Cyber Security Overview at Blickfeld GmbH

Document revision 1.0, 17.02.2025

Revision history

Rev.	Date	Authors	Reviewed by	Approved by
1.0	17.02.2025 #55180	W. Rosenfeld	R. Wojtech	M. Müller

Introduction

In today's digitally interconnected landscape, cybersecurity has become a cornerstone of organizational resilience and operational integrity. This document outlines the comprehensive measures undertaken by Blickfeld to provide secure products and solutions, protect its digital assets and ensure business continuity.

At the heart of our approach is a robust **Information Security Management System (ISMS)**, which provides a structured framework for managing sensitive data and mitigating risks. The ISMS follows the framework set by the globally recognized standard ISO 27001:2022.

Blickfeld employs stringent **organizational measures** which foster a culture of cybersecurity awareness and accountability across all levels of the organization.

Our **Software and System Development Life Cycle (SDLC)** integrates security best practices at every stage, ensuring the delivery of secure and reliable products and solutions. Additionally, we maintain an active threat intelligence monitoring and **Common Vulnerabilities and Exposures (CVE) tracking** program, enabling us to promptly address known vulnerabilities and minimize potential exploit risks.

Recognizing the importance of preparedness, we have established a comprehensive **Incident Response Plan**, designed to facilitate rapid detection, containment, and remediation of security breaches.

This document serves as an overview of Blickfeld's cybersecurity measures, highlighting our proactive approach to safeguarding digital operations in an ever-changing threat landscape.

Organization and Information Security Management System (ISMS)

Blickfeld recognizes the critical importance of protecting its information assets in today's digital environment. To address this need, we have established an **Information Security Management System (ISMS)** following the frameworks of ISO/IEC 27001:2022 as a structured approach to managing information security risks.

At the organizational level, our ISMS is built on a set of tailored policies that define security objectives, establish key processes, and outline practical controls suited to our company's size and operations. Roles and responsibilities are clearly defined to ensure accountability and efficiency. Senior management actively supports the ISMS, dedicating resources and oversight to its implementation. The use of **segregation of duties** ensures that access to sensitive information is appropriately limited, reducing the risk of errors or misuse.

Management responsibilities include regular risk assessments, updates to security policies, and fostering a culture of security awareness among employees. These efforts are critical as we work toward the continuous improvement of our ISMS and its alignment with recognized best practices.

More details are provided in the document "**Information Security Management System**".

General Measures for ensuring Cybersecurity

To protect its information assets and ensure secure operations, Blickfeld has implemented a set of general cybersecurity measures tailored to its size and needs. These measures provide a foundational layer of security, addressing both technical and organizational aspects.

General guidelines serve as the backbone of our approach, outlining best practices for data handling, password management, and secure communication. These guidelines are accessible to all employees and are regularly reviewed to remain current with emerging threats.

A **Policy for Office and Remote Working** ensures that employees follow secure practices regardless of their location. This includes requiring secure connections for remote work via VPNs, and adherence to office access protocols. All **user endpoint devices** must comply with baseline security requirements, such as encryption, regular updates, and the use of approved security software. The **use of cryptography** is a key measure for protecting sensitive data.

We enforce strict controls on **privileged access rights**, granting administrative privileges only to those with a clear operational need. Additionally, **information access restrictions** are applied to ensure employees can only access data relevant to their roles. **Access to office rooms** where sensitive data or equipment is stored is similarly restricted to authorized personnel. Regular **backups** are conducted to safeguard critical data, with secure storage locations ensuring its availability in case of data loss or compromise.

Finally, we emphasize **training and awareness**, equipping employees with the knowledge to identify and respond to security threats. Regular workshops and updates help foster a culture of vigilance and accountability, ensuring everyone contributes to maintaining a secure environment.

Overall these measures minimize the exposure to potential Cybersecurity threats and ensure Blickfeld's **business continuity**.

More details are provided in the document **"General Measures on Cybersecurity"**.

Software and System Development

Blickfeld adopts a structured and security-focused approach to software and system development aligning with industry best practices. **Roles and responsibilities** are clearly defined within the development process to promote accountability. Developers, testers, and project managers each have specific duties to ensure security is integrated into every stage of the **Software Development Life Cycle (SDLC)**. IT-responsibles make sure all policies and guidelines are maintained and followed. Senior management provides oversight and ensures adequate resources are allocated to maintain quality and security standards.

The **SDLC** is structured to include security considerations from the planning phase through release and maintenance, helping to identify and mitigate vulnerabilities early.

We recognize the importance of using **third-party components** in our development efforts, such as open-source libraries or external APIs. To manage associated risks, all third-party components undergo rigorous evaluation for known vulnerabilities, licensing compliance, and compatibility with security requirements.

To support this framework, regular **training and awareness programs** are conducted for development teams. These programs focus on secure coding practices, awareness of emerging threats, and adherence to internal security guidelines.

More details are provided in the document **"Cyber Security Guideline for Software & System Development"**.

Common Vulnerabilities and Exposures (CVE) Tracking

A structured CVE tracking process is implemented to ensure timely identification and remediation of vulnerabilities that could pose risks to the company's operations.

The process is based upon regularly reviewing trusted sources, such as https://github.com/CVEProject/cvelistV5 for newly published CVEs. Each identified CVE is evaluated for its potential impact based on severity, exploitability, and relevance to the company's environment. Patches, updates, or configuration changes are applied to mitigate identified vulnerabilities. For critical vulnerabilities, immediate action is taken implementing temporary measures until a permanent fix is developed and applied. All identified CVEs, their assessments, and remediation actions are documented in a vulnerability management log. Relevant information is communicated to affected employees and stakeholders, while a dedicated Webpage area is maintained under https://www.blickfeld.com/resources/#security-advisories .

Incident Response

Effective management of cybersecurity incidents is essential for minimizing damage and ensuring a swift recovery. Blickfeld follows a structured approach to identify, respond to, and resolve security incidents.

A dedicated **Incident Response Team (IRT)** oversees the process through all stages starting with the detection of an incident through its assessment and resolution. Prompt communication to affected parties and thorough documentation are important components for improvement of related processes and elimination of future incidents.

More details are provided in the document **"Incident Response Policies and Procedures"**.

Security of solutions hosted at external providers

At Blickfeld, we prioritize the security and reliability of your data, which is why our dashboard and data processing platform Blickfeld Services is hosted on infrastructure certified with ISO 27001 for robust information security management and ISO 9001 for high-quality process standards. These internationally recognized certifications ensure that your data is handled with the utmost protection and operational excellence, providing a secure, compliant, and dependable environment for all your data processing needs.