6 Documentation

- Maintain a detailed incident log documenting all actions taken during the response.
- Complete the **Incident Report Form** for each incident.
- Collect and store all relevant evidence (electronic evidence like logs, device status or physical evidence like devices, storage media, etc. where appropriate).

5.7 Communication

- Notify relevant stakeholders, including management, employees, and external parties, as appropriate.
- Provide regular updates during the incident response process.
- If external parties are exposed, provide a Security Advisory on https://www.blickfeld.com/resources/#security-advisories

5.8 Review and Improvement

- Conduct a post-incident review to identify lessons learned.
- Update incident response policies and procedures based on review findings.

6. Roles and Responsibilities

- **Employees and Contractors**
  - Report suspected security incidents immediately.
  - Cooperate with the IRT during incident investigations and response.
- **Incident Response Team (IRT)**
  - Lead and coordinate the incident response effort.
  - Differentiate security incidents from security events for escalation.
  - Ensure timely detection, reporting, and resolution of incidents.
- **Chief Information Security Officer (CISO)**
  - Overseeing incident response.
- **Management**
  - Provide support and resources for incident response activities.
  - Approve incident response policies and procedures.

7. Approval and Review

- The incident response policy and procedures must be approved by senior management.
- This document will be reviewed annually or after each significant incident to ensure its effectiveness.

8. Communication Plan

- Incident response policies and procedures will be communicated to all employees and contractors during onboarding and through regular training sessions.
- Updates to the policies and procedures will be communicated via email and posted on the internal intranet site.

9. Evaluation and Maintenance

- Regularly evaluate the effectiveness of the incident response processes through simulated incidents and audits.
- Maintain and update the incident response plan based on evaluation outcomes and changes in the threat landscape.