

Information Security and Privacy Plan

Information security and privacy within Safeguard



Department Data protection
Company name Safeguard B.V.
Contact info@safeguardapp.nl

Classificatie	Copyright ©	Pagina
Vertrouwelijk	Safeguard B.V.	Pagina 1 van 32

Table of contents

1. Introduction	4
1.1 Purpose	4
1.2 Reading guide	4
2. Physical security and security of work environments	5
2.1 Physical access to office buildings	5
2.2 Physical security of data centres	6
2.3 Physical device management	6
2.3.1 Computers and mobile device security	6
2.3.2 Configuration Management and distribution	6
3. Password policy and account access	7
3.1 Password policy	7
3.2 Multi-factor Authentication (MFA)	8
3.3 Account access	8
4. Security IT	10
4.1 DDoS Protection	10
4.2 Cryptography	10
4.3 Transfer of personal data	10
4.4 PEN-testing	10
4.5 Data validation	10
4.6 Malware, hardening & patching	11
4.7 Security checks	11
5. Security incidents	12
5.1 Incident reporting	12
5.2 Incident handling	12
6. Software-updates and development	13
6.1 Development Process	13
6.2 Third party dependencies, patches & vulnerabilities	14
6.3 Release policy	15
6.4 Source code & Technical Documentation	15
6.5 Risk assessment	16
7. Logging	17
7.1 Division of roles and accountability	17
7.2 Log management	17
7.2.1 Log File structure	17
7.2.2 Events to be logged	18
7.2.3 Events outside log scope	19
7.2.4 Log file protection	19
7.2.5 Time synchronisation	19

Classificatie	Copyright ©	Pagina
Vertrouwelijk	Safeguard B.V.	Pagina 2 van 32

7.3 Reporting and monitoring	19
7.3.1 Reporting	19
7.3.2 Monitoring	19
7.3.3 Distribution	20
8. Backup and recovery	21
9. Processing of personal data	22
9.1 Classification of user data	22
9.2 Exit strategy	23
9.3 Sub-processors	23
10. Business Continuity Management (BCM)	24
10.1 IT-Service Continuity Management	24
10.2 Escrow	25
11. Personnel	26
11.1 Screening	26
11.2 Training	26
11.3 Confidentiality	26
12. Security Policy	27
12.1 From Vision, Mission to Strategy	27
12.1.1 Services	27
12.1.2 Mission and Vision	27
12.1.3 Core Values	27
12.2 From Strategy to Policy	28
12.2.1 Place of Information and privacy Security and privacy in the strategy	28
12.2.2 Concrete policy points	29

Classificatie	Copyright ©	Pagina
Vertrouwelijk	Safeguard B.V.	Pagina 3 van 32

1. Introduction

This information security plan is an elaboration of the information security policy¹.

1.1 Purpose

The purpose of this document is to provide insight into the current measures, procedures and processes that have been implemented at Safeguard to guarantee the quality of information security.

1.2 Reading guide

Chapter 2 explains the procedures for protecting the physical access of the office and servers.

Chapter 3 explains the procedures surrounding password protection, multi-factor authentication and the authorization matrix.

Chapter 4 explains how Safeguard deals with security in the field of; DDos protection, Cryptography, Pen testing and Malware and hardening.

Chapter 5 explains how the process surrounding reporting security incidents works.

Chapter 6 explains the Safeguard development process, how Safeguard deals with patches, how the release policy is structured, what the documentation processes are and how the risk assessment is guaranteed.

Chapter 7 explains how Safeguard handles logging, division of roles and accountability, log management and reporting and monitoring.

Chapter 8 describes the Backup and recovery procedures.

Chapter 9 explains which personal data Safeguard stores and how long they are stored, the exit strategy and withholds a list of sub processors.

Chapter 10 describes how Safeguard deals with business continuity management.

Chapter 11 describes the personnel policy.

Chapter 12 described the Security policy

¹ Information security policy - [Informatiebeveiligingsbeleid - Protocol - v1.0.1.pdf](#)

Classificatie	Copyright ©	Pagina
Vertrouwelijk	Safeguard B.V.	Pagina 4 van 32

2. Physical security and security of work environments

This chapter explains how access management to the office buildings, devices and access to the servers are arranged within Safeguard.

2.1 Physical access to office buildings

When starting employment at Safeguard, all employees are provided with a tag that allow access to our office building. Distributed tags are registered in an overview². One tag is required for full access to the office. Each tag has a unique identification number which tracks what employee opens what door and when. This also allows for the blocking and replacement of lost tags.

The office is secured with a security tag, which is also provided when the employee starts employment at Safeguard. Employee(s) that leave the building last will have to close all doors and windows within the office, and reactivate the alarm using this security tag.

Before the shutter at the main door for the building is closed, employees will have to check if all other people have left the building.

Twice per year there's a check by our facility manager to ensure all tags are present and functioning. All employees are obligated to report missing tags to office management.

If one or more tags are missing or the amount of tags is not correct after the annual check, the following procedure³ will be followed.

1. Check which person is missing a tag.
2. Check for how long the tag has been missing.
3. If tag(s) are lost within the same day, firstly, a general search will be done.
4. If tag(s) are not found before 15:00 that same day, there will be a report to the building manager to block the tag and receive a replacement tag.

² Tag distribution overview - [Safeguard | Access to building](#)

³ Checklist tags - [Missende sleutel procedure](#)

Classificatie	Copyright ©	Pagina
Vertrouwelijk	Safeguard B.V.	Pagina 5 van 32

2.2 Physical security of data centres

Safeguard uses ISO 27001 and FISMA certified data centers which are managed by Amazon Web Services (AWS). AWS has years of experience with designing, building and operating large scale data centres. More information about how AWS secures their data centres can be found on their website.^{4 5}

2.3 Physical device management

2.3.1 Computers and mobile device security

Computers and mobile devices should not be left unlocked. Automatic locking should be enabled with a maximum of 5 minutes. When leaving the device, it should be locked manually. Unlocking should be done with a password that conforms to the password policy, or via biometric access.

Mobile devices should use disk and data encryption where possible, and should not store company information where possible ('Zero footprint').

Mobile equipment used by Safeguard personnel is protected by special profiles that are only accessible with a password that complies with the guidelines and/or by means of biometric access and multi-factor authentication. Safeguard personnel do not store data related to clients on Mobile Devices.

The Security Officer will check twice per year if all devices are secured correctly⁶.

2.3.2 Configuration Management and distribution

An inventory of used mobile devices⁷ is maintained in the Configuration Management Database (CMDB).

When a device is taken to a location outside the Safeguard work area, permission must be requested from the configuration manager. Devices outside the working area must be secured by the above measures.

The Configuration Manager is responsible for updating the CMDB when anything changes, and will update the CMDB at least once every three months.

⁴ AWS Controls - <https://aws.amazon.com/compliance/data-center/controls/>

⁵ AWS Cloud security - <https://aws.amazon.com/security>

⁶ Device security form - [Control form devices](#)

⁷ Inventory of mobile device distribution - [Safeguard | Devices](#)

Classificatie	Copyright ©	Pagina
Vertrouwelijk	Safeguard B.V.	Pagina 6 van 32

3. Password policy and account access

At Safeguard, we make sure that all employees are using their accounts and passwords correctly. There are several procedures in place to manage this:

3.1 Password policy

All employees are required to use safe passwords for all accounts.

The password policy is divided in generic and specific requirements. All accounts have to meet the requirements of both the generic and specific requirements. Initial passwords and passwords that have been reset have a maximum validity of one business day and must be changed on first use to a password compliant with the password policy.

The generic requirements are stated below:

- Passwords have to contain at least 4 out of 5 character types:
 - Lowercase letters
 - Uppercase letters
 - Numbers
 - Punctuation (for example: “;?;!)
 - Symbols (for example: @#\$%^&* < > ~ +=)
- Reusing the same password when the password needs to be changed is prohibited.
- Default account names and passwords will be changed after the first login. After initiating an information system, default account names and passwords may not be present anymore.

All accounts need to be classified as a specific account type; these types are explained below. These accounts have to comply with the requirements linked to their type. These requirements are in addition to the generic requirements:

Application management account

- Description: A personal account used to manage applications running on systems.
- Type: personal (traceable to a specific person)
- Password length: minimum of 15 characters

Administrator account

- Description: A personal account that provides the user full access using administrator permissions.
- Type: personal (traceable to a specific person)
- Password length: minimum of 15 characters

Classificatie	Copyright ©	Pagina
Vertrouwelijk	Safeguard B.V.	Pagina 7 van 32

Office automation Account (OA-account)

- Description: A personal account that allows employees to work using an office automation environment.
- Type: personal (traceable to a specific person)
- Password length: minimum of 8 characters

There must be a risk assessment and necessary actions for information systems that do not meet our generic and specific password requirements. These anomalies will be documented and communicated. (security checklist)

We use 1Password⁸ as a vault for passwords. The Security Officer is responsible for the correct enforcement of the password policy outlined above via 1Password. The security officer periodically checks if employees adhere to our password requirements⁹.

3.2 Multi-factor Authentication (MFA)

Where possible, MFA will be enforced by the systems we use. When enforcement is not possible, personnel are still required to turn on MFA where possible. When no MFA is available, a risk assessment must be performed by the Security Officer, which should be documented.

MFA codes may not be stored in the Password Manager software we use (as described in 4.3), but in the Google Authenticator app where possible. If there is no option to use the Authenticator app, SMS may be used.

3.3 Account access

Personnel will be granted access using a need-to-know principle. They should use Single Sign-On (SSO) via Google where possible, to decrease the number of accounts used. (security checklist)

When a person joins the company, appropriate access will be granted according to protocol.¹⁰ There is a similar protocol when an employee leaves the company.¹¹

Account names must not contain a description of the access level it has (for example 'Henk Administrator' may not be used).

Separate accounts should be used for different access levels. Conflicting roles and responsibilities should use separate accounts to minimise the risk of unauthorized or accidental changing or misuse of company resources.

Which person has which access is maintained in the Authorisation Matrix¹². The security officer checks these twice per year to determine if it is still up to date¹³. The security officer will also

⁸ 1Password - <https://1password.com/business/>

⁹ Periodic check Security Officer - [Security check](#)

¹⁰ Checklist indiensttreding - [Checklist indiensttreding](#)

¹¹ Checklist uitdiensttreding - [Checklist uitdiensttreding](#)

¹² Authorisation Matrix - [Authorisation Matrix](#)

¹³ Authorisation control form - [Authorisatiematrix controleformulier](#)

Classificatie	Copyright ©	Pagina
Vertrouwelijk	Safeguard B.V.	Pagina 8 van 32

check twice per year if the access levels are still up-to-date and if an employee does not have access to services they should have access to¹⁴.

When an employee requires access to a service they did not have access to before, the following procedure is followed:

1. The employee sends a request for access¹⁵ to the security officer.
2. The security officer then performs a risk assessment for the request for access.
3. If the security officer accepts the request for access, a new account will be created for the employee. This account should preferably be a temporary account depending on the actual needs of the employee and security risks involved.
 - a. The employee will receive the necessary information regarding the new account from the Security Officer.
 - b. The account will be created by the owner of the IT asset.
 - c. Security officer will update the authorization matrix.
4. If the security officer declines the request, they will notify the employee regarding the request and the reason(s) why it was declined.

¹⁴ Periodic check Security Officer - [Security check](#)

¹⁵ Request Access form - [Controleformulier toegang](#)

Classificatie	Copyright ©	Pagina
Vertrouwelijk	Safeguard B.V.	Pagina 9 van 32

4. Security IT

Security is an important part of the Safeguard platform therefore we have included the following measures, which are stated in this chapter, to ensure this.

4.1 DDoS Protection

For DDoS protection, we use AWS Shield Standard. This is a DDoS protection service provided by AWS that safeguards applications. AWS Shield provides always-on detection and automatic inline mitigations that minimize application downtime and latency¹⁶.

4.2 Cryptography

We use TLS 1.2 certificates for all client-server communication. Once per year we refresh these certificates, and update to a new TLS version if applicable.

We have an encryption-by-default policy, and use the industry standard where available. We use EBS Encryption¹⁷ by AWS in combination with the AWS Key Management Service(KMS)¹⁸.

4.3 Transfer of personal data

When personal data is transferred to customers it will always be encrypted. The password required to unlock the data will always be sent through a different medium (for example SMS). See 9.2 for more information regarding data transfer.

4.4 PEN-testing

We have an external party perform a black box PEN-test annually on the Safeguard system. When a PEN-test fails in meeting the success criteria, we will resolve the high and critical finding(s) within three months and will execute a new PEN-test within three months after resolving the finding(s). All PEN-test reports are saved and organized in the Safeguard file system¹⁹.

4.5 Data validation

We require validating all incoming data, employing suitable frameworks within our code to guarantee its integrity. This validation encompasses safeguarding against injection attacks, verifying data types, eliminating invalid characters, monitoring for out-of-range values, and respecting predefined data limits.

¹⁶ AWS Shield - <https://aws.amazon.com/shield/>, more information: [How AWS Shield works - AWS WAF, AWS Firewall Manager, and AWS Shield Advanced](#)

¹⁷ EBS Encryption - <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html>

¹⁸ AWS KMS - <https://aws.amazon.com/kms/>

¹⁹ Pen test folder - [PEN Tests](#)

Classificatie	Copyright ©	Pagina
Vertrouwelijk	Safeguard B.V.	Pagina 10 van 32

4.6 Malware, hardening & patching

In the AWS environment we make use of the existing functionality in the form of services that make sure that the workloads present there are set up and configured correctly according to the requirements set.

In the first place, we use AWS Config for this. This is a service that makes sure that everything happening in an AWS environment is done via a set list of requirements. Whenever it doesn't conform to those requirements, automatic action can be taken. For example, a requirement could be that system log information is sent to the correct AWS account. Whenever this would be disabled, AWS Config can re-enable it automatically. Hardening is also enforced this way.

Next to these checks, we use Amazon Inspector to check if workloads are vulnerable to known vulnerabilities, and use automated systems to bring environments to the correct level of performance.²⁰

For anti-malware we make use of a reputable anti-malware solution, at the moment this is Trend Micro.

We use NordLayer's 'ThreatBlock' as a web filter.

More information can also be found in Chapter 6.2.

4.7 Security checks

Twice per year the security officer will perform a security check. This check includes the following:

1. Password check on Safeguard personnel to ensure the policy described in chapter 3 is followed.
2. Physical security check on tags to ensure the policy described in chapter 2 is followed.
3. Clear desk and clear screen check to ensure the policy described in chapter 12 is followed.
4. Equipment check to ensure laptops and mobile phones are up-to-date and maintained per the policy described in chapter 2.
5. A privacy check so that there's no personal data stored on personnel laptops.
6. Making sure the authorisation matrix is up-to-date.
7. Perform a logfile analysis.

²⁰ Amazon inspector check - [Checklist Amazon Inspector](#)

Classificatie	Copyright ©	Pagina
Vertrouwelijk	Safeguard B.V.	Pagina 11 van 32

5. Security incidents

This chapter explains how the process surrounding reporting security incidents works.

5.1 Incident reporting

We have a 24/7 incident reporting process in place for notifying clients in case of security incidents. These incidents should be reported to the agreed upon clients contacts²¹.

The incident report process is laid down in the SLA, processor agreement and general terms and conditions concluded between Safeguard and the client.

Conversely, clients may report incidents detected by them 24/7. These incidents include but are not limited to:

- Distribution Denial of Service: attack that makes a contracted service unavailable to its users, where the attack source is more than one unique IP address. DDoS testing is further documented in Chapter 4.1.
- Advanced Persistent Threat: a set of stealthy and continuous computer hacking processes to monitor or extract data from a specific target related to the Service.
- Data corruption: the intentional introduction of unauthorized changes to Client Data.
- Data Leakage: the unauthorized transmission of Client Data from within an organization to an external destination or recipient.
- Ransomware: form of malware which holds a user's computer hostage until a "ransom" fee is paid.
- Money Fraud: the illicit use of Client's or its service provider's IT systems for deliberate deception to secure unfair or unlawful gains. Money fraud includes cyber crimes such as (large scale) electronic identity theft or unlawful intrusion into a network.

5.2 Incident handling

When we identify a security incident, we will communicate this to the affected parties within 24 hours. When an external party (e.g. clients) detect a security incident, we will cooperate with said party to resolve the incident as soon as possible.

We will have a retrospective meeting with the Development and Security teams to learn lessons from the incident and the process itself, and inform the affected parties of those lessons learned. All factors regarding incidents are logged in a document, based on a specified template²².

The security incidents, together with the solutions for them and the lessons learned will be documented in the security incident log. Logs are further documented in Chapter 7.

²¹ Client contacts for incident reporting - [Safeguard | Contacts per customer](#)

²² Incident report template - [Checklist datalek](#)

Classificatie	Copyright ©	Pagina
Vertrouwelijk	Safeguard B.V.	Pagina 12 van 32

6. Software-updates and development

This chapter elaborates on the development process of the Safeguard platform. This process is secured by the versioning history and logging on the Jira and Github platforms.

6.1 Development Process

Safeguard uses a DTAP (Development, Test, Acceptance, Production) strategy with environments that are separated physically to minimise the interference of data. The environments are hosted on AWS servers. Safeguard uses Privacy by design in all its development processes.

We use JIRA as a Project Management tool, using an Agile methodology. There are generally two reasons for creating a ticket on JIRA:

1. A bug reported internally or externally;
2. To design and develop a new feature or to update and improve an existing feature.

When a bug is reported an impact assessment will determine how quickly it needs to be resolved. Ranging from critical to low priority.

The idea for a new feature or improvement can come from customer feedback, research or internal discussions. When the idea is ready for the design and development phase it gets moved to JIRA and will go through the following steps:

1. To-do in design: the tickets for a designer to work on it;
2. Research: the designer and product manager gather information;
3. Design: the designer creates an initial concept of the feature and its workings;
4. Review: the design gets reviewed by another member of the design team;
5. Create tickets for development: the designer creates tickets for the development team;
6. To-do in development: the ticket waits for a developer to work on it;
7. In progress: a developer is working on the ticket;
8. Code-review: every ticket must first pass code review by at least 1 other developer, and pass automatic tests and other quality checks;
9. Test 1: the ticket will be tested by a qualified member of the testing team;
10. Test 2: another member of the testing team will test the same ticket;
11. Tested: the ticket waits to go from the Development environment to the Acceptance environment;
12. Quality Assurance (QA)1: the ticket will be tested against the Acceptance environment;
13. QA 2: the ticket will be tested again by a different qualified tester;
14. Waiting-for-release: once a ticket has been fully tested and passed said tests, it will wait for release;
15. Released: the ticket has been released onto the production environment.

Classificatie	Copyright ©	Pagina
Vertrouwelijk	Safeguard B.V.	Pagina 13 van 32

On top of the steps described above, there are three more independent tests done before each new release:

- A regression test that tests every functionality of the product, this is done to ensure new changes haven't affected other functionalities;
- An acceptance test once the quality assurance phase has been completed. This tests the most critical features of the product and is the last check before a release;
- A release test is carried out after a new release to ensure its working on the production environment.

Steps 7 and 8 will be conducted on the Development environment, steps 9 and 10 are carried out on the Test environment, steps 12 and 13 are carried out on the Acceptance environment and step 15 is on the Production environment.

All test data is done by using dummy test data. No personal data from customers is used in developing or testing.

If at any point in the testing process a bug is found or the ticket doesn't work as intended, the ticket will be rejected and put back to the 'To-do in development' phase, under a new component: test failed. The ticket will resume all the steps until it's ready for release.

Personnel responsible for the testing has actual, specialist knowledge, skills, training and experience with regards to testing, privacy and security.

6.2 Third party dependencies, patches & vulnerabilities

We risk assess every dependency with a checklist.²³ We review this list annually. Reviewing each newly added dependency is part of our code review process which contains checks which make sure each dependency is only added when appropriate. For dependencies that are managed by a supplier, no risk assessment is needed, as we assess all our suppliers as laid out in 9.3.

We use Dependabot²⁴ to automatically check for known vulnerabilities and patches in our dependencies, and create Pull Requests to fix these. Our security officer will be automatically notified if there are any major issues.

On top of this, every release the Lead developer for every platform will manually check all dependencies for their platform for possible patches or vulnerabilities, and update them accordingly. This is logged using the Dependency Control Form.²⁵

²³ Dependency toevoegen - [Dependency toevoegen checklist](#)

²⁴ Dependabot - <https://dependabot.com/>

²⁵ Dependency controle - [Dependency controle checklist](#)

Classificatie	Copyright ©	Pagina
Vertrouwelijk	Safeguard B.V.	Pagina 14 van 32

6.3 Release policy

Safeguard has a release policy that defines when and how releases are handled. Major releases are planned according to our development roadmap. We keep every release as 'small' as possible, making sure the impact on other functionalities is kept to a minimum. Each release of the app is rolled out in phases, contains a backup plan and is documented.

A functionality request or improvement proposal is assessed by the Contractor and the submitter is informed of the outcome of this assessment. In the event that the requested functionality or the requested improvement proposal is implemented, the submitter will also be informed in which release (minor release or major release) it will become available.

Safeguard's release policy is based on impact and scope and is divided into three different types of releases:

- Major release: an important roll-out of functions, with a significant extension of functionality. These releases often provide solutions for a number of known errors, work-arounds and quick fixes. These releases are identified as version 1, version 2 and so on.
- Minor release: a rollout of changed functions with changes in functionality and improvements for known errors, work-arounds and quick fixes. These releases are often referred to as version 1.1, version 2.1 and so on.
- Patch release: a set of non-functional changes and minor improvements for known errors, workarounds and quick fixes. These releases are often referred to as version 1.1.1, version 2.1.2 and so on.

For every release, the CTO will document the release using a specified form²⁶.

For big releases, Functional Managers will inform clients before the release about the changes made in the release, and where necessary provide them with training after the release.

6.4 Source code & Technical Documentation

All source code and technical documentation is under GIT version control using Github²⁷, and will never reside in a production environment.

Developers are granted access on a need-to-know basis, following the account access policy outlined in Chapter 3.3.

²⁶ Safeguard Release form - [Release formulier](#)

²⁷ Github - <https://github.com>

Classificatie	Copyright ©	Pagina
Vertrouwelijk	Safeguard B.V.	Pagina 15 van 32

6.5 Risk assessment

A risk assessment²⁸ in relation to the Safeguard system shall be performed by the Security Officer when:

- The scope of the system is expanded to include new information assets with new functionalities; and
- A new community of users is introduced; or
- Other major changes impact functional and non-functional requirements that justify a risk and impact analysis

²⁸ IB Ontwikkel protocol - [Informatiebeveiligingsprotocol ICT ontwikkeling](#)

Classificatie	Copyright ©	Pagina
Vertrouwelijk	Safeguard B.V.	Pagina 16 van 32

7. Logging

Events within Safeguard systems are recorded in the form of log files in an audit trail. Log files are used for problem identification, detecting system abuse, problem investigation and troubleshooting.

Audit trails must comply with the ISO/IEC 27001 and ISO 27701 requirements to ensure integrity, availability and confidentiality.

7.1 Division of roles and accountability

To safeguard the logging process, roles have been set up for monitoring log files, technical research, functional research, checking security requirements and a role of owner, who is considered ultimately responsible for the system.

Log manager

In the log system of Safeguard, the Log manager is responsible for managing and monitoring the log system. The log manager is considered responsible for the log system

Security officer

In the log system of Safeguard, the Security officer is responsible for investigating any possible security threats and informing the right people in case of a threat.

Functional manager

The functional manager conducts research in the functional area. In Safeguard, this is the person who deals with the contact with clients.

Technical manager

The technical manager conducts technical investigations in the event of an incident. Required information is provided by the Security officer.

7.2 Log management

7.2.1 Log File structure

In order to collect sufficient information about an event, a log file must be provided with information about the moment, the location, the cause and the content of the event. The 4 W's (Who, What, Where, When) are used here. Detailed Information can be found in Table 1.

Table 1: Requirement matrix for logbook files

	Description	Required
When	Time & Date	Yes
Where	Systemname	Yes

Classificatie	Copyright ©	Pagina
Vertrouwelijk	Safeguard B.V.	Pagina 17 van 32

	System IP-address	Yes
	System version	Optional
	Service name, protocol and port	Optional
	Use module	Optional
What	Event description	Yes
	Event result	Yes
	Unique ID	Yes
Who	Source (IP-address, e-mail, phone et cetera)	Yes
	User ID	Optional

This information can be used to troubleshoot potential issues. When contacted by a customer we can use the information in the audit logs to address inquiries or perform root cause investigations. This information is never passed down to customers.

7.2.2 Events to be logged

Events are automatically logged where possible. Specifically in the Safeguard system, an Audit Log module is used, which is structured as described in chapter 7.2.1.

If it is not possible to use automatic logging within a system, a logbook may be used by administrators, for example. Manually logged operations²⁹ are stored within the Safeguard system.

Events that are at least included in log files in the audit trail are:

- Use of technical management functions. Examples include changing a configuration, running system commands, and performing a backup or system restore.
- Use of functional management functions. Examples of this are the release of new functionalities and interventions on databases.
- Security management operations. Examples include adjusting rights and issuing (or confiscating) keys.
- Security incidents. Examples of this are incorrect login attempts and unauthorized use of system functionalities.
- Disruptions in a system. Examples are the unavailability of services and the filling of server capacity.
- Actions by users. Examples include login attempts (both correct and incorrect), changes to the Safeguard system and access to files.

²⁹ Manually logged operations - [Safeguard | Audit Logs 2020](#)

7.2.3 Events outside log scope

The purpose of logging is to identify events and investigate the cause of what happened. The following data should not be included in a log file:

- Privacy sensitive data that is not necessary to perform this task.
- Security sensitive data such as: passwords, encryption codes, access codes, dial-in numbers, etc.
- Misuse-sensitive data such as credit card numbers and bank accounts.

7.2.4 Log file protection

Log files are protected against forgery and unauthorized access. All log files are stored on a separate AWS account. These files are automatically deleted after 90 days. If an incident is suspected, the log files involved are stored for at least 3 years. This ensures that log files are available within the period in which a log analysis is deemed necessary.

Consultation of log files is reserved for authorized users; these users can only view the log files and cannot mutate or delete them. Log files in the Safeguard system may not be modified.

An overview of current authorizations can be found in our authorization matrix³⁰.

There are checks for the storage of the audit trail. When the storage capacity of the database for the log files falls below a certain limit, this leads to automatic alarms to the Log Manager and Security Officer. Even if the log server is not accessible (or file storage is no longer possible), they are automatically alerted.

7.2.5 Time synchronisation

It is necessary to synchronize the system time of relevant information systems in order to reliably analyze log files on the different systems. All relevant information processing systems are therefore synchronized with an NTP server. Amazon Time Sync Service is used for this.

7.3 Reporting and monitoring

7.3.1 Reporting

Reports are made during every security check using a template³¹. Log files of administrators have the highest priority under normal circumstances (no critical messages) when analyzing log files in the Safeguard system.

Reports consist of an analysis of the situation, investigation of the cause and, where possible, a proposal for a solution or measures to be taken.

7.3.2 Monitoring

Active monitoring is applied to the following points (see Chapter 4):

³⁰ Safeguard authorisation matrix - [Authorisation Matrix](#)

³¹ Safeguard Log file analysis form - [Logfile analysis formulier](#)

Classificatie	Copyright ©	Pagina
Vertrouwelijk	Safeguard B.V.	Pagina 19 van 32

- Reports that cause problems in live environments. Triggers have been set up for this, generated by AWS and Updown.IO. Warnings are communicated directly to the relevant personnel.
- Threats such as:
 - DDoS attack (See Chapter 4.1)
 - Virus or Malware notifications
 - Log file changes
 - Storage capacity
 - Unauthorized access

7.3.3 Distribution

In order to take action on notifications that have been made, it has been mapped (see Table 2) with tasks for the persons per role. Within Safeguard, all types of threat notifications are handled the same. Reports that are not perceived as a threat are monitored by the log manager and escalated as deemed necessary by the security officer.

Table 2: Role assessments for logging

Threat type	Log manager	Security officer	Technical manager	Functional manager
Threats	Detect threats and inform security officer	Research security issues.	Research and resolve.	Investigate effects and possibly inform end users.
Non-threats	Monitoring and periodic checking.	When an issue is found; research security issues.	When a report is a technical problem; research and resolve.	When a report is a functional problem; research and investigate a solution.

8. Backup and recovery

All physical systems are located within secure Amazon Web Services (AWS) data centers that are up to the highest quality and security standards and are compliant with ISO 27001.

There's a backup made every 24 hours. This data is stored for 7 days.

Within our AWS environment there is a difference between accounts that have access to different systems. Per AWS account there is decided what can and can not be done on the basis of 'least privilege'. This applies to users, groups of users and roles the AWS system can use. All back-up data is placed within a separate account where access is strictly regulated. Access to this data is for authorized personnel only.

We will test this recovery procedure³² every year or when significant changes are made to ensure reliability in case of emergency. Our Security Officer is responsible for this procedure and will follow a specified form³³. A test report will be made and filed so that we can ensure the correct procedure is followed.

³² BCP Test - [BCP Test Template](#)

³³ Safeguard AWS Recovery

Procedure Form -  [DDMMYYYY] Back-up en herstel test

Classificatie	Copyright ©	Pagina
Vertrouwelijk	Safeguard B.V.	Pagina 21 van 32

9. Processing of personal data

Personal data within Safeguard is stored on servers in the EU, Ireland and the back-up location is in Germany, EU. Safeguard follows the guidelines of the GDPR when processing personal data. Processor agreements are drafted and signed in consultation with customers.

Clients remain the owners of the data generated in the Safeguard platform. Safeguard personnel may only process this personal data for the intended purpose. Access to this personal data is logged. Files exchanged between Safeguard and clients that contain personal data will be encrypted.

Safeguard personnel who are allowed to process personal data are in possession of a valid VOG (Verklaring Omtrent Gedrag). This is maintained in the personnel folder.

9.1 Classification of user data

Safeguard stores user data in order to function correctly. This data is viewed as personal and classified. The evaluation of the classification is checked annually by the Privacy officer.

- Name - Until termination of contract
- E-mail address - Until termination of contract
- Phone number - Until termination of contract
- Function - Until termination of contract
- General phone hardware information (brand and type) - 90 days
- Phone settings (Push notifications, GPS, WiFi, OS version and App version) - 90 days
- Presence of users when they are on a predefined location - 90 days
- Data regarding the creation of and responses to alarms - 90 days
- Audit logs - 90 days
- Profile pictures - Until termination of contract
- Logfiles we use to determine problems and provide support - 90 days
- Conversations with our support team via in-app chat function or via email - Until termination of contract

We collect this data for the following purposes:

1. To deliver and personalise our services.
2. To inform users about our products and services.
3. Financial administration.

Data that is stored until termination of contract will be deleted upon said termination. Data that is stored for 90 days will automatically be deleted.

Classificatie	Copyright ©	Pagina
Vertrouwelijk	Safeguard B.V.	Pagina 22 van 32

9.2 Exit strategy

With regard to the exit plan that Safeguard uses, the following is assumed:

1. Upon termination of the user agreement, the option to use the Safeguard app expires.
2. The conditions with regard to the use of the Safeguard app are laid down in the agreement concluded with the affected client.
3. The exit plan that Safeguard uses applies both at the expiration of the agreement and in cases where the agreement may not have expired, but the relationship with Safeguard as the contractor ends, for whatever reason.
4. The operation of any concluded processor agreement applies until the moment that the execution of the exit plan has been completed. In practice this will mean that the data has been transferred.
5. When providing the data, based on the exit plan, Safeguard will add an overview that can be used to check whether the transfer of the data is complete. In consultation with the client, Safeguard will record at the start of the relationship which data is processed and stored by Safeguard and how the completeness of this data can be checked in case of exit.
6. Safeguard can provide the data that is processed and generated using the app, if desired. Safeguard uses JSON as standard format. Safeguard provides the client with the data from 90 days before the date of expiry of the contract.
7. The client will receive all data when making it available.
8. The exit plan will be completed within a maximum of 30 days after termination of the user agreement.

9.3 Sub-processors

Safeguard uses subcontractors to provide the service to our clients. Subcontractors who process personal data must be ISO 27001 or SOC II certified or have demonstrably comparable documented processes. We consider ISO 27001 or SOC II as an industry standard and therefore sufficient. Certificates or management statements from subcontractors that process personal data must be submitted annually. Electronic messages communicated between subcontractors and Safeguard are encrypted according to the guidelines stated in chapter 10.

Safeguard must have a processing agreement with any subcontractors that process user data in place.

Classificatie	Copyright ©	Pagina
Vertrouwelijk	Safeguard B.V.	Pagina 23 van 32

10. Business Continuity Management (BCM)

Safeguard has continuity plans in which measures have been taken to prevent interruption of the services for the clients for the critical service processes. This protects them from the consequences of major failures and restores them. This also guarantees the continuity of information security. These plans are reviewed annually and refined where necessary, and communicated with clients that wish to.

10.1 IT-Service Continuity Management

Safeguard has set up a decision structure and organization for rapid recovery in the event of an emergency (see Table 3). In the event of a serious emergency, a Recovery Plan and a Contingency Plan are in place.³⁴

Table 3: Crisis escalation matrix

Role	Normal	Crisis
Managing board	• Determine BCM-policy and -strategy • Human Resource management • Determine access to processes	• Crisis management • External contact
Management	• Process management • Communication and awareness • Integration ITSCM within BCM • Conducting a risk analysis • Define products • Drawing up contracts • Performing tests	• Coordination • Process control • Making resources available • Start of continuity and recovery • Teamlead • Report
Employees	• Develop products • Negotiate • Run tests • Create reports • Develop procedures	• Perform recovery • Teamwork

Our hosting partner AWS applies its own Business Continuity Management process followed by an IT Service Continuity Management process³⁵.

³⁴ Business Continuity Plan - [Business Continuity Plan](#)

³⁵ AWS Disaster Recovery - <https://aws.amazon.com/disaster-recovery/>

10.2 Escrow

In the interest of the continuity of the service, Safeguard has made a Cloud Secure arrangement that can be used by clients for a fee. The Cloud secure arrangement allows the client to continue to use the service in the event of a bankruptcy of Safeguard, without any downtime to their service.

Safeguard has a redundant legal structure by means of various legal entities, in which the Intellectual Property of the service is separated from the operating company.

In case of bankruptcy of Intellectual Property B.V. the Cloud Secure arrangement³⁶ comes into effect for clients who have purchased it. Continuity of the service is then guaranteed by the Safeguard Secure Foundation, which can only continue in the service under predetermined conditions.

³⁶ More information on Softcrow arrangement - <https://softcrow.com/nl-cloudsecure/>

Classificatie	Copyright ©	Pagina
Vertrouwelijk	Safeguard B.V.	Pagina 25 van 32

11. Personnel

At Safeguard we care greatly about our personnel and the safety of the data of our customers therefore we have procedures in place that explain how our personnel are screened and trained. These procedures can be found in this chapter.

11.1 Screening

Safeguard performs a screening process when hiring new personnel. Safeguard personnel have a VOG no older than 3 years. Every year, the HR Manager checks which VOG's expire and whether they are still valid. We have a control form³⁷ in place to perform this check.

11.2 Training

Every year, the security officer of Safeguard provides training appropriate to the nature of the work to be performed to the staff members, which at least also includes personal responsibility. Specific requirements with regard to security frameworks of Clients will be included in the training in the next training courses.

Part of this training is the awareness program for behavioral aspects of safe mobile working, and all other matters regarding account security and privacy. All personnel is required to submit a signed form³⁸ which states they have completed the training.

The employment contract of employees contains a provision for mobile working, by which they declare that they are aware of the dangers of mobile working and that they will do so safely.

Employees sign a user agreement for working on mobile devices, in which they declare that they are aware of the dangers of working (remotely) on mobile devices and that they will do so safely. This agreement applies to all mobile equipment that the employee uses for business activities.

11.3 Confidentiality

Safeguard personnel and subcontractors sign a nondisclosure agreement. The following matters are included in this confidentiality statement:

- The relationship between parties;
- The reason why the confidential information is provided;
- To which the confidential information relates;
- What the consequences (could be) if the receiving party violates the confidentiality statement;
- Whether the receiving party has employees. The receiving party must also bind these employees to the confidentiality statement.
- Penalty clause.

³⁷ VOG Control Form -  [DDMMYYYY] Controleformulier personeelsdossiers

³⁸ Safeguard Training Confirmation Form -  [DDMMYYYY] Presentielijst Bewustwordingstraining

Classificatie	Copyright ©	Pagina
Vertrouwelijk	Safeguard B.V.	Pagina 26 van 32

12. Security Policy

12.1 From Vision, Mission to Strategy

12.1.1 Services

Safeguard B.V. offers the following services:

The Safeguard app, an application to call up emergency responders and provide communication during an incident.

We offer these services to the following customers (groups):

Organizations and companies with an emergency response organization of at least 5 emergency response officers.

Scope of service: Development, implementation, management and support of Safeguard Cloud software for supporting emergency response.

12.1.2 Mission and Vision

Our mission is to alert the right people in an emergency so they can provide assistance. We achieve this by designing, developing and selling our Safeguard app. Usability, scalability and reliability are our core values that we use as a compass to determine further steps in our company.

Our vision is to create a global network of emergency responders that can be alerted to provide assistance in an emergency.

12.1.3 Core Values

We have the following core values:

- Integrity of our services is essential. The correctness of the information that is processed within our application and within the organization is of great importance to us.
- Information is handled according to our information security policy and protocols.
- The user experience of our application is of great importance to us and our customers.
- Scalability of our service is important to realize our vision.
- Reliability of our service is critical because our customers rely on Safeguard to function properly during an incident. Our ICT infrastructure is set up in a redundant manner.

Classificatie	Copyright ©	Pagina
Vertrouwelijk	Safeguard B.V.	Pagina 27 van 32

12.2 From Strategy to Policy

12.2.1 Place of Information and privacy Security and privacy in the strategy

Information flows within Safeguard B.V. almost always have to do with the availability, integrity and confidentiality of privacy-sensitive personal or business data. It is therefore very important for Safeguard B.V. to ensure that these data are properly and adequately secured and that only those persons have access to the data who, based on their role, need to use the data for the further performance of work. This greatly contributes to the satisfaction of our customers.

- Information security and privacy supports our mission, vision and core values:
 - We strive for continuous improvement of the quality of services and processes and information security of our data through the Plan-Do-Check-Act cycle.
- Information security and privacy support our strategic goals:
 - The objectives in the field of quality, privacy and information security of Safeguard B.V. support the realization of the policy objectives. The objectives of the past year are evaluated annually and the new objectives for the coming year are formulated.
 - As indicated earlier, we have four strategic goals:
 - Be relevant to our customers;
 - Sufficient profitability to be able to make investments;
 - Sufficient scale to guarantee continuity;
 - Enough customers to be able to overcome risk of failure.
 - The following information relates to security objectives: the recovery time objective (RTO) is 4 hours and the recovery point objective (RPO) is 28 hours.
- Information security and privacy support our competitive strategy:
 - We generate trust with our customers because we strive to meet or exceed customer expectations and an optimal balance in confidentiality, integrity and availability of information and data.
 - We are compliant with the requirements of legislation and regulators, such as the General Data Protection Regulation (GDPR).
 - Information security and privacy are essential in our competitive strategy, because Safeguard B.V. uses a Product Leadership in combination with a Customer Intimacy strategy. It is important that all information security and privacy matters are in order, in order to continue to deliver the best product. When security or privacy incidents occur, this is at the expense of customer confidence and we are less able to implement our Customer Intimacy strategy.
- Quality, privacy and information security support our value chain:
 - We set out processes in a clear, goal-oriented and transparent manner and ensure that information is available, honest and confidential.
 - We safeguard our quality and information security processes in a formal management system.
 - We certify our management system according to the ISO 27001: 2022, ISO 27701:2019 and ISO 9001:2015 standard.

Classificatie	Copyright ©	Pagina
Vertrouwelijk	Safeguard B.V.	Pagina 28 van 32

12.2.2 Concrete policy points

General policy

Our general policies are:

- We work according to established ISO processes;
- We work and communicate transparently to our customers and have a no-nonsense approach;
- We have appointed a compliance officer, a quality manager, a privacy officer and a security officer to support and coordinate our management system.
- We have hired a Data Protection Officer externally for knowledge and expertise.

Quality policy

Our quality policy focuses on the following aspects:

- We use a skills matrix and provide well-trained personnel who have the necessary certifications;
- There's continuous training and personal goals for each employee to develop in their fields;
- There are customer satisfaction surveys and other means of feedback to improve our services;
- An extensive test plan is used within the development process. The testing is done by different people and goes through several stages. After tickets have been approved within test 1, test 2 and QA, an extensive system test is performed;

It is always assessed whether a desired / requested function is of added value to the system and will be assessed before any development is started;

Information security policy

Our information security policy focuses on the following aspects:

- As a board, we actively support information security within the organization by providing clear direction, showing commitment and explicitly recognizing and assigning responsibilities for information security. Tasks, responsibilities and authorities are laid down in our job profiles to which we refer in chapter 1 of our integrated management manual.
- We have established policies to protect the exchange of information through the use of all types of communication facilities.
- We have established, documented and assessed access policies based on business and security requirements for access.
- We have a "clear desk" policy for paper and removable storage media and a "clear screen" policy for IT facilities. Specific agreements on this are laid down in our HR Information Security Protocol and in our code of conduct.
- With regard to the use of network services, our starting point is that users are only granted access to services for which they are specifically authorized. Detail Agreements regarding network services are laid down in our Information Security Protocol ICT Management.

Classificatie	Copyright ©	Pagina
Vertrouwelijk	Safeguard B.V.	Pagina 29 van 32

- We have a strict policy to protect against risks associated with the use of portable computers and communication facilities. The details of this are laid down in both our Facility Management Information Security Protocol and our code of conduct.
- We have a strict home working policy. The details of this are laid down in both our Facility Management Information Security Protocol and our Code of Conduct.
- We have a policy on cryptographic controls for the protection of information. This is especially important when exchanging information with customers with a high information security profile.
- We work with a business continuity plan in which information security plays an important role. Details about the organization of business continuity can be found in the BCP.
- We follow the law when it comes to privacy, intellectual property rights and competition. An overview of relevant legislation and regulations is included in our integral management manual.

Privacy policy

Our privacy policy focuses on the following aspects:

- We are transparent in our communication with customers, partners, and (government) agencies regarding privacy.
- We have appointed a Privacy Officer / Data Protection Officer to ensure compliance with the GDPR and related laws and regulations.
- We ensure that we always meet the legal requirements for data processing. To this end, the following principles are applied:
 - Purpose limitation: Personal data is only processed for the purpose specified in the processing register.
 - Lawfulness: All personal data is processed based on a clear legal basis.
 - Minimal data processing: Our organization only processes personal data that is necessary for the purpose.
 - Accuracy of processing and data erasure: Personal data that is processed is accurate and updated when necessary. In addition, personal data that no longer serves a purpose is actively deleted.
 - Storage of personal data: Personal data is stored in a way that enables individuals to be identified only for the purposes for which the data is processed. If personal data is stored for longer periods for archiving purposes in the public interest, scientific or historical research, or statistical purposes, appropriate technical and organizational measures are taken to ensure that the rights and freedoms of individuals are protected.
 - Technical and organizational measures: Our organization takes technical and organizational measures to protect personal data against unlawful processing, loss, destruction, or damage. Please refer to our information security policy for more details.

Following this, our organization has taken the following measures:

- We maintain a processing register that lists all processing activities related to personal data, both in the primary process and in supporting processes.

Classificatie	Copyright ©	Pagina
Vertrouwelijk	Safeguard B.V.	Pagina 30 van 32

- To identify the most significant risks, our organization conducts a Data Privacy Impact Assessment (DPIA). Based on the risks identified, technical and organizational measures are taken to mitigate those risks.
- In cases where our organization acts as the data controller, data processing agreements are concluded with processors. The processing agreement describes the purpose, nature, scope, duration, and technical and organizational measures.
- We manage data breaches in a demonstrable manner through an established workflow. Depending on the impact of the data breach, notifications are made to the supervisory authority and affected individuals.
- The rights that data subjects can exercise are described in the privacy statement on our website. The statement also describes the process for submitting requests. Our organization has established an internal process for handling requests adequately. Data subjects can request access, rectification, erasure, restriction of processing, data portability, and object to processing.
- Our employees are aware of the personal data they process and act accordingly. The code of conduct for privacy and information security is the guiding principle.
- Our organization has appointed a Data Protection Officer (DPO). The DPO ensures that personal data is processed and protected in compliance with the requirements of the GDPR. The DPO also collaborates with the supervisory authority if requested and, if necessary, fulfills the rights of data subjects. A complete overview of the responsibilities and powers of the DPO is provided in the job description.
- We apply the Privacy by Design principle when designing and developing mechanisms for processing personal data, taking into account the privacy of data subjects as much as possible. Furthermore, we limit the processing of personal data to what is necessary to achieve our objectives and for which there is a legal basis.
- Privacy by Default is applied to all systems, using specific rights for an employee based on their role. All default settings are chosen to maximize privacy.
- When designing and maintaining policies for the protection of PII, applicable PII laws and regulations will be taken into account.

Policy points for information security and privacy have been translated into a practical code of conduct for our employees.

Classificatie	Copyright ©	Pagina
Vertrouwelijk	Safeguard B.V.	Pagina 31 van 32