Document ID: E4	Document name: Information Security Procedures
Version: 0.7	Owner: CISO
Date: 15-08-2025	Classification: Confidential

LOGO

[COMPANY LOGO]

Information Security internal procedures

[ORGANIZATION]
Version: [MONTH] 2025 [VERSION]
Approved by management: NOT YET APPROVED

Table of contents

Introduction

This template was created by the people of ICT Institute. You can find the latest version and other templates here: https://ictinstitute.nl/free-templates/

Background

Information security is extremely important for our organization, in order to avoid fraud, business interruption or loss of data. Management has decided to adopt an information security policy with a number of important measures. Some of these measures apply to all staff and are described in the staff guidelines. Other measures are relevant for specific security roles. These measures are described in this document. This document describes per measure what needs to be done and who is responsible. For each measure, a responsible person and optionally a backup is indicated.

This document is part of our Information Security Management System (ISMS), an integral approach to information security.

This document has been set up as a central place where all procedures can be found. Everyone who performs a procedure must therefore be able to access this document. These are e.g. department heads, IT staff and also HR or administrative staff. This document may be freely distributed within our organization. It is not intended for external parties.

This document is revised at least once a year. The information security team keeps a working version with improvement proposals. In the management review, this new version is presented to and approved by management. This document is then distributed to all concerned.

This document follows the chapter structure of the ISO 27001. First the main structure is defined. Then the control measures are defined based on the annex of the standard. This annex is numbered from A5 to A8.

ISMS High level structure

Context of the organization (4)

Context and scope

This is documented in the InfoSec Policy.

Issues and stakeholders

The organization annually identifies internal and external issues and records them in a register. The stakeholders and their requirements and expectations are also determined, and whether these requirements and expectations are met through the ISMS. This is input for the risk management process.

Leadership (5)

Top management shows leadership and commitment to the ISMS. This is done, among other things, by:

- Taking final responsibility for the ISMS
- Ensuring that policies and objectives are established
- Ensuring that ISMS requirements are integrated into the organization
- Ensuring sufficient manpower and resources
- Communicating the importance of the ISMS
- Ensuring goals are met
- Active participation in training and consultation of the ISMS
- Participating in the management review
- Promoting continuous improvement
- Supporting the managers to show their leadership within their areas of responsibility

Top management has established the InfoSec Policy and ensures that it is appropriate for the organization, contains objectives or a framework for setting objectives, and a commitment to comply with requirements and to continuously improve.

Top management also sets objectives including the designated resources, deadline and responsible and communication. These are often linked to KPIs that are used in monitoring.

Top management also designates roles and responsibilities for information security. These are laid down in this procedure document, section 5.2.

Planning (6)

The InfoSec team uses a continuous improvement methodology. Using this methodology, the team is aware of the business goals, defines actions, checks whether the actions are effective and makes changes if necessary. The chosen method is Plan-Do-Check-Act, a well-known method that is also known as the Deming cycle (https://en.wikipedia.org/wiki/PDCA).

To identify and address risks, we use a risk management methodology that classifies risks based on their impact and likelihood. The risk overview also contains a treatment plan, consisting of control measures for significant risks.

Any changes to the ISMS are planned in advance. The IS team or security officer creates a change plan. Any changed documents must be quality checked and approved by the document owner.

Support (7)

Top management makes resources available to achieve the ISMS objectives. This is evidenced, among other things, by the defined roles and all measures described in this procedure document.

A recurring awareness training is included in the annual planning. New employees also receive appropriate awareness training.

The InfoSec team has regular meetings for this (see annual planning). The following is discussed during these meetings:

- **Incidents**: Have there been any recent incidents and are appropriate actions planned?
- **Changes**: Are there any new projects, changes or contracts that the InfoSec team should be looking at?
- **Annual planning**: What activities are planned for the past month in the annual planning? Have these been planned and executed?
- **Monitoring and measuring**: Are there any objectives or KPIs that need to be evaluated from last month or in the next month? What are the results?
- **Nonconformities**: Are there any new nonconformities? Are corrective actions properly implemented on audit findings or other non-conformities?

Documentation management: All ISMS documents are stored digitally in a way that they are accessible to the people who need to access them. All documents have a version, owner and date.

Operation (8)

Our organization has an InfoSec Team that monitors the implementation of ISMS actions and ensures that objectives are achieved. This is done by:

- Drawing up and follow annual planning
- Keeping track of information security objectives
- Discussing current actions and matters in the InfoSec team meeting.

During the meetings, it is discussed whether things are going well and, if necessary, measures are taken.

Performance evaluation (9)

Monitoring and measurement

There is a document “Objectives and monitoring”, that records the objectives and also what is being measured, including how often and by whom.

Internal audit

(mandatory for ISO 27001, not for security verified)
[ORGANIZATION] has appointed an internal auditor who annually conducts internal audits to obtain information whether the ISMS complies with our own requirements and the requirements of ISO 27001, and whether it has been effectively implemented.

The frequency of the internal audits is annually. The criteria for each audit are compliance with the ISO 27001 norm and our own policies and procedures. The scope of the audit is defined in the audit program (additional sheet in the yearplanning). This sheet defines which parts of the standard and which departments are included in the audit.
The results of the audit are discussed in the next information security team meeting, and in the management review. The audit reports are saved for at least three years so that they are available during next audits.

Management review

[MANDATORY FOR ISO 27001, NOT FOR SECURITY VERIFIED]
The organization conducts an annual management review in which top management reviews the organization's ISMS to ensure continued suitability, adequacy and effectiveness. The following matters are discussed:

- The status of actions as a result of previous management reviews;
- Changes in external and internal topics relevant to the ISMS;
- Feedback on information security performance, including trends in:
    - Non-conformities and corrective actions;
    - Results of monitoring and measuring;
    - Audit results; and
    - Meeting information security objectives;
- Stakeholder feedback;
- Risk assessment results and the status of the risk treatment plan; and
- Opportunities for continuous improvement.

Improvement (10)

Non-conformity and corrective actions

[ORGANIZATION] records all nonconformities in a register of nonconformities and corrective measures [DOCCUMENT NAME]. The InfoSec team completes the registry and ensures that the anomaly is acted upon, assessed, root causes evaluated and corrective action taken.

Continuous improvement

Both top management and the InfoSec team make every effort to continuously improve our approach to information security.

Organizational controls (A5)

5.1 Policies for information security

We have an Information Security Policy, called [NAME DOCUMENT]. It is the main document of our ISMS that links to the procedures, InfoSec rules, statement of applicability, risk register, asset register, and incident register. It contains our ISMS's Context, Goals, Scope, a Stakeholder analysis, and information on Leadership, Risk assessment and treatment, resources, awareness, training, operations, performance evaluation, and of course our commitment to continuous improvement.

The Information Security policy and other policies are reviewed every year by the management team. If a review is needed in between, one will be done. This may be as a result of an information security incident or a major change in corporate structure or process.

5.2 Information security roles and responsibilities

The entire management is aware of the information security policy and is committed to support this effort on an ongoing basis. [ORG_REP] is the management representative who interacts directly with the security team. There is an information security team that is responsible for implementing and maintaining information security. The team consists of the following people:

1. A (Information Security Officer)
2. B
3. C

All other staff of the company is regularly updated by the information security team and is responsible for following policies and guidelines.

The information security responsibilities are as follows:

Role	Responsibility	Requirements for role
CEO / general manager	Ultimately responsible for Information Security. Establish goals and policies.	[EDUCTION?] [X] years of experience in a management role.
CISO	Maintaining the ISMS in order to conform to goals and polies. Report ISMS status to CEO.	Completed [EDUCTION]. [CERTIFICATION REQS?] Experience with InfoSec audits.
Privacy Officer	Checks compliance with GDPR and other privacy laws. Data breach and data subject request follow-up.	CIPP/E-certified, or followed other relevant privacy training.
CTO	Manages external IT-services. Access control management.	[X] year experience in a technical role.
Head of HR	Responsible for employee screening and on/off-boarding.	Completed HR eductation.

Internal auditor	Performing the annual internal audit.	Experience with InfoSec audits. Certified ISO 27001 lead auditor.
All staff	Knowing and following the InfoSec policies, rules, and procedures.	n/a

5.3 Segregation Of duties

Some assets, such as [EXAMPLE], are quite sensitive. This sensitivity is due to the fact that misuse of the asset can result in significant consequences for our company and/or clients. We prevent accidental and malign misuse of these assets by splitting the responsibility in two: [PRACTICAL SITUATION WHERE THIS IS DONE]. All activity on [SYSTEM(S)] is logged.

5.4 Management responsibilities

Management requires all employees to sign and comply with information security rules. This is done upon [ONBOARDING/CONTRACT SIGNING].

Employees must read and follow the role-relevant policies and procedures. Access to policies and procedures is provided during [ONBOARDING] and [INTRODUCTORY TRAINING].

5.5 Contact with authorities

Contact with authorities, e.g. in the case of reporting criminal behavior, is handled by management as follows:

Authority	Our contact person
Police	CEO
Tax authorities	CFO
Privacy Supervisory Authority (Autoriteit Persoonsgegevens in The Netherlands)	DPO
[NATIONAL CSIRT] (NCSC in The Netherlands for vital sector)	CISO
[SECTOR-SPECIFIC SUPERVISORY AUTHORITY]	[ROLE]
…	…

5.6 Contact with special interest groups

The security team will make sure they are up to date on security developments by following and interacting with:

- The Information Security NL security group https://www.linkedin.com/groups/13533313/
- The International Association of Privacy Professionals (https://iapp.org)
- Platform voor Informatiebeveiliging (PvIB**)**
- The National Cyber Security Center (ncsc.nl)
- Security.nl
- $(ISC)^2$ (isc2.org)
- ISACA (isaca.org)

- CompTIA (comptia.org)

5.7 Threat intelligence

Threats are possible future events with a negative impact on the organization's CIA of information.

The following sources are monitored: [CHOOSE AT LEAST 2 CATEGORIES AND 1 SOURCE EACH]:

Name	Description	Source
Advisories	Advisories from national CERT	https://advisories.ncsc.nl https://cert.europa.eu https://www.cisa.gov/news-events/cybersecurity-advisories
Trends and news	Tools, techniques, and procedures used by hackers	https://www.security.nl https://thehackernews.com
Newsletters	News and analyses	https://krebsonsecurity.com https://www.schneier.com/ Substack(s)
Vendor and tech specific	Operation and technical info	https://www.cvedetails.com https://msrc.microsoft.com

The IS team scans the sources [QUARTERLY/BEFORE IS MEETINGS] to share and discuss relevant threats, vulnerabilities and reports within the IS team.

Relevant or interesting information is shared [#CHANNEL or DISCUSSED DIRECTLY] with each other. In the event of an immediate risk, an event/incident is created and action is taken.
During the infosec meeting, interesting reports are discussed and noted in the agenda.

[ORGANIZATION] does/does not actively hunt for threats in its own infrastructure.
[IF YES, EXPLAIN HOW].

5.8 Information security in project management

For each change in organizational processes, a project plan is created. The plan must contain the following sections:

- Description of project goals
- Changes to the ISMS needed
- Security measures in the case of significant product changes
- Privacy if new personal data is collected or personal data is used in a new or different way.

[ROLE] will review all requirements, analyses and specifications.

5.9 Inventory of information and other associated assets

Our company uses many information assets that need to be protected. The ISMS list document [DOC_NAME] provides an overview of the assets used in this company. This overview has been created by management and company staff and is regularly updated. For each information asset in scope, this policy aims to assure the following security aspects:

- Confidentiality
- Integrity
- Availability

All assets in the inventory, so of the whole company if the inventory is complete, must have an owner. Thanks to asset ownership, assets are watched and taken care of through their whole lifecycle. Similar assets may be grouped and the day-to-day supervision of an asset may be left to a so-called custodian, but the owner remains responsible. Asset ownership must be approved by management.

5.10 Acceptable use of information and other associated assets

Users of the asset should be aware of the information security requirements regarding asset use, and follow them. Rules for acceptable use of assets are set out in [DOCUMENT].
Users of the assets must use proper care to use all assets responsibly in according to their classification. Confidential documents must be stored in locked cabinets.

The three types of information should be handled in the following way:

Public information:
Information that is already public may be freely shared with customers and others. The information is often even meant to be shared, such as marketing material or our normal contact information. [FURTHER EXAMPLES OF PUBLIC INFORMATION]

For internal use:
Internal documents contain information that has specific business or strategic value to us. Documents such as these procedures, working schedules, agendas, and internal phone numbers are not meant to be known and used by outsiders. [FURTHER EXAMPLES OF INTERNAL USE DOCUMENTS].

Confidential:
Confidential information should, as the name suggests, remain confidential. It has a high business, strategic, or personal value, and can cause serious harm to [ORGANIZATION] or a person if it ends up in the wrong hands. [EXTRA RULES FOR WORKING WITH CONFIDENTIAL INFORMATION]. [FURTHER EXAMPLES OF CONFIDENTIAL DOCUMENTS] If a document contains a signature of a manager (ours or of another company) or customer, the document is most likely confidential.

5.11 Return of assets

When an employee or external party may no longer access an asset due to, for example, the end of employment of agreement, they must return the asset to the [DEPARTMENT]. There should be a clear policy for this, which has to be known by all involved. Non-tangible assets important to current operations such as specific knowledge that is not yet documented should be documented and returned as such.

5.12 Classification of information

Certain information is considered to be sensitive due to e.g. monetary or legal value, and has to remain confidential while other information is less crucial. [ORGANIZATION] should have a policy in place on how to handle classified information. The accountability to classify information assets lies with its owner. To distinguish between the importance of different classified assets, the following classification of assets is made:

- Public
- Internal use
- Confidential

If you are not sure into which category a document or asset falls, ask your manager! We would rather have the same question several times than an internal or confidential document made public.

5.13 Labelling of information

[ORGANIZATION] labels information in accordance to their classification when needed. Unlabeled information is for internal use only.

In the case that medical data, or other sensitive personal data is handled, all patient data must be labelled Confidential.

5.14 Information transfer

Since everyone works from the same location, there is no need for internal physical transport procedures. Information is transferred electronically as much as possible, using [SOFTWARE]. Information transfer methods are agreed with individual clients where necessary and form part of the project plan.

Information transfers are setup with clients when necessary. [METHOD] is preferred, but other methods may be used following discussion with client.

The following type of messaging is allowed at [ORGANIZATION]:

1. TYPE A
2. B
3. C
4. n

5.15 Access control

People gain access from management based on role, following the least-privilege principle.

[ORGANIZATION] has a matrix that describes what access is needed for what role. This is reviewed by management yearly.

Guests are not allowed on the [ORGANIZATION] network. There is a separate [BUILDING] (building) network.

5.16 Identity management

The HR responsible is updated by the rest of the management team about changes in HR, and creates user accounts when a new employee onboards. After an employee leaves occupation, the HR responsible deactivates the user account and deletes it when all valuable information has been transferred and secured.

5.17 Authentication information

Generated passwords must be securely generated and confirm to best practices. The access control responsible is responsible for checking whether all systems have access control enabled (e.g. pin, biometrics or password) and demanding that access control is enabled. Two factor authentication is used whenever possible. It must be used for [SOFTWARE].

Password and PIN (personal identification number) security is an important aspect of all security. For all work-related passwords, employees must follow the following rules:

- For each service, employees must choose a fresh password not used before or for any other service
- Passwords should not be easy to guess, so no names, birthdays or common words, and no passwords of less than 8 characters.
- Passwords must be changed at least once a year.
- Personal passwords and accounts cannot be shared with anyone else.
- Employees need to store their passwords in a secure way, e.g. using a password manager. [ORGANIZATION] selected [PASSWORD_MANAGER] for shared information. Employees can ask their security officer for more information about how to install and use [PASSWORD_MANAGER]. Use of alternative services such as [OTHER_SERVICE] is accepted.
- Employees are not allowed to leave passwords visible in the workplace. If devices such as mobile devices have the option of setting a PIN for device access, it is mandatory to set a PIN of at least 6 digits.

The same rules that apply to passwords (fresh, not visible) apply to PINs.

[ORGANIZATION] uses the [PASSWORD_MANAGER] password management system.

5.18 Access rights

The HR responsible modifies or retracts access rights within one week after a person leaves or changes roles. A list of access rights revoked is included in the offboarding checklist. In case of shared passwords, passwords are actively changed.

Asset owners regularly review who may access their asset, and role changing or leaving trigger an access rights review by management, for instance in [SERVICE], [SOFTWARE]. Platform admin rights are reviewed in the quarterly review.

Once a contract or agreement has been terminated, the access rights of the receiving party are removed. If complete removal is not needed due to a continuation of some sort, the rights may be changed instead of removed.

5.19 Information security in supplier relationships

We maintain a register of suppliers, which includes our information security requirements, relevant documentation and contact details. All new suppliers are added to the register, and the register is reviewed once per year.

5.20 Addressing information security within supplier agreements

We make sure information security is addressed in agreements with suppliers. This is done via ISO 27001, a data processing agreement or another agreement depending on the size of the company.

5.21 Managing information security in the information and communication technology (ICT) supply chain

We determine the relevant information security requirements for our suppliers. For business critical suppliers, we required evidence of ISO27001 compliance, which ensures the supply chain is secure.

5.22 Monitoring, review and change management of supplier services

We review supplier information security certification for all relevant suppliers once per year. We also monitor business critical metrics such as service uptime and review this as part of our [WEEKLY/MONTHLY/QUARTERLY] information security team meeting.

We review suppliers once per year. If suppliers do not meet our security requirements, we will investigate alternative providers. In the case of changes supplier agreements or services providers, new services will be implemented following analysis and assessment by asset owner and management.

5.23 Information security for use of cloud services

[ORGANIZATION] uses several cloud services. The most important ones are as follows:

Software as a Service (**SaaS**): [LIST]

Platform as a Service (**PaaS**): [LIST]

Infrastructure as a Service (**IaaS**): [LIST]

Our full list of cloud services can be found in the asset register. All cloud service providers are documented in the [supplier overview register].

Before entering into contract with a new cloud service provider, the security officer checks whether the contract conforms to [ORGANIZATION's] security requirements.

Acquisition requirements:

- EU/EEA based
- Support of MFA/the [ORGANIZATION] password policy can be followed

- If personal data is processed, a valid Data Processing Agreement (DPA) is signed
- The supplier is ISO 27001-certified or similar (e.g. SOC 2)
- Best practices for encryption at rest and in transit/[ACCORDING TO OUR POLICY]
- Single Sign-On (SSO) integration is possible
- …

Use and management:

- Employees authorized to use the service have their own account
- Two admin roles are assigned [OPTIONAL: and admins track costs]
- Admins review logs / get release notes
- …

Exit:

- For supplier [SUPPLIER1, SUPPLIER2], external backups and/or exports are available
- Return of data clause in contract
- …

Exceptions to these requirements can be accepted by the asset owner. They will document this as a risk in the risk register.

5.24 Information security incident management planning and preparation

A data breach is any event in which personal data is potentially lost or leaked to the outside world. Any such incident must be investigated and potentially be reported to the Autoriteit Persoonsgegevens (AP) and the subjects that are affected.
Other staff must inform the responsible of any (suspected) data breach and support investigations.

5.25 Assessment and decision on information security events

The person responsible for this control must study the official AP guidelines and do the reporting.

5.26 Response to information security incidents

See appendix 0 for the full procedure.

5.27 Learning from information security incidents

All major incidents are discussed by the information security team. They will determine root causes and suggest additional measures.

5.28 Collection of evidence

Technical staff will store a description of security incidents (logs, screenshots). For major incidents, log files are securely stored for later analysis.

5.29 Information security during disruption

[ORGANIZATION] strives to keep a similar level of information Confidentiality and Integrity in case of an Availability incident.
The building has an evacuation plan is case of fire.

We have a business continuity plan which security analyses several risk scenarios and defines business continuity objectives, among which, maintaining the standard level of information. In the majority of cases, the use of cloud services and remote working ensures that the business can continue with an appropriate information security level.

5.30 ICT readiness for business continuity

We perform a backup restore annually to test our systems. Our employees regularly work remotely therefore we are confident that unavailability of the physical office does not present a threat to business continuity.

Major continuity risks are managed by the use of a cloud-based architecture. Backups are placed outside [NORMAL_STORAGE_LOCATION] in case of a [NORMAL_STORAGE_LOCATION] disruption.

[IN CASE APPLIES]
We implement additional protections against [SPECIFC CASE, E.G. RANSOMWARE] by means of [MEANS, E.G., LOCAL BACKUP ON NAS].

5.31 Legal, statutory, regulatory and contractual requirements

We have an oversight document of all relevant legislation and contractual requirements. If we somehow happen to receive a third-party claim involving the data of or collaboration with a client, we will inform that client within 30 days from the date we became aware of the claim. [ORGANIZATION] has a liability insurance ([INSURER]).

In some countries, the use of cryptography is restricted. [ORGANIZATION] [ROLE] will check which rules apply before travelling outside the EU. Our employees do not travel outside the EU for business, however if needed, a clean empty device will be provided.

5.32 Intellectual property rights

[ORGANIZATION] respects intellectual property. Staff must validate if an asset can be used before using it. No use may be made of illegal software or software without a valid license.

Texts and images are subject to copyright, and we are not allowed to use all texts and images just like that. The following is allowed:

- You may quote 1-2 sentences at a time with source reference (name of document or URL). No permission is required for this. A screenshot of a website you are discussing is also allowed.
- You may use images from creative commons sources such as Noun Project, Unsplash, or Wikimedia Commons. State the maker's name on the same page or at the back of the document. Other images from the Internet are not allowed.
- For photos with recognizable people, you need permission from the person. The easiest is not to use photos where people are recognizable.

5.33 Protection of records

Import assets are stored under version control. [CLOUD] provider also provides backups and version control.

5.34 Privacy and protection of personal identifiable information (PII)

Personally identifiable information (PII), also known as Personal Data, should be handled with the utmost care. Example of PII are social security numbers, email addresses and names. This leads to the following rules:

- Limit the distribution and storage of PII as much as possible
- When sending PII, notify the receiver of the intended use. For example, working in HR, when sending a CV of a possible new hire, explicitly mention that the person can use it for the job interview and needs to delete it afterwards. Mention that they cannot forward the CV and should ask you for more information if they need it.
- Only use trusted systems for the distribution and storage of PII.
- Delete the information securely, so remove the file from the system and also the 'trash folder'.

If it is contractually agreed, then customer data is stored in a separate database. This is typically done for publishing houses.

We have a data processing register and have data processing agreements in place. Our privacy policy is published on our website.

There is a procedure in place for reporting a data leak to the AP and informing subjects.

5.35 Independent review of information security

An internal information security audit will be conducted once per year by an independent member of staff/external consultant to check the working of the ISMS complies with ISO27001 and/or NEN7510. This will be followed by a management meeting to discuss the results.

5.36 Compliance with policies, rules and standards for information security

With all these security policies, standards and procedures, it is important for managers to regularly review whether the activities and/or processes they are responsible for are fully compliant. For this to be done correctly, they should be aware exactly which rules and requirement they need to comply with and check this.

Information systems are regularly reviewed on compliance as well. Vulnerability tests such as penetration tests are done yearly, just like pre-audits.

Clients, such as [CLIENTS] may request to (hire a party to) perform a PEN-test on parts of our system. This test may only be done with our explicit written permission and on by us appointed/approved parts of the system.

5.37 Documented operating procedures

In the case of custom developed systems, at least four types of environments must be used (development, test, acceptance and production). All changes must be tested in acceptance before moving to production.

People controls (A6)

6.1 Screening

The HR responsible is required to screen or cosign any employment contract (including temporary contracts and internship contracts) and makes sure that each contract includes compliance with the staff guidelines. The HR responsible also checks that for functions where this is appropriate that a Verklaring Omtrent Gedrag is requested or references are called. The VOG should have the following boxes ticked for the following job levels:

Job level	Boxes ticked
Intern	Informatie
Entry level	…
Departement management	…
Middle management	…
Upper management	…
C-level executives	Informatie, Geld, Diensten, Zak. trans., Proces, Aanst. org.
Board members	…

During the onboarding process, the following checklist is used to make sure only suitable employees are hired, employees are provided with registered devices, the right documentation is read and signed, and they are provided with access according to the Least Privilege principle and on a need to know base according to our access policy. [LINK CHECKLIST ONBOARDING]

6.2 Terms and conditions of employment

The employees' contracts contain a link to HR procedures and our IS policy, and what role the employee fulfils in it. New employees are made aware of it, and sign for compliance to it in their contract. This way, they are familiar with all rules and procedures.

6.3 Information security awareness, education and training

[ROLE] also makes sure that each person receives an information security training or instruction in the first week. A security awareness training is organized at least once a year and you should attend such a training in the first week of working at this organization, and at least once a year. The training is mandatory for all staff handling information. If employees have not received any training, they must contact the information security officer.

6.4 Disciplinary process

Failure to follow these guidelines will lead to disciplinary measures such as formal warnings, suspension or being fired. [ORGANIZATION] does this on a case-by-case basis.

6.5 Responsibilities after termination or change of employment

When employees leave the company (e.g. end of contract or end of employment), they must do the following:

- Hand in all devices and information carriers from company.

- Hand in all documents containing confidential data (or dispose of these in a secure way).
- Erase all company data from private devices they have used during their employment.

The HR responsible makes sure:

- The user account is disabled and marked for deletion
- Any external and internal forwarding of emails is deleted
- External SaaS accounts are suspended or handed over

Even after the end of the contract, employees are still bound to keep information secure: they may not disclose any sensitive or confidential data to outsiders after departure from the company.

When an employee changes job responsibilities, the HR responsible makes sure the following is done:

- The VOG categories are re-evaluated and, if needed, updated
- Access permissions are updated following the access policy, taking Least Privilege and Need to Know into account
- Keys are handed in and/or extra keys are given to the employee
- The access area of the tag (access fob) are updated

For every end of employment and internal change in employment, the checklist ([CHECKLIST OFFBOARDING AND SWITCH]) is filled out by the HR responsible.

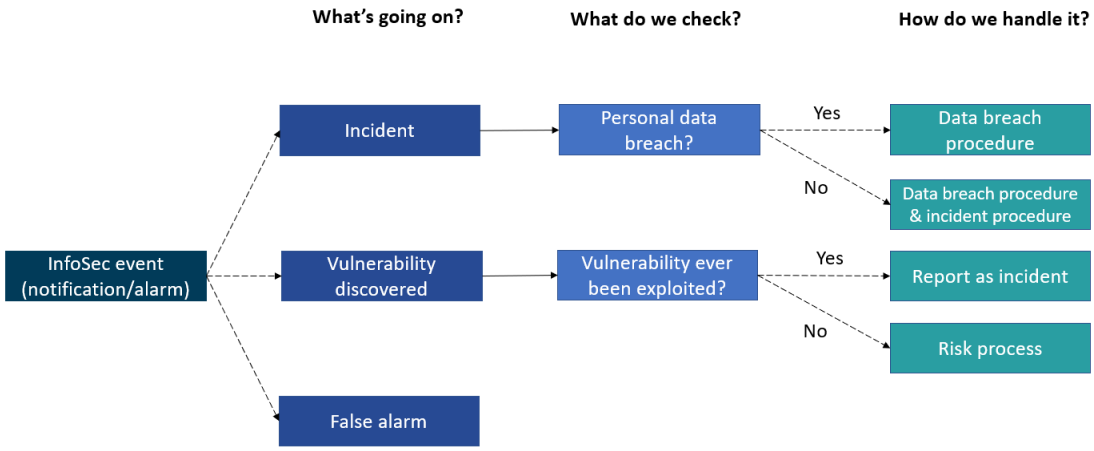
6.6 Confidentiality or non-disclosure agreements

By contract, [ORGANIZATION] employees are bound to confidentiality. This is also the case for part-time contracts, interns, and freelancers.

6.7 Remote working

Employees must only use known and secure networks. When working in public spaces, they should explicitly check the network they are connected to. A known network is the company network or one's home network. If on public networks, only TLS-secured websites can be used.

6.8 Information security event reporting



Our definitions are as follows:
InfoSec event: An identifiable occurrence (with time and date) that is related to information security.
Incident: An event where the C, I, and/or A of an information asset is violated.
Vulnerability: weakness of an asset or control that can be exploited by one or more threats.

If employees have good reason to believe an incident has occurred, they should report the incident **immediately** to the information security officer. In many cases, the company is obliged to immediately investigate and report incidents to customers or the authorities. The company can only do this if staff is alert. When the information security officer cannot be reached, report the incident to other information security members or to management. When in doubt, employees always need to report the incident.

A vulnerability should also be reported but is less urgent. They need to be reported on the same day or next day to the information security officer or to the infosec team via email. They will analyze the vulnerability and resolve it. If employees are unsure whether something is a vulnerability, they can still report it as a potential vulnerability and the info-sec team will determine if it is a vulnerability and what action is needed.

Physical controls (A7)

7.1 Physical security perimeters

In the map shown below, you see our office building. On the map we have indicated the different security 'zones':

- Green: accessible to staff and visitors. No sensitive information should be left in these areas
- Yellow: only accessible to our own staff.
- Red: Storage area/location for sensitive assets/information. These rooms/areas should be locked when not supervised.

[Insert plan of business area]

Details in physical security: *(example)*
Within the office, there is a locked cupboard for sensitive documents and stored IT equipment.
The servers and network equipment are in a secure room accessed from within the office,
All data and code are stored on the cloud. Internet access is provided by the building facilities service. [ORGANIZATION] therefore has no servers or communication equipment that require extra security.
The office is located within a building which has a reception and physical security is managed by building services: Out-of-hours access is controlled by keycards and the building is patrolled by security staff.

7.2 Physical entry

Secure areas are locked off from common areas, and the access to them are authorized and documented. Non-personnel such as visitors are accompanied, and their identity is authenticated

To avoid any (accidental) unauthorized access to other parts of the organization, the delivery takes place at the front desk or to employees' home address.

7.3 Securing offices, rooms and facilities

Each security zone must have physical protection in place, in the form of a physical or electronic lock. The person that is the last one leaving the office needs to be sure to always check that:

- all windows are closed
- the door is locked
- the alarm is on
- all electronic devices are turned off
- The secured cabinet has two keys, held by [MANAGER] and [MANAGER].
- The servers and network equipment are accessible only to [TECHNICAL STAFF/MANAGEMENT].

7.4 Physical security monitoring

The building [ORGANIZATION] is situated in, is monitored 24/7 with a CCTV system by the building owner. From 23.00 – 06.00, the front door is locked and the building is protected using a motion-sensor based alarm system. There is a clause in the rental contract with [BUILDING OWNER] stating that [ROLE] will be informed in case of an incident related to our office space.

7.5 Protecting against physical and environmental threats

[ORGANIZATION] considers the risk of external and environmental threats to be low. All of our data are stored in the cloud and can be access remotely should the physical office be unavailable. All employees have the necessary equipment for homeworking.

7.6 Working in secure areas

The secure area in [ORGANIZATION] is the locked cabinet. It is unlabeled and access is limited to management.

The network system and servers are in a secure room, accessed only by [MANAGER].

7.7 Clear desk and clear screen

When leaving the office, all documents must be removed from desks and stored in a non-visible way. Confidential documents must be stored in locked drawers or filing cabinets.

- Computers and phones must have a screensaver with a password or similar security measure (e.g. fingerprint reader). Employees must always lock devices when leaving them unattended.
- Screens need to be clear of company information (also no notifications popping up) when shown to people outside of the company, e.g. hooked up to an external projector. Virtual desktops need to be clean of documents.
- Sensitive data should never be viewed in a public place or open office space.

7.8 Equipment siting and protection

The office is locked when empty. Employees may not leave computer equipment or documents out in the office overnight. All equipment and documents must be locked in the secure cabinet.

Security for data and processing equipment is outsourced to our Cloud provider.

No paper or other material is stored in the server room due to fire risk. There is an appropriate fire extinguisher for electrical equipment.

7.9 Security of assets off-premises

Equipment and assets should be properly secured, looked after, and protected.

Devices must have appropriate covers and be transported in suitable bags. They should never be left unattended in public places or in vehicles. All devices must be transported in cabin baggage on airplanes.

7.10 Storage media

Company data may not be stored on USB-sticks. Removable media can only be used with explicit permission given by the security officer.

When media is no longer needed, it is properly disposed of to prevent leakage. To make sure nothing gets lost, we document the disposal of media. Sensitive media is disposed of with extra care by the information security team. Cloud media is sanitized by the cloud provider as described in their terms and conditions.

Media are not to be transported physically.

All of our digital assets are stored in the cloud. The only physical assets are laptops and smartphones. Employees are authorized to use these in any appropriate setting, provided remote working and device protection procedures are followed.

7.11 Supporting utilities

Supporting utilities are provided and maintained by the building services, who are responsible for inspection and testing. In the event of failures, employees can work remotely.

7.12 Cabling security

Cabling is maintained by the building facilities services and internet service provider. Management of cabling for the Cloud data centers is outsourced to our Cloud provider.

7.13 Equipment maintenance

The only equipment used by the company is laptops and smartphones. These are updated regularly to ensure the latest operating system is in use. If maintenance is required, a authorized repair shop for the device brand will be used.

7.14 Secure disposal or re-use of equipment

Media carriers might be re-used at some point, but it is important to properly control this process. The medium could have contained classified contents, which should be made non-retrievable by overwriting it. When overwriting cannot be done securely, the medium should not be re-used and might have to be physically destroyed after overwriting. Wiped media are stored in the locked cupboard in the office prior to re-use.

Technological controls (A8)

8.1 User endpoint devices

Many people have their own personal laptops, tablets and smartphones and use these for sharing information. It is technically possible to use these devices for work-related matters, but this poses severe security risks. [ORGANIZATION] therefore asks its employees:

- If they have a company email account, not to use their personal email account for work-related emails.
- To make sure any device is from a respectable manufacturer, password-protected, free from malware and viruses and updated regularly. This is for their own protection and as an extra precaution in case work related information does leak to a personal device.

Equipment is not always in use and is therefore properly protected in those cases. Log-in sessions are automatically terminated after a short period of inactivity, and personnel should manually log out after sessions. User equipment should never be left unattended in public places.

8.2 Privileged access rights

Admin access and other unrestricted access (e.g. database passwords) is only given to a very limited set of active administrators who have received additional instructions. These are reserved for platform administrators or IT administrators. One can review in the platform database who is platform admin.
Other users are only provided with regular, non-admin accounts.

8.3 Information access restriction

[ORGANIZATION] has an access rights policy that states access to certain systems, assets or information should be limited. These access rights are in practice restricted in exactly that way. Access is reviewed in the quarterly review.

8.4 Access to source code

All source code is stored in [STORAGE_SOFTWARE]. Source code of internal applications can by no means be accessible to unauthorized personnel, and personnel authorization is reviewed regularly.

8.5 Secure authentication

The access rights policy states that access to systems is secured, and how users can log on.

8.6 Capacity management

We use the following system to monitor the use of computing power and storage:

- [EXAMPLE TOOL]

This is done by the [ROLE OF RESPONSIBLE PERSON/TEAM]

Alerts are managed by [REPORTING/ALERTING TOOL].

[IN CASE] Automatic scaling is configured for flexible capacity.

[ALTERNATIVELY]

There is no automated capacity management. Infrastructure is scaled with future growth in mind and is reviewed by [ROLE] regularly.

8.7 Protection against malware

All computers (servers, PCs and laptops) must be equipped with a regularly updated virus scanner and a firewall. If possible, users should be prevented from switching off scanners, firewalls or make other security changes. This is recorded using [Bitlocker/manually checked by management.]

8.8 Management of technical vulnerabilities

At least annually an architecture review takes place, identifying all versions of major software components. It is validated that all versions are still supported and either the most recent or second most recent version.

Information systems are regularly reviewed on compliance as well. Vulnerability tests such as penetration tests are done yearly, just like pre-audits.

Clients, such as [CLIENTS] may request to (hire a party to) perform a PEN-test on parts of our system. This test may only be done with our explicit written permission and on by us appointed/approved parts of the system.

8.9 Configuration management

Since standard configuration of systems, devices, and software often do not conform to the "security by default" principle, [ORGANIZATION] performs a configuration check for all new systems, devices, networking equipment, and software.

Where possible, the following baseline is followed:

- Disabling unnecessary features/ports/accounts
- Restricting access to administrator features for non-admin users
- Changing default passwords
- …

For assets processing Confidential information, the CIS benchmarks are used.

Once an initial safe configuration is made, a back-up of this configuration is made. This back-up is tested annually.

8.10 Information deletion

When information has served its purpose, it is deleted by the asset owner. The retention requirements for personal data are documented in the Register of processing activities. Other information is retained according to the following retention policy:

Information	Retained for
Standard log data	Three months
Admin log data	Twelve months
Standard back-ups	Three months
Confidential back-ups	Eighteen months
…	…

8.11 Data masking

[ORGANIZATION] limits the exposure of sensitive information using several data masking techniques. The following techniques and principles are applied:

- **Anonymization:** wherever possible, personal data are made anonymous by removing identifiers that cause the data to be linked to an individual. For example: removing name, email and contact details when performing analysis on user data.
- **Pseudonymization:** if anonymization is not an option, since the connection to an individual person cannot be severed, pseudonyms are to be used. This is, e.g., done using User ID's instead of usernames and email addresses.
- **Access control:** all employees follow the access control policy to prevent internal unauthorized access to information.
- **Encryption:** data are encrypted in rest and in transit according to our encryption standard.
- **Password hashing:** all our systems and software store and transmit passwords in hashed format. No plain text passwords are stored nor transmitted.
- **…:** …
-

8.12 Data leakage prevention

[ORGANIZATION] has both technical and organizational procedures in place to prevent data leakage:

Technical:

- Microsoft DLP
- ZIVVER
- Watermarking of files
- Firewall-level traffic inspection (volume, traffic, and content)
- USB-drive blockers
- Monitoring and alerting on admin activities
- …

Organizational:

- NDA in place with employees
- NDA's with contractors and suppliers
- …

8.13 Information backup

[ORGANIZATION] takes care of adequate back-up and restore services to ensure availability of the service and data. The data is stored in a database and is stored for as long as the client remains client of [ORGANIZATION]. A daily back up is made with which the application can be restored up to [AMOUNT] days in the past on a daily basis.

The back-up procedures are tested annually on correctness and completeness of data storage, correctness of procedures and needed recovery time in the event of an incident.

8.14 Redundancy of information processing facilities

We rely om the availability of [STORAGE_SOFTWARE]. Security and availability of processing facilities are managed by [CLOUD] and their information security policies meet our requirements. They provide a flexible service allowing us to increase availability if necessary.

8.15 Logging

Logging of events must be enabled for all servers. Events to be logged include failed log-in attempts, upgrades of access rights, creation of accounts, access to log files, access to sensitive information and all changes/deletions. [SOFTWARE] is used for logging.
The logs must be stored securely, protected against tampering and have alerts/notifications set for irregular activity. The logs are stored at least one year in order to allow for investigations.

Privileged accounts such as admin or operator accounts have access to logs, so it is important to restrict their access to the logs of their own activity. To retain the integrity of privileged account logs, another logging system that cannot be accessed by the privileged individuals is put in place.

8.16 Monitoring activities

[OPTION 1 AUTOMATED CENTRAL MONITORING]
All logs from software, endpoints, networking hardware and our IAM-solution are sent to [SYSTEM]. Logs are analysed for use cases and anomalies. The following use cases alert [ROLES]:

- Large data transfers
- Incorrect password more than three times in a row
- Log-in attempt from outside the EU
- …

[OPTION 2 MANUAL DISTRIBUTED MONITORING]
All used software, endpoints, networking hardware, and our IAM-solution produce logs. [ROLE] inspects these logs [PERIOD] for the following use cases:

- Large data transfers
- Incorrect password more than three times in a row
- Log-in attempt from outside the EU
- …

8.17 Clock synchronization

All servers must have a time synchronization service installed so that log files contain accurate timing information. This is handled by [SYSTEM], which is synchronized to [INTERNAL/EXTERNAL NTP SERVER]

8.18 Use of privileged utility programs

Programs that provide privileged access to assets or systems are controlled tightly. Due to the possibilities to override controls and access part of a system that could affect the performance, their use is as limited as possible.

8.19 Installation of software on operational systems

Installation of software on operational systems is controlled. There is a documented procedure of how software is checked before installation, and who installs/updates/deletes the software and how. Installing, updating, or deleting software without assessing the impact on the operational environment may have negative outcomes.
Server installation is automated as much as possible to minimize user errors.

Important: Software updates are scheduled [TIME_PERIOD].

[ORGANIZATION] does not restrict the access of users. They can install software themselves. Employees may not install leisure software. Employees must also verify the source of software and avoid high-risk downloads. This is covered in the information security training.

8.20 Networks security

All networks must have security measures in place to protect against tampering and eavesdropping. [BUILDING SEVICES/NETWORK MANAGER] is responsible for managing the network. The router is password protected and only [BUILDING SEVICES/NETWORK MANAGER] can make changes to settings.

8.21 Security of network services

The WiFi networks have password protection and a firewall. The following firewall rules are applied:

- [RULE 1]
- [RULE 2]
- Etc.

[FOR CLOUD-BASED NETWORKS]
The network protections of cloud-based environments are implemented by means of:

- Secure communications
  - VPN connections from on-premises to cloud connections
  - Software-Defined WAN (e.g., Cisco, PaloAlto) [LARGE COMPANIES]
  - TLS 1.3 at load balancers [IF ANY] and at service-to-service communication
- Access control with
  - Zero Trust model with Identity provider (Azure AD), endpoint management (Intune) and risk-based access control
  - Risk-based access control /Identity-aware networking (e.g., Google IAP, Azure AD Application Proxy, Zscaler)
  - MFA required for all administrative access
- Configuration management with
  - Security policies (e.g., Security Groups on AWS)
  - Automated configuration checks (e.g., AWS Security Hub, Azure Defender for Cloud, GCP Security Command Center)
- Monitoring
  - Cloud-native logging tools (AWS Flow logs, Azure Network Watcher, GCP Flow logs)
  - Cloud IDS tools (AWS GuardDuty, Azure Sentinel, GCP Cloud IDS)

Service requirements and agreements are addressed in sections 5.19 - 5.21.

8.22 Segregation in networks

There is a separate guest network, namely [SSID NETWORK]. Guests and other visitors are only allowed to connect to this network. Employees are only allowed to use the main network [SSID NETWORK]. The two networks are separate. Passwords are changed annually.

[FOR CLOUD-BASED NETWORKS]
Cloud-specific security policies (e.g., Security Groups) control inbound/outbound traffic between public and internal Virtual Private Cloud (VPC), and between internal sub-networks in VPCs, such as development, staging and production environments. Private endpoints are used for service-to-service communication, such as storage and databases.

[COMPANY] has the following virtual networks in the cloud:
- Network 1
- Network 2

A schematic representation of the network architecture can be found here: [LINK DIAGRAM].

8.23 Web filtering

[ORGANIZATION] blocks access to certain websites to maintain a professional and secure environment. The current content is blocked by default:

- Websites
  - containing violence
  - adult content
  - Gambling
  - Torrenting, pirate and illegal content
- Known malicious websites, phishing URLs
- Command and Control servers, Malvertising
- …

Blocking is done on the network level in our [LOCATION] office and on [ORGANIZATION] devices at device level. Should your job require you to access to blocked content, request an exception to your manager. [ROLE] is responsible for creating exceptions and maintaining an overview.

8.24 Use of cryptography

Since some information has to remain confidential to those not entrusted with it and keep its integrity/authenticity, it has to be encrypted. For these types of situations, the cryptography control policy is in place. In this policy is stated when cryptographic controls are needed and what types fit what situations.

The following encryption is mandatory:

- Use of https for all web traffic (TLS version 1.2 or above)
- All servers must score at least A in SSL labs: https://www.ssllabs.com
- For email security, a check is made regularly with https://internet.nl
- Databases (except with public content) are encrypted with an algorithm + key combination that creates a sufficiently strong work function

- Planned improvement: [PLANNED_IMPROVEMENT]
- Passwords are stored in hashed format and salted. Only currently secure and collision-resistant algorithms are used. (e.g. no MD5)

All data must be encrypted at rest and in transit.

Passwords and other keys must be stored securely in a password manager or in a secure place. To prevent loss, make sure each key is accessible to at least two people.

Keys and password must be generated via a program designed for secure key generation.

Shared keys are changed at least annually, and more often when key staff leaves.

8.25 Secure development lifecycle

[IN CASE ORGANIZATION DEVELOPS SOFTWARE/FROM SUPPLIER]
Our agile development process includes the requirements, design, implementation, verification and release phases. Specifically:

- **Requirements**: The requirements for each change are documented as tickets / stories on [YOUR BORAD, E.G., JIRA/ASAN/TRELLO/SLACK], and contain acceptance criteria. Where applicable, the acceptance criteria include security requirements, such as role based access restrictions, how incorrect input is handled or checks to ensure data integrity. The product owner checks the acceptance criteria when approving the ticket/story.
- **Design**: When needed, the lead developer / CTO creates a design and has it peer reviewed by another developer / architect to make sure it preserves security. This includes checking for sufficient availability/redundancy, proper data storage and ability to reach required performance and not introducing hard to maintain new technologies. During the design process the product owner also considers ‘privacy be design’ and tries to minimise the collection or display of personal information.
- **Implementation/coding**. Developers must know and apply our coding guidelines, including secure coding guidelines (See 8.28)
- **Verification/testing**: Code is checked by developers against the acceptance criteria and peer reviewed when checked in. Where possible the development pipeline is automated with automated unit tests or other defined quality gates.
- **Release**: Software is tested in a staging / acceptance first, and must be approved by the CTO or product owner before deploying to production. The release into production is done via an automated pipeline based on our change management process.

The relevant phases are documented on [YOUR BORAD, E.G., JIRA/ASAN/TRELLO/SLACK]

8.26 Application security requirements

The following requirements are specified for developing and/or acquiring applications:

- All applications that communicate using the Internet or public networks must use encrypted secure connections for data transport, using TLS.
- The web applications must use encryption that scores at least 60% on internet.nl.

- The supplier of each SaaS solution (Software as a Service application) must have a GDPR compliant privacy policy on their website. Larger vendors must have ISO 27001 or similar certification. Specifically:
    - [LIST HERE YOUR MAIN SAAS SOLUTIONS AND/OR LARGE VENDROS WITH RESPECTIVE CERTIFICATION]
    - [ALTERNATIVELY, REFERENCE THE SUPPLIER MANAGEMENT/PROJECT PLANS WITH SUCH DATA]

- Applications that are used for confidential data must offer secure authentication, preferably based on single sign on or multi factor authentication.

- Applications that are used for confidential data must have role based access, so that we can give different access rights to different roles in our organization.
    - [YOU CAN LINK HERE THE ACCESS MATRIX]

- Applications must have a well-defined test process and change process.
    - [FOR EXAMPLE] The [ORGANIZATION] has access to an acceptance environment and tests changes beforehand.
    - [ALTERNATIVELY: and/or the supplier tests all changes in their acceptance environment.]

8.27 Secure system architecture and engineering principles

The following principles for secure systems are in place:

- Standard web frameworks are used for developing web systems. [FOR EXAMPLE, Laravel for PHP or Django/Flask for Python]
- Cloud infrastructure to ensure secure hosting and scalability
- Implementation of logging of significant events through a standard logging library or service [YOU CAN LIST YOUR TOOLS]
- REST APIs to protect against data loss or replay attacks
- Securing APIs using session management
- Application of the ‘least privilege’ principle [YOU CAN REFER TO ACCESS MATRIX]
- [IF APPLICABLE] Zero trust [LIST YOUR SOLUTION/DOCUEMNTATION]
- Data encryption at rest and in transit

[IN CASE OF HARDWARE DEVICES]

- Attack surface minimization: devices are configured so that the least number of services are exposed
- Fault tolerance to detect faults and correction
- The use of security-oriented design reviews when making significant changes
- Security features are documented

[ROLE] is responsible for maintaining a secure architecture. They perform an architecture review every [PERIOD], and make sure the best-practices are applied.

8.28 Secure coding

There is a standard/guideline for secure application development such that each developer knows the importance of security and understands the OWASP top 10 vulnerabilities and how to prevent these. Developers receive regular security training (at least once per year).

Systems owners, designers and administrators are instructed on the importance of privacy and security by design. As part of the instruction, they must learn that they are responsible for the following aspects:

- Personal data cannot be collected when not needed, without cause or permission.
- Personal data must be stored securely and be protected e.g. using encryption or hashing.
- Personal data must be actively removed after use as it is not allowed to store it longer than necessary.
- In software development, we work with user stories, which define acceptance requirements. Where applicable, security is included, for example, input control, rights control, logging, and proper error messages.

All software created by [ORGANIZATION] must conform to the Secure Coding Standard [you can find in LINK TO YOUR CODING STANDARD].

[OR REPORT STANDARD HERE]
This standard is as follows:

- All pages and services must check authentication or authorisation before doing other actions.
- Input validation:
    - Test external input for reasonable size to protect against buffer overflows and denial of service attacks (Input validation)
    - Restrict the uploading of files to specific types, and change the name of files so that hackers cannot create or overwrite specific files
    - Test all user input for acceptable characters (e.g. numbers only contain numerical characters) before storing or using user input
- Parametrization:
    - SQL queries are not made by concatenating strings. You must use a secure query building method to insert parameters into queries, or use a secure database access method
- Fail secure (no revealing information in errors)
    - Do not disclose information in error messages to users.
    - Do not disclose passwords in log files
- Use a recent and supported version of all third party components or frameworks\
- Use a recent and supported version of cryptographic frameworks
- Log all significant user actions or significant events, including errors, access rights changes and admin-only actions

8.29 Security testing in development and acceptance

Security testing is executed regularly for all systems as part of the development process. At least every year, an independent, outside security firm is asked to conduct a PEN-test (penetration test) to test if any IT systems have obvious weaknesses. The findings are reported to management and used for strengthening both the systems and development and testing processes.

During development, the security of the new/updated system is also tested during regular testing.

8.30 Outsourced development

[ORGANIZATION] does not have outsourced software development.

8.31 Separation of development, test and production environments

All the development, test, acceptance and production environments are separated. All environments have authorization enabled and/or are not accessible from outside.

For all major IT systems, tests are carried out in separate test environments before and after changes or tests can be run in production.

Only developers have access to the development environment. The development environment is fully segregated from production and acceptance environments. Developers do not have unregulated access to the production environment.

Acceptance environment is accessible [IF APPLIES, for all customers or one per customer.]

[IN CASE APPLIES]
No specific controls are in place, since our risk analysis has indicated this is not a significant risk. The same security measures are in place for production and acceptance.

8.32 Change management

Any changes to and inside the organization that may affect the information security are controlled and approved by management. Such changes can, for example, be the use of a new system or change in an important business process.

The ticketing system [TICKETING_SOFTWARE] is used to document all changes. Changes are reviewed by [ROLE] before implementation and must meet the quality standards set out in our development policy.

After a change, operational systems are reviewed on their performance and security. The change might have negatively influenced the system or overall information security and/or performance.

Software packages require updates every once in a while, which can be minor or major. A procedure for updating software is in place: The major version is pinned and minor version are accepted when they become available.

8.33 Test information

Anonymized production data is used in acceptance. In test environments no production data is used. [UPDATE FOR YOUR CASE: , e.g. use made-up data in test environments and a carefully minimised and reduced copy of production data in acceptance.]

[IN CASE APPLIES]
Dummy dataset is used in testing. Screenshots based on this dataset can be safely used in bug reports or user documentation without risk of data breaches.

[IN CASE APPLIES]

Anonymised copy of production data. A dataset is anonymized by replacing full names and numbers with masked versions (e.g., Anthony becomes A****y). [CHECK IF SPECIRFIC REGULATIONS APPLY, e.g., specific regulations exist that forbid the use of customer data in acceptance environment].

8.34 Protection of information systems during audit testing

[ORGANIZATION] allows audits from customers in contractually agreed manner. Audits might require deep access to a lot of information, which should not disrupt the day-to-day activities of personnel. To ensure a smooth audit:

- All auditors must have a clear audit plan
- The audit plan must be communicated at least two weeks in advance

Appendix 0: Procedure incidents and data breaches

[ORGANIZATION] uses the following procedure for personal data breach notifications. It is based on the guidelines of the authority personal data and adjusted on the basis of the GDPR.

Report to security team

Everyone at [ORGANIZATION] has been instructed to send possible leaks, security incidents and even questions to the security team.
Suppliers have also been informed through processing agreements of their obligation to report data breaches via support@[ORGANIZATION].com
The contact details are mentioned in each training session.

Definitions

[ORGANIZATION] uses the following definitions:

A **(security) incident** is a concrete event in which the availability, confidentiality or integrity of an information asset has been violated.

A **(personal) data breach** is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Personal data is any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Handling of reports possible data leaks

The information security team is responsible for handling incidents personal data breaches. Every security incident must be reported to the security team and logged and studied by the team.

This procedure is followed for each data breach:
1. The team studies the incident and determines what happened when and where, and what equipment and parties were involved. A record is made in the register of incidents.

2. If relevant, the team takes immediate action to close or stop the leak, or encourages IT stakeholders to do so immediately.

3. The team determines the root cause, which personal data of how many and which persons are involved. As a result, the number of persons, which types of data and whether personal data of the special category is involved is recorded. Based on this, it is decided whether this is a data breach.

4. In case of data breach: The team determines who is responsible for the data. This is determined by examining how the data was obtained and by examining all data processing agreements under which the data was transmitted.

5. In case of data breach: the team determines risks: whether it can be reasonably ruled out that personal data have been processed unlawfully. This is the case, for example, with the theft of a laptop that is equipped with strong encryption.

6a. In case of data breach: If we are not the controller but the processor, notification to the controller is made in accordance with the contact details in the processing agreement. If this is not clear or not feasible, contact is made via telephone number on the website of the party. The aim is to do this within 8 business hours after discovery of the incident (or according to terms in data processing agreement).

6b. If there is a data breach and [ORGANIZATION] is the controller, the security team will do the following:

- Inform top management so that they can provide input on the assessment of the potential for serious adverse consequences. The management engages, if they wish, the help of external experts.
- Completing research and properly recording outcomes in a separate incident report.
- Report, when required, the incident via the web form to the Dutch Data Protection Authority Autoriteit Persoonsgegevens. This should, if possible, not be later than 72 hours after discovery.
- The security team assesses whether reporting to the parties involved is possible and whether a report possibly has adverse consequences for the person concerned. Note: if there is good encryption and the chance of consequences for this is minimal, notification is not required.

If it is possible to report, reporting has no disadvantages for those involved and there is no good encryption, the data breach will be reported to those involved.

All decisions about, for example, seriousness, exclusivity, reporting / not reporting are recorded in a report about the incident.
The details of the incident and the report are kept as part of the ISMS by the information security team. We store incident management data for at least three years in order to continue to evaluate and improve the ISMS.

About this template

This template was created by the people of ICT Institute. You can find the latest version and other templates here:
https://ictinstitute.nl/free-templates/