SecureBlock

Information Security Policy

Secure Block d.o.o.

January 8th 2026

Contents

Revision history:

Version	***Revision Date***	***Author***	***Description***
1.0	*January 10th 2023*	*Luka Šikić*	*Initial version*
1.1	*September 13th 2023*	*Luka Šikić*	*Updates to Network Security*
1.2	*September 8th 2024*	*Mirna Novak*	*Updates to AV Policy*
1.3	*January 8th 2026*	*Mirna Novak*	*Updates to Audit and Log review*

1. Introduction

This Policy Document encompasses all aspects of security surrounding confidential company information and must be distributed and/or accessible to all Secure Block d.o.o. employees. All company employees must read this document in its entirety and sign the form confirming they have read and understand this policy fully. This document will be reviewed and updated by Management on an annual basis or when relevant to include newly developed security standards into the policy and distribute it to all employees and contracts as applicable.

At Secure Block, we are fully committed to information security – both for ourselves and for our clients. We prioritize the protection of systems, data, and communications by continuously improving our practices to stay ahead of cyber threats and build trust with those we serve.

Our vision is to create a more secure digital infrastructure by equipping penetration testing professionals with the best tools to uncover vulnerabilities and strengthen defences.

Our mission is to redefine the penetration testing process by using advanced automation and collaboration tools, enabling security teams to test more efficiently, transparently, and accessibly.
We believe that security testing should be fast, reliable, and accessible – helping organizations detect vulnerabilities in time and proactively defend against threats.

Our goal is to improve the penetration testing process, making it simpler and highly efficient.

2. Information Security Policy

Secure Block d.o.o. handles sensitive and private customer information. Sensitive Information must have adequate safeguards in place to protect them, to protect customer privacy, to ensure compliance with various regulations and to keep customers safe.
Secure Block d.o.o. commits to respecting the privacy of all its customers and to protecting any data about customers from outside parties. To this end management are committed to maintaining a secure environment in which to process sensitive and/or personal information so that we can meet these promises.
Employees handling Sensitive client data should ensure:

- Handle company and client information in a manner that fits with their sensitivity
- Limit personal use of Secure Block d.o.o. information and telecommunication systems and ensure it doesn't interfere with their job performance
- Protect sensitive client information
- Keep passwords and accounts secure
- Always leave desks clear of sensitive data and lock computer screens when unattended
- Secure Block d.o.o. reserves the right to monitor, access, review, audit, copy, store, or delete any electronic communications, equipment, systems, and network traffic for any purpose

- Information security incidents must be reported, without delay, to the individual responsible for incident response locally (director)
- Employees should not use email, internet and other Secure Block d.o.o. resources to engage in any action that is offensive, threatening, discriminatory, defamatory, slanderous, pornographic, obscene, harassing, or illegal
- Employees should not install unauthorised software or hardware, including modems and wireless access. Prior approval must be requested from management prior to establishing any new software or hardware, third party connections, etc.
- Employees should not disclose personal or other personnel information unless authorised

We each have a responsibility for ensuring our company's systems and data are protected from unauthorised access and improper use. If you are unclear about any of the policies detailed herein you should seek advice and guidance from your supervisor.

3. Acceptable Use Policy

The Management's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to the established culture of openness, trust, and integrity of Secure Block d.o.o. Management is committed to protecting the employees, partners and Secure Block d.o.o. clients from illegal or damaging actions by individuals, either knowingly or unknowingly.

Secure Block d.o.o. will maintain an approved list of technologies and devices and personnel with access to such devices as detailed in Appendix A. Employees are responsible for exercising good judgement regarding the reasonableness of personal use.

This policy applies to employees, contractors, consultants, temporaries, and other workers at Secure Block d.o.o., including all personnel affiliated with third parties.

This policy applies to all equipment that is owned or leased by Secure Block d.o.o.

- Employees should ensure that they have appropriate credentials and are authenticated for the use of technologies
- Employees should take all necessary steps to prevent unauthorised access to private and sensitive data which includes client data
- Employees should ensure that technologies are used and setup in acceptable network locations
- Employees must keep passwords secure and not share accounts
- Authorised users are responsible for the security of their passwords and accounts
- All PCs, laptops and workstations must be secured with a password-protected screensaver with the automatic activation feature
- When applicable, all POS and PIN entry devices should be appropriately protected and secured so they cannot be tampered or altered
- Postings by employees from a Company email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Secure Block d.o.o., unless posting is in the course of business duties

- End users must not be able to modify any settings or alter the antivirus or EDR (Endpoint Detection and Response) software solutions
- Email messages with attachments coming from suspicious or unknown sources should not be opened. All such e-mails and their attachments should be deleted from the mail system as well as from the trash bin. No one should forward any email, which they suspect may contain viruses. Such emails will be reported to the acting security appointee (Operational Security Authority) or the director directly
- Employees must use extreme caution when opening email attachments received from unknown senders, which may contain various malware

3.1. Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during their legitimate job responsibilities (e.g., Operational Security Authority role holder may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of Secure Block d.o.o. authorised to engage in any activity that is illegal under local, state, federal or international law while utilising Secure Block d.o.o.-owned resources.

The lists below are by no means exhaustive but attempt to provide a framework for activities which fall into the category of unacceptable use.

3.1.1 System and Network Activities

The following activities are strictly prohibited, with no exceptions:

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Secure Block d.o.o.
- Unauthorised copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Secure Block d.o.o. or the end user does not have an active licence is strictly prohibited
- Accessing data, a server, or an account for any purpose other than conducting Secure Block d.o.o. business, even if you have authorised access, is prohibited
- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
- Introduction of malicious programs into the network or server (e.g., viruses, worms, trojan horses, ransomware, etc.)
- Revealing your account password/passphrase to others or allowing use of your account by others. This includes family and other household members when work is being done at home. Desk and the area around the desk where the work is being done should be clean and should not contain any sensitive information.

- Using a Secure Block d.o.o. computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction
- Making fraudulent offers of products, items, or services originating from any Secure Block d.o.o. account
- Making statements about warranty, expressly or implied, unless it is a part of normal job duties
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorised to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, ping floods, packet spoofing, denial of service, brute-forcing accounts, and forged routing information for malicious purposes
- Port scanning or security scanning is expressly prohibited unless prior notification to the Operational Security Authority is made
- Executing any form of network monitoring which will intercept data not intended for the employee’s host, unless this activity is a part of the employee’s normal job/duty
- Circumventing user authentication or security of any host, network, or account
- Introducing honeypots, honeynets, or similar technology on the Secure Block d.o.o. network
- Interfering with or denying service to any user other than the employee’s host (for example, denial of service attack)
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user’s terminal session, by any means, locally or via the Internet/Intranet/Extranet
- Providing information about, or lists of, Secure Block d.o.o. employees to parties outside Secure Block d.o.o.

4. Policy compliance

4.1. Compliance Measurement

Director or Operational Security Authority of Secure Block d.o.o. will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, system penetration tests and feedback.

4.2. Exceptions

Any exception to the policy must be approved by the responsible personnel in advance.

4.3. Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Protection of stored data

All sensitive customer data stored and handled by Secure Block d.o.o. and its employees must be securely protected against unauthorised use at all times. Any sensitive and/or private data that is no longer required by Secure Block d.o.o. for business reasons must be discarded in a secure and irrecoverable manner.

Further instructions, procedures and processes related to sensitive personal data are available in the following internal document: Data Protection Policy.

6. Information classification

Data and media containing data must always be labelled to indicate sensitivity level.

- **Classified (Confidential)** data might include information assets for which there are legal requirements for preventing disclosure or financial penalties for disclosure, or data that would cause severe damage to Secure Block d.o.o. if disclosed or modified. Confidential data includes sensitive PII (Personal Identifiable Information) of customers.
- **Sensitive (Internal Use)** data might include information that the data owner feels should be protected to prevent unauthorised disclosure.
- **Non-Classified (Public)** data is information that may be freely disseminated.

7. Access to sensitive PII data

All access to sensitive PII should be controlled and authorised. Any Job functions that require access to private data should be clearly defined.

- Employee Access:
    - Access rights to privileged user personal data must be restricted to least privileges necessary to perform job responsibilities and/or employees that have a legitimate need to view such information
    - Privileges must be assigned to individuals based on job classification and function (Role based access control)
    - No employees should have access to confidential data unless they have a genuine business need
- Service Providers:
    - If PII is shared with a Service Provider (3rd party) then a list of such Service Providers will be maintained as detailed in Appendix B
    - Secure Block d.o.o. will ensure a written agreement that includes an acknowledgement is in place that the Service Provider will be responsible for the customers private data that the Service Provider possesses
    - Secure Block d.o.o. will ensure that there is an established process including proper due diligence in place before engaging with a Service provider

Where sensitive or personal data is used outside of its primary production context (such as in development, testing, analytics, or training environments) masking, pseudonymisation, or anonymisation techniques should be applied to reduce exposure and ensure that individuals

working in those environments are not granted unnecessary access to real personal or confidential information.

8. Physical security

Access to sensitive information in both hard and soft media format must be physically restricted to prevent unauthorised individuals from obtaining sensitive data.
Employees are responsible for exercising good judgement regarding the reasonableness of personal use.

- “Employee” refers to full-time and part-time employees, temporary employees and personnel, and consultants who are “resident” on the Secure Block d.o.o. sites
- A “visitor” is defined as a vendor, guest of an employee, service personnel, or anyone who needs to enter the premises for a short duration, usually not more than one day
- “Media” is defined as any printed or handwritten paper, USB flash drives, back-up media, computer hard drive, etc.
- Physical entrance must be locked at all times.
- Employees must ensure that they have appropriate credentials and are authenticated for the use of technologies
- Employees must take all necessary steps to prevent unauthorised access to confidential data which includes PII data
- Employees must ensure that technologies are used and setup in acceptable network locations
- Employees must keep passwords secure and not share accounts
- Authorised users are responsible for the security of their passwords and accounts
- Media containing sensitive information must be handled and distributed in a secure manner by trusted individuals
- Visitors must always be escorted by a trusted employee when in areas that hold sensitive information
- Procedures should be in place to help all personnel easily distinguish between employees and visitors, especially in areas where sensitive data is accessible
- If applicable, network jacks located in public and areas accessible to visitors must be disabled and enabled when network access is explicitly authorised
- All computers that store sensitive client data must be password protected to prevent unauthorised use

9. Protection of data in transit

All sensitive client data must be protected securely if it is to be transported physically or electronically.

- In case of collecting data from web application forms, collecting data via CSV, XML, or other appropriate table format for direct input by privileged personnel, or in case of API, HTTP(S) based transmission, applicable encryption will be used (SSL encryption, etc.)
- Databases containing PII and/or private client data are kept exclusively on the Amazon (AWS) Cloud Services internal cloud instances and are appropriately protected

- If applicable, physical transportation of media containing sensitive data to another location must be authorised by management, logged, and inventoried before leaving the premises. Only secure courier services may be used for the transportation of such media. The status of the shipment should be monitored until it has been delivered to its new location

10. Disposal of Stored Data

All data must be securely disposed of when no longer required by Secure Block d.o.o., regardless of the media or application type on which it is stored.

Online data shall be permanently deleted as described in the Operational Security Procedure document (Operational Security_Procedure_SB), when no longer required.

If applicable, hard copies of sensitive data must be manually destroyed when no longer required for valid and justifiable business reasons. A quarterly process shall be in place to confirm that all non-electronic sensitive private data has been appropriately disposed of in a timely manner. If such data exists, Secure Block d.o.o. will require that all hardcopy materials are crosscut shredded, incinerated, or pulped so they cannot be reconstructed, as a procedure for the destruction of hardcopy (paper) materials.

Secure Block d.o.o. has documented procedures for the destruction of electronic media as defined in the Operational Security Procedure (Operational Security_Procedure_SB) document. These will require:

- All sensitive and/or private data on electronic media must be rendered unrecoverable when deleted e.g., through degaussing or electronically wiped using secure deletion processes or the physical destruction of the media
- If secure wipe programs are used, the process must define the industry accepted standards followed for secure deletion
- All sensitive and/or private data on electronic media must be rendered unrecoverable when deleted from the cloud instances by disabling soft delete or applying similar measures

11. Security awareness and procedures

The policies and procedures outlined below must be incorporated into company practice to maintain a high level of security awareness. The protection of sensitive data demands regular training of all employees and contractors.

- Review handling procedures for sensitive information and hold periodic security awareness meetings to incorporate these procedures into day-to-day company practice
- Store electronically in an organisation wide accessible place for all company employees to read. It is required that all employees confirm that they understand the content of this security policy document by signing an acknowledgement form (Agreement to Comply with Information Security Policies)
- All third parties with access to PII and/or sensitive data are obligated to comply with data protection standards (GDPR)
- Company security policies must be reviewed annually and updated as needed

12. Network security

12.1. Remote Access Policy

It is the responsibility of Secure Block d.o.o. employees, contractors, vendors, and agents with remote access privileges to the Secure Block d.o.o. corporate internal AWS cloud network to ensure that their access and connection are established in accordance with best security practises.

Secure remote access must be strictly controlled. WireGuard VPN must be deployed and enabled in order to ensure secure connection to Secure Block d.o.o.. Control will be enforced by two factor authentication via one-time password authentication or public/private keys with strong pass-phrases.

Vendor accounts with access to Secure Block d.o.o. network will only be enabled during the time period the access is required and will be disabled or removed once access is no longer required. No more than 24 hours after the end of vendor engagement.

Remote access connection will be set up to be disconnected automatically after maximum of 60 minutes of inactivity.

All hosts that are connected to Secure Block d.o.o. internal AWS cloud network will be monitored on a regular basis.
Company users with a legitimate business need to connect to Secure Block d.o.o. cloud databases will do so using two factor authentication, allowing them administrative privileges. Non-company users with a legitimate business need to connect to Secure Block d.o.o. cloud interfaces for the purposes of accessing the Secure Block d.o.o. proprietary tool PentestPad will do so using two factor authentication, allowing them administrative privileges and enabling them to access the restricted view of the interface related directly to them. All Client instances hosted in the Secure Block internal AWS cloud network shall be segmented in accordance with best security practices.

All remote access accounts used by vendors or 3rd parties will be reconciled at regular interviews and the accounts will be revoked if there is no further business justification. Vendor accounts with access to Secure Block d.o.o. network will only be enabled during the time period the access is required and will be disabled or removed as soon as access is no longer required.

12.2. Wireless Communication Policy

Installation or use of any wireless device or wireless network intended to be used to connect to any of the company networks or environments is prohibited. A test shall be run twice a year to discover any wireless access points connected to the company network.

Usage of appropriate testing using tools must be periodically performed to ensure that any devices which support wireless communication remain disabled or decommissioned.

If any violation of the Wireless Policy is discovered as a result of the normal audit processes, the Operational Security Authority role holder has the authorization to stop, cease, shut down, and remove the offending device immediately.

If the need arises to use wireless technology, it should be approved by the company and the following wireless standards must be adhered to:

- Default SNMP community strings and passwords, passphrases, Encryption keys/security related vendor defaults (if applicable) should be changed immediately after the installation of the device and if anyone with knowledge of these leaves the company
- The firmware on the wireless devices has to be updated accordingly as per vendor's release schedule
- The firmware on the wireless devices must support strong encryption for authentication and transmission over wireless networks
- Any other security related wireless vendor defaults should be changed if applicable
- An Inventory of authorised access points along with a business justification must be maintained (Appendix A)

12.3. Cloud Access Policy

This policy applies to Amazon Cloud Services cloud instances used by Secure Block d.o.o.

The purpose of this policy is to define the activities associated with the provision of security for cloud-supported activities that protect Secure Block d.o.o. cloud-based information systems, networks, data, databases, and other information assets.

The scope of this cloud security policy is all information technology systems, software, databases, applications, and network resources that are implemented in cloud-based and/or managed service infrastructures needed by Secure Block d.o.o. to conduct its business.

Cloud security policy compliance is managed by the Operational Security Authority role holder. Cloud security processes must include appropriate procedures and identify staffing and technology resources to meet multiple compliance requirements.

Cloud service vendors are required to demonstrate compliance with this policies affecting Secure Block d.o.o.

As part of its due care to its customers and as a matter of good business practice, the confidentiality, integrity and availability of all IT applications, data, systems, and network resources implemented in a cloud environment at Secure Block d.o.o. AWS cloud are to be managed and continually monitored to stay aligned with best security practices. The alignment is achieved by implementing a controlled method by which access to cloud-based Secure Block d.o.o. information systems are requested and granted, security of cloud-based systems and data is monitored and analysed, violations of cloud security are addressed and mitigated, and changes to cloud security systems and procedures are requested, tested, approved, and communicated for audit and recordkeeping purposes.

- This policy addresses all Secure Block d.o.o. technology, systems, data, and networks implemented in private, hybrid and/or public cloud infrastructures, plus all other Secure Block d.o.o. IT assets implemented in cloud services

- The Operational Security Authority role holder will define cloud security processes; secure and utilise specialised software and systems to reduce the threat of cloud security breaches
- The Operational Security Authority role holder will use security related built-in controls and services in Amazon Cloud Services across identity, data, networking, and apps for easier maintenance and security overview
- A policy for data media implemented in cloud services, its creation, storage, and destruction will be established and described in detail for sensitive private data in the Data Protection Policy document
- A policy for accessing Secure Block d.o.o. systems, networks, applications, and files implemented in cloud services, both locally and remotely, including passwords and other cloud security access controls is described in the Remote access policy in this document; this policy also includes authentication of company and non-company users
- The Operational Security Authority role holder will ensure that malware (e.g., viruses, spam, phishing attacks, denial-of-service attacks, and other unauthorised access attempts) is prevented through the use of antivirus software, EDR (Endpoint Detection and Response), or other appropriate prevention and detection resources
- Cloud related security incidents are reported and managed as described in the Incident Response Policy document
- Secure Block d.o.o. shall have appropriate service level agreements (SLAs) with cloud service providers to ensure acceptable third-party cloud vendor performance, or quarterly ensure third-party cloud vendors are adequately certified and in accordance with Secure Block d.o.o. Security policy document, as well as best security practices, based on the vendors' publicly available information
- Data in use at Secure Block d.o.o. cloud, whether at rest or in motion, within any approved cloud environment, will be encrypted

13. System and Password Policy

All users, including contractors and vendors with access to Secure Block d.o.o. systems are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

- System configurations must include common security parameter settings
- The systems configuration standard should be applied to any new systems configured
- All vendor default accounts and passwords for the systems have to be changed at the time of provisioning the system/device into Secure Block d.o.o. network and all unnecessary services and user/system accounts have to be disabled
- All unnecessary default accounts must be removed or disabled before installing a system on the network
- Security parameter settings must be set appropriately on system components
- All unnecessary functionalities (scripts, drivers, features, subsystems, file systems, web servers etc.,) must be removed
- All unnecessary services, protocols, daemons etc., should be disabled if not in use by the system
- Any insecure protocols, daemons, services in use must be documented and justified

- All users must use a password to access the company network or any other electronic resources
- All user credentials for terminated users must be deactivated or removed as soon as possible, no later than the end of the first working day after a user is terminated
- The user will be locked out if there are more than 5 unsuccessful access attempts. This locked account can only be enabled by the system administrator. Locked out user accounts will be disabled for a minimum period of 30 minutes or until the administrator enables the account
- All system and user level passwords must be changed on at least a yearly basis
- A minimum password history of five must be implemented
- A unique password must be set up for new users and the users prompted to change the password on first login
- Group, shared or generic user account or password or other authentication methods must not be used to administer any system components
- Where SNMP is used, the community strings must be defined as something other than the Standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively
- All non-console administrative access will use appropriate technologies like SSH, VPN, SSL, etc., or strong encryption is invoked before the administrator password is requested
- System services and parameters will be configured to prevent the use of insecure technologies like telnet and other insecure remote login commands
- The responsibility of selecting a password that is hard to guess generally falls to users. A strong password must:
    - Be as long as possible (never shorter than 8 characters)
    - Include mixed-case letters
    - Include digits and punctuation marks
    - Not be based on any personal information

  When an operating system without security features is used for storing and/or transferring sensitive data (such as DOS, Windows or MacOS), then an intruder only needs temporary physical access to the console to insert a keyboard monitor program. If the workstation is not physically secured, then an intruder can reboot even a secure operating system, restart the workstation from his own media, and insert the offending Program. If applicable, to protect against network analysis attacks, both the workstation and the server should be cryptographically secured. Examples of strong protocols are the encrypted Netware login and Kerberos.

14. Anti-Virus Policy

All machines must be configured to run the latest anti-virus software as approved by Secure Block d.o.o. The preferred application to use is the SentinelOne Endpoint Detection and Response (EDR) solution – a next-generation antivirus. SentinelOne must be configured to retrieve the latest updates to the antiviral program automatically. The antivirus should have periodic or continuous scanning enabled for all the systems.

If applicable, all removable media (for example USB sticks and others) should be scanned for viruses before being used.

All the logs generated from the antivirus solutions have to be retained for at least 3 months.

15. Patch Management Policy

All workstations, servers, software, system components etc. owned by Secure Block d.o.o. shall have up-to-date system security patches installed to protect the asset from known vulnerabilities. Where possible, all systems and/or software must have automatic updates enabled for system patches released from their respective vendors. Security patches shall be installed within one month of release from the respective vendor.

16. Vulnerability Management Policy

All identified vulnerabilities would be assigned a risk ranking such as High, Medium, and Low based on industry best practices, such as CVSS base score.

Secure Block d.o.o. will run internal, external network and/or application vulnerability scans periodically, as applicable (e.g., yearly, after major architectural changes, etc.).
Scans conducted after network changes may be performed by Secure Block d.o.o. internal staff. The scan process should include re-scans until passing results are obtained.

17. Change Control Process

Changes to information resources shall be managed and executed according to a formal change control process. The control process will ensure that changes proposed are reviewed, authorised, tested, implemented, and released in a controlled manner; and that the status of each proposed change is monitored. The changes shall be formally defined and documented.

A change control process shall be in place to control changes to all critical company information resources (such as hardware, software, system documentation and operating procedures). This documented process shall include management responsibilities and procedures. Wherever practicable, operational and application change control procedures should be integrated.
All change requests shall be logged whether approved or rejected on a standardised and central system. The approval of all change requests and the results thereof shall be documented. No single person should be able to effect changes to production information systems without the approval of other authorised personnel.
A risk and impact shall be considered when making control changes.

Changes shall be tested in an isolated, controlled, and representative environment (where such an environment is feasible) prior to implementation to minimise the effect on the relevant business process, to assess its impact on operations and security and to verify that only intended and approved changes were made (e.g., test environment).

Any software change and/or update shall be controlled with version control. Older versions shall be retained in accordance with corporate retention and storage management policies.
All changes shall be approved prior to implementation.

Approval of changes shall be based on formal acceptance criteria i.e., the change request was done by an authorised user, impact assessment was taken into consideration and proposed changes were tested.

All users, significantly affected by a change, shall be notified of the change.

Fall back procedures will be in place to ensure systems can revert back to what they were prior to implementation of changes.

Information resources documentation shall be updated on the completion of each change and old documentation shall be archived or disposed of.

To ensure data leakage prevention, developer workstations and tools used to access source code should meet the organisation's end-point security requirements, and direct access to production source code environments should be avoided where development and production repositories can be separated. To ensure resilience and recoverability, as well as prevent leakage, source code backups are maintained on a dedicated Network Attached Storage (NAS) device, which must itself be subject to appropriate access controls, encryption at rest, and regular backup verification to confirm that stored copies are complete, uncorrupted, and recoverable within the organisation's defined recovery time objectives. All access to source code repositories and backup locations should be logged and periodically audited to detect any unauthorised or anomalous activity.

18. Audit and log review

This procedure covers all logs generated for systems within the critical Secure Block d.o.o. environment, including the following components:

- Operating System Logs (Event Logs and OS logs).
- Database Logs
- Antivirus or EDR Logs
- Web server/application access and error logs via PostHog (no personal data collected, anonymized dataset only)

Audit Logs must be maintained for a minimum of 3 months for analysis.

Only responsible predefined personnel are permitted to access log files in AWS Cloud Watch and Sentry (used for error logs when incidents occur in PentestPad – Secure Block d.o.o. proprietary platform environment).

The following Operating System Events are configured for logging, and are monitored:

a) Any additions, modifications, or deletions of user accounts.
b) Any failed or unauthorised attempt at user logon.
c) Any modification to system files.
d) Any access to the server, or application running on the server.
e) Any creation / deletion of system-level objects installed by Windows (almost all system-level objects run with administrator privileges, and some can be abused to gain administrator access to a system).

The following Database System Events are configured for logging, and are monitored:

a) Any login that has been added or removed as a database user to a database.
b) Any login that has been added or removed from a role.
c) Any database role that has been added or removed from a database.
d) Any password that has been changed for an application role.
e) Any database that has been created, altered, or dropped.
f) Any database object, such as a schema, that has been connected to.

The following Firewall Events are configured for logging, and are monitored by:

a) Invalid user authentication attempts.
b) Logon and actions taken by any individual using privileged accounts.
c) Configuration changes made to the firewall (e.g., policies disabled, added, deleted, or
d) modified).

The following Switch Events are to be configured for logging and monitored:

e) Invalid user authentication attempts.
f) Logon and actions taken by any individual using privileged accounts.
g) Configuration changes made to the switch (e.g., configuration disabled, added, deleted, or modified).

The following Intrusion Detection Events are to be configured for logging, and are monitored:

a) Any vulnerability listed in the Common Vulnerability Entry (CVE) database.
b) Any generic attack(s) not listed in CVE.
c) Any known denial of service attack(s).
d) Any traffic patterns that indicated pre-attack reconnaissance occurred.
e) Any attempts to exploit security-related configuration errors.
f) Any authentication failure(s) that might indicate an attack.
g) Any traffic to or from a back-door program.
h) Any traffic typical of known stealth attacks.

The following File Integrity Events are to be configured for logging and monitored by:

a) Any modification to system files.
b) Sensitive actions taken by any individual with administrative privileges.
c) Any Creation / Deletion of system-level objects installed by Windows. (Almost all system-level objects run with administrator privileges, and some can be abused to gain administrator access to a system.)

19. Secure Application Development

The Secure Application Development policy is a plan of action to guide developers' decisions and actions during the software development lifecycle (SDLC) to ensure software security. This policy aims to be language and platform independent so that it is applicable across all software development projects.
Use of Secure Application Development Coding Policy and actions described is a guideline for all software development on Secure Block d.o.o. information technology systems and trusted contractor sites processing Secure Block d.o.o. data.

Each phase of the SDLC is mapped with security activities, as explained below:
a) Design

- Identify Design Requirements from security perspective
- Architecture & Design Reviews
- Threat Modelling

b) Coding
- Coding Best Practices
- Perform Static Analysis

c) Testing
- Vulnerability Assessment
- Fuzzing

d) Deployment
- Server Configuration Review
- Network Configuration Review

Only validated code shall be implemented into Secure Block d.o.o. production environment.

Application Code Developers shall act according to best security practices best as possible:
- Ensure code meets the level of confidence that software is free from exploitable code vulnerabilities, regardless of whether they are already designed into the software or inserted later in its life cycle
- Ensure code provides predictable execution or justifiable confidence and that the software, when executed, will provide security functionality as intended
- Coding techniques must address injection flaws particularly SQL injection, buffer overflow vulnerabilities, cross site scripting vulnerabilities, improper access control (insecure direct object reference, failure to restrict URL access, directory traversal etc.,), cross site request forgery (CSRF), broken authentication and session management
- Never trust incoming data to the system, apply input validation
- Never rely on the client to store sensitive data no matter how trivial
- Disable Error messages that return any information to the user
- Use object inheritance, encapsulation, and polymorphism when appropriate
- Use environment variables prudently and always check boundaries and buffers
- Applications must validate input to ensure it is well-formed

20. Incident Response Plan

Security incident means any incident (accidental, intentional, or deliberate) relating to the communications or information processing systems. The attacker could be a malicious stranger, a competitor, or a disgruntled employee, and their intention might be to steal information or money, or just to damage the company.

Employees of Secure Block d.o.o. will be expected to report to the Operational Security Authority role holder or to an employee with similar job description for any security related issues.

Security incident response related to breach of personal and/or sensitive data is detailed in the Incident response plan.

21. Roles and Responsibilities

Operational Security Authority role holder (or equivalent, such as GSA) is responsible for overseeing all aspects of information security, including but not limited to:

- Creating and distributing security policies and procedures
- Monitoring and analysing security alerts and distributing information to appropriate information security and business unit management personnel
- Creating and distributing security incident response and escalation procedures and spread security awareness
- Monitor and control all access to data
- Maintain a list of service providers
- Ensure there is a process for engaging service providers including proper due diligence prior to engagement where applicable
- Facilitating participation in the security awareness program upon hire and at least annually
- Ensuring that employees acknowledge in writing that they have read and understand Secure Block d.o.o. information security policy

22. User Access Management

Access to company is controlled through a formal user registration process beginning with a formal notification the director.

Each user is identified by a unique user ID so that users can be linked to and made responsible for their actions. The use of group IDs is only permitted where they are suitable for the work carried out.

There is a standard level of access established; other services can be accessed when specifically authorised by the director.

As soon as an individual leaves Secure Block d.o.o. or company related employment, all their system logons must be immediately revoked.

As part of the employee termination process, the supervisors will inform the Operational Security Authority role holder of all leavers and their date of leaving.

23. Access Control Policy

Access Control systems are in place to protect the interests of all users of Secure Block d.o.o. computer systems by providing a safe, secure, and readily accessible environment for work.
Secure Block d.o.o. will provide all employees and authorized users with the information they need to carry out their responsibilities in as effective and efficient manner as possible.

- The allocation of privilege rights (e.g., local administrator, domain administrator, super-user, root access) shall be restricted and controlled, under authorization of Operational Security Authority role holder
- Technical teams shall guard against issuing privilege rights to entire teams to prevent loss of confidentiality

- Access rights will be accorded following the principles of least privilege and on a need-to-know basis
- Every user should attempt to maintain the security of data at its classified level, even if technical security mechanisms fail or are absent
- Users electing to place information on digital media or storage devices or maintaining a separate database must only do so where such an action is in accord with the data's classification
- Users are obligated to report instances of non-compliance to the Operational Security Authority role holder (or equivalent) of Secure Block d.o.o.
- Access to Secure Block d.o.o. IT resources and services will be given through the provision of a unique VPN and appropriated services accounts alongside complex password
- No access to any Secure Block d.o.o. resources and services will be provided without prior authentication and authorization of the director
- Password issuing, strength requirements, changing and control will be managed through formal processes
- Access to Confidential, Restricted and Protected information will be limited to authorised persons whose job responsibilities require it, as determined by the data owner or their designated representative
- Users are expected to become familiar with and abide by Secure Block d.o.o. policies, standards, and guidelines for appropriate and acceptable usage of the networks and systems
- Access for remote users shall be subject to authorization by the Operational Security Authority role holder and be provided in accordance with the Remote Access Policy
- No uncontrolled external access shall be permitted to any network device or networked system
- Access to data is variously and appropriately controlled according to the data classification levels described in the Information Security Policy
- Access control methods include logon access rights, Windows share and NTFS permissions, user account privileges, server and workstation access rights, firewall permissions, IIS intranet/extranet authentication rights, SQL database rights, isolated networks, and other reliable methods if necessary
- A formal process shall be conducted at regular intervals by the Operational Security Authority role holder to review users' access rights

Data masking should be applied in accordance with the organisation's access control policies and other relevant topic-specific policies and business requirements, taking into account applicable legislation including data protection and privacy regulations. Where sensitive or personal data is used outside of its primary production context – masking, pseudonymisation, or anonymisation techniques should be applied to reduce exposure and ensure that individuals working in those environments are not granted unnecessary access to real personal or confidential information. The appropriate masking technique should be selected based on the classification of the data involved and the specific use case, ensuring that masked data remains functionally sufficient for its intended purpose while no longer constituting a meaningful risk if accessed without authorisation.

Appendix A

Asset/ Device Name	Description	Owner/Approved User	Location
AWS Cloud	Internal cloud network	Luka Šikić	Cloud

Appendix B

List of service providers:

Name of Service Provider	Contact Details	Services Provided	GDPR Compliant
Amazon Web Services	https://aws.amazon.com/contact-us/benelux/	Amazon Web Services internal cloud network	YES