*Note: this is an example document that shows what rules have to be communicated to all staff for information security. The name of the document can be “Acceptable use policy”, “Personnel handbook” or any other name that suits the organisation. Make sure this document contains all InfoSec-related rules staff should follow, and there are no conflicts with other ISMS documentation. (e.g. Procedures).*

*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/*

*You can do the following with the templates:*
*Share. You can share the templates and any documents made with these templates freely, with any one that you want to share it with.*
*Adapt. You can make new documents based on the templates, make changes, add elements or delete elements as much as you want. You can even do this in commercial organisations of for commercial purposes.*

*If you are a customer, you do not have to mention ICT Institute anywhere. If you are not a customer, you must keep the text "create by the people of ICT Institute" somewhere*
*Note that the use of these templates is of course at your own risk. Note also that the ISO standards are copyrighted. You must buy the standard from NEN or ISO before using it*

# Information Security rules

Anyone with access to information in our organisation has an important role in keeping information secure. It does not matter if work in IT or in other parts of the business: the rules apply to all staff. The IS-rules apply to any staff working in or for our organisation. This includes:

- Permanent staff.
- Interns and temporary staff.
- [optional]Independent professionals or supplier staff with access to our premises or information.

You should receive a copy of this document with your employment contract or in your first day at work.

The scope of this document is the broad use of information and includes hardware, software and the information itself. You should follow the rules for all locations and devices you use to do your work.

Failure to follow these rules will lead to disciplinary measures such as formal warnings, suspension or being fired. More details can be obtained at HR.

## General obligation for information security

Anyone working in this organisation is obligated to keep information secure.

- You cannot disclose sensitive information to outsiders or publish information unless this is part of your role and the classification of the information allows it.

- You are obligated to know and respect all information security rules.
- You are obligated to take due care with any data, especially with personal data.
- You are obligated to take due care with company issued devices.
- You are obligated to mention security incidents immediately to …. This includes loss of a device, suspicion of a hack or any unworkable situation.

These rules have been created by the management as part of the overall information security policy. Management is fully committed to information security, and is available for any questions about these rules. You can ask questions to:

- [CEO / CFO / CIO]
- Email address:
- Phone number (general questions):
- Phone number (for emergencies such as incidents):
- Infosec team members:

## Classification of information (A5.9, A5.12)

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
- Very 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.

Please follow these instructions for handling information according to their classification.

| Classification | Examples | Where to store | When to share |
|---|---|---|---|
| Very confidential | Passwords, trade secrets | On systems explicitly designed for such information | Only when told to do so |
| Confidential | Source code, contracts, documents with personal data | Internal shares/drives | Only to people who need it in their role (ask manager when in doubt) |
| Internal use | Templates, instructions, procedures | Internal shares/drives | With colleagues |
| Public | White papers, information already published online | Internal shares/drives, website | With colleagues or other people |

You should label documents when created. Documents not labelled should be considered internal-use-only, unless it is clear from context that the information is open (e.g. brochure) or that it is confidential (contains sensitive information).

## Use of phones, tablets and other mobile devices (A8.1)

If you receive a mobile phone tablet or other device, please use this device with care to ensure that the information on this device is secure. Specifically, stick to the following rules:

- Do not disable security features on the device.
- Do not share the device with other people.
- Do not open suspicious emails.
- Do not install apps from unknown origin.
- Secure the device with a safe password/pin.
- Encrypt the storage on devices.
- (for laptops: regularly scan for viruses/malware)
- Keep software up to date, in line with recommendations from the manufacturer.
- If a device seems compromised, turn off the device and hand over to IT staff.
- If a device is lost or stolen, report this immediately to the Information security officer.

## Working from home (A6.7)

In the 'classification of 'If you work from home or an external location, you must follow the following rules:

- Do not handle personal data from our users and customers on non-company devices. Use only company devices for work.
- If you do have to use a home computer for handling company information, make sure the computer has a firewall and virus/malware scanner installed

## End of contract/employment (A6.5)

When you leave the company (e.g. end of contract or end of employment), you 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)

Even after the end of the contract, you are still bound to keep information secure: You may not disclose any sensitive or confidential data to outsiders for at least two years after departure from the company.

## Security awareness training (A6.3)

A security awareness training is organised at least once a year and you should attend such a training in the first week of working at this organisation, and at least once a year. The training is mandatory for all staff handling information. If you have not received any training, contact the information security officer.

## Using and storing passwords (A5.17)

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

- For each service, you 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.

- We recommend writing down the passwords offline (e.g. in a paper notebook) and keep this notebook out of sight when you are not present, or use a secure, encrypted password manager on your computer.
- You 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.

## Clean desk and clear screen policy (A7.7)

- When leaving the offices, 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
- Your computers and phones must have a screensaver with a password or similar security measure (e.g. fingerprint reader). You must use the screensaver when leaving the device unattended.

## Reporting incidents and vulnerabilities (A6.8)

An **information security event** is a situation where information could be compromised. You can report report any event. The security team will determine the next steps.
An **information security vulnerability** is a situation where an event could occur, but there is no indication an event has occurred. E.g. a broken window is a good reason to believe an incident has occurred. A window without a lock is a vulnerability.

If you think an event happened, you **should report this immediately** to the information security officer. In many cases, the company is obligated to immediately investigate and report incidents to customers or the authorities. The company can only do this if staff is alert.

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

## Using personally identifiable information (A5.34)

Personally identifiable information (PII) should be handled with the utmost care. Example of PII are social security numbers, email addresses, 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’.

For functions that handle PII on a daily basis, more specific procedures apply.

## Use of safe networks (A8.21)

Only use known and secure networks. When working in public spaces, explicitly check the network you're connected to. A known network is the company network or your home network. Check wireless networks explicitly on being secure.

## Bring your own device rules and use of private email accounts (A5.10)

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. We therefore ask you to:

- Not use personal devices for sharing work-related information, unless the information is public. Our security staff cannot guarantee the security of devices that they did not select or configure.
- Do not use your personal email account for work-related emails.
- Make sure any device is from a respectable manufacturer, password-protected, free from malware and viruses and updated regularly. This is for your own protection and as an extra precaution in case work-related information does leak to a personal device.

| | |
|---|---|
| Place for signature<br>*(Sign here if you have been asked to sign a version of this document as prove that you received and read these rules. You should sign one copy and keep one copy yourself)* | Name: ________________<br>Place, Date: ________________ |