Employee Handbook

Kastelo Group

2024-01-30

Contents

Kastelo Employee Handbook

This document makes up the “employee handbook”, which is mostly a collection of policies explaining how we work at Kastelo. Everyone should be familiar with these policies as they are expected to follow them. This handbook is a living document, subject to change and discussion. Please feel free to file issues and PRs in the repository.

- Working Hours & Benefits are the ground rules we abide by.
- Remote Work explains how we handle working remote.
- Our Systems list the tools and services we use.
- Mobile Access Policy defines how we use mobile devices, i.e., all our computing things.
- Information Security Policy are the principles we operate under, information security wise.
- Password Policy explains how to structure and use your passwords…
- Hardware Policy defines what hardware we use to do our job.

There’s a certain amount of “cover-our-ass”-ness in this: we need to have these policies in place, and we need to follow them, or bad things can happen legally speaking. We intend for them to mostly codify existing common sense and best practice and not be onerous in day-to-day work.

If the policies create road blocks in our daily work we need to adjust the policies, how we work, or both.

Legal Entities

If you need to fill in information about Kastelo anywhere, this is who we are.

Kastelo AB
Prästkragevägen 23
SE-236 35 Höllviken
Sweden

Swedish company registry no: 559071-2146
VAT ID: SE559071214601

Kastelo USA, Inc.
600 N Broad St, Suite 5 #3780
Middletown, DE 19709
USA

Employer Identification Number (EIN): 35-2750989

Working Hours & Benefits

Working Hours

Unless otherwise agreed in the contract, everyone is expected to work eight hours per day on average. We apply flexible work hours, but at least a few of those hours should be between 8 and 17 CET, i.e., “office hours”. Vacation days, sick days, and similar should be communicated to your manager *and* noted in Fortnox.

Vacation

We can take 25 days of paid vacation per year. Vacation is accrued during the working year, April 1 through March 31, and is available for use the following working year. Advance vacation will be available to new hires.

Vacation must be cleared with your manager ahead of time and noted in Fortnox.

Summer Hours

We work four-day work weeks (32 hours) from June 1 through August 31 every year. When a holiday occurs to reduce the week to a four-day work week or less, summer hours don’t reduce the week any further.

Health Stipend

We provide a stipend for health and sports, up to 5 000 SEK per calendar year. Inquire for details, but in principle we allow what the tax authority allows.

Car Travel

If you are required to travel using your own car we will reimburse by 5,00 SEK/km. Out of this, 2,50 SEK are tax free, 2,50 SEK will be taxed as a benefit as per 2023 rules.

Parental Pay

We provide parental pay (“föräldralön”) to cover the difference up to 90% of your normal salary, as per the terms of the Unionen collective agreement.

Remote Work

Kastelo doesn't have a central office, we are 100% remote workers. We provide your choice of hardware within our policy, and up to 10 000 SEK (excl. VAT) every three years to furnish your home office.

We do not provide for a home internet connection; we assume one exists that is adequate.

Online Presence

While working, we should generally be available on Slack. That said, we do try to be mindful of everyone's need for uninterrupted work time and will keep unnecessary interruptions to a minimum.

We encourage everyone to manage their notification settings so that:

- you get reasonably prompt notifications during work hours, and
- notifications are suspended during non-work hours.

This enables colleagues to reach you when you are available, and also enables them to leave messages in an asynchronous fashion if they are working when you don't, without disturbing you during your off-work hours.

Weekly Report

Everyone should file a short report on their work once every week. This is a bullet point summary of the past week and should include the following:

1. What did you do the past week?
2. Which problems or blockers, if any, did you run into?
3. What do you intend to work on the coming week?

Keep it short and to the point – if it takes more than five-ten minutes to compose you're most likely overthinking it. File the report in the appointed channel on Slack.

Our Systems

Azure AD / Microsoft 365

Company accounts live in Azure Active Directory. You can manage your account there, for changing password or 2FA.

Email

We use Microsoft 365 as our email provider. You can access it on the web or add it as an Exchange/IMAP account it your native email client.

Slack & Teams

We use Slack for internal chat and voice. For customer calls we use Teams.

Sharepoint

There are file shares on Sharepoint with various company-internal information, the parts of it that doesn't make sense to have in a repo on GitHub. Think financial reports and stuff like that.

GitHub

Login: Create your own account

We use GitHub for all source code and development. You should have an account, and it must have 2FA enabled. We'll add you to the Kastelo organisations so you are able to access the private repositories.

Our repositories are divided in two organisations with slightly different policies.

- github.com/kastelo for Serious Business. These are our paid customer and internal projects repos. Any public repos are relevant to our purpose and officially supported in some manner. Development is mostly structured – `main` is a protected branch, pull requests are used, etc.

- github.com/kastelo-labs where things are more relaxed. Anyone can create repositories, public or private, and this is where forks of other open source repos go. Experiments and quick hacks are welcome. No development process is enforced.

You are invited (but not required) to set your membership to public on both organisations.

Set your Git client to use your Kastelo identity:

```
git config --global user.name "First Last"
git config --global user.email "first@kastelo.net"
```

You can also do this per repo if you prefer to have a different configuration on other repositories.

Set your GitHub account to know about your Kastelo address, and to not hide your email address – it needs to be visible/available during pull requests, etc.

Issue Tracking

We use GitHub's built in issue tracker for the software projects on GitHub, as well as for this employee handbook. Though there is a Jira instance, as seen below, we don't use it for development projects.

Fortnox

Login: Fortnox account via invite, then typically BankID.

Fortnox is our bookkeeping service. It is used for salaries, so you need to report vacation days, sick days and expenses in Fortnox.

Use the web service or mobile app to add vacation and sick days as soon as possible. Every month you need to check off ("klarmarkera") the previous month to signify that any anomalies have been fully reported. This should happen no later than the first Tuesday of the following month.

You can also use the mobile app to upload receipts for any expenses, and to log trips for compensation.

Additionally, we track billable time for customer projects in Fortnox so that we can invoice for that time. If and when you are involved on time-and-materials projects for customers you need to report the amount of time worked and details on what you did. You'll be briefed on the details when it's required.

Jira

Login: Azure AD, after invite.

We use Jira to track customer support requests. If and when you get to help out with that you'll get an account and an introduction.

DocuSign

Login: DocuSign account, after invite.

We use DocuSign for electronically signing documents, both internally and with customers.

Mobile Device and Access Policy

Introduction and scope

The purpose of this policy is to provide rules and guidelines on how to access Kastelo IT-resources in a secure way, protecting Kastelo assets as well as integrity and privacy of Kastelo employees, customers and contractors.

The policy applies to all laptops or other type of mobile devices such as e.g. smartphones and tablets ("clients") used for accessing of Kastelo IT resources.

It is the personal responsibility of anyone accessing Kastelo IT-resources to comply with this policy.

General rules of usage

No equipment that connects to Kastelo networks or IT-resources, whether it be Kastelo standard equipment, personal equipment or equipment provided by another company (applies to contractors, partners, customers, etc.) may be used in a way that goes against Kastelo policy, is illegal, or otherwise unethical. This means that any equipment connecting to Kastelo networks or IT-resources may not be used for accessing, downloading, storing, transferring or in any other way relaying information that:

- is in conflict with applicable laws and regulations, e.g. incitement against ethnical groups, child pornography, slander, molestation, data breaches or copyright infringement
- can be considered political, ideological or religious propaganda
- is in conflict with personal data protection regulations such as e.g. the GDPR or is otherwise violation of personal integrity
- can of other reasons be considered offensive or objectionable
- may in any way harm the Kastelo business, associates or customers

If there is a conflict o between these rules and any rules set down by a partner or contractor organization[1] then the equipment may not be used for accessing Kastelo networks or IT -resources or for handling of Kastelo proprietary data or confidential information.

Workstations, laptops and other mobile devices

Use of Kastelo workstations and laptops and access to Kastelo resources

- You may not lend your Kastelo equipment to anyone that does not have their own Kastelo account. This includes your children, spouses, other family, contractors, partners etc.
- You are not allowed to give anyone access to Kastelo resources that doesn't have their own Kastelo account and is an approved user of Kastelo resources.
- No one but yourself is allowed to use your personal Kastelo account, and you are not allowed to reveal credentials (password and username) to shared accounts without having received explicit and documented approval to do so from your manager or the application or system owner.
- Usage that goes against Kastelo policy, is illegal or unethical is not allowed on Kastelo equipment or resources, using Kastelo accounts or Kastelo credentials, or in any way that can be connected to Kastelo
- The workstation or laptop should have screen saver or locked-screen functionality enabled and password protected (face and fingerprint recognition is also allowed)
- Always lock your screen when leaving your equipment unattended, even at home or in the office

Use of mobile phones

When using a mobile phone for accessing or processing Kastelo IP or resources the following applies:

- If possible install/activate Antivirus on your mobile phone
- The mobile phone should have screen saver or locked-screen (autolock) functionality enabled and password protected (face and fingerprint recognition is also allowed)
- Always lock your screen when leaving your mobile phone unattended, even at home or in the office .

[1] If the rules set down by a partner or contractor are stricter than the Kastelo rules access is allowed unless the rules will have an in any way adverse effect on the Kastelo business. This is to be assessed case-by-case.

- Avoid public wi-fi networks if possible. For sharing of confidential data the mobile phone connection or a secure network should be used.
- Consider what data you store on your phone. Don't download Kastelo confidential or IP data onto your phone
- Ensure that your phone has a cloud-based backup service
- Make sure that you can remote swipe your phone on short notice
- Be as vigilant about malicious websites and phishing e-mails when using your phone as you are when using other mobile devices such as your laptop
- Be vigilant of "smishing"; SMS typically containing "important message from your bank" or similar with a link to a fake webpage

USB sticks and removable media

Usage of removable storage media for Kastelo data should be limited and only used if remote access to storage areas (e.g. file shares or collaboration tools) are unavailable. USB sticks and other removable media (e.g. removable hard drives) are only allowed if password protected and if antivirus is configured to scan the media when plugged in.

Personal use of Kastelo mobile devices

Personal use of Kastelo mobile devices is allowed, as long as any content or accessed or downloaded is legal and ethical and doesn't in any way compromise or negatively affect Kastelo.

It is recommended that Multi-Factor-Authentication (MFA) be enabled on any personal e-mail accounts accessed on the mobile device as e-mail accounts is a vulnerable attack vector.

Applications

The following applies to applications on Kastelo mobile devices:

- Installation of unlicensed applications are not allowed
- Standard applications and programs installed by Kastelo may not be uninstalled or inactivated by the User. This includes: antivirus, encryption, remote administration, monitoring, agents for updates and security patches.
- Software updates and security updates which are prompted must be applied as soon as possible to ensure that any security issues in the applications are remediated.
- For applications that are installed on the mobile devices which are not provided by the IT department the user is personally responsible for keeping the

applications updated and security patches applied. The same applies to applications that are not provided by the IT-department.

Virtual Meetings, collaboration tools and phone calls

The following applies when using virtual collaboration tools, meetings or phone calls regarding Kastelo business:

- Ensure that there's a confidentiality agreement in place before discussing or sharing confidential information
- Verify that there are no uninvited participants in your digital meetings by checking the names of the participants
- Approval must be given by all participants in the meeting when recording a virtual meeting, seminar, demonstration or similar
- Do not post meeting login information on social media or in other official forums where they can be apprehended by unauthorized persons
- If participating in a virtual meeting or call when in a public area, ensure that your screen cannot be viewed by others ("shoulder surfing") and be careful of mentioning confidential information that could be overheard . Do not conduct sensitive or confidential virtual meetings or phone calls in public spaces where the conversation can be overheard
- Use primarily Kastelo approved communication tools. If invited to a meeting by anyone external make sure that the communication tool offers security features such as end-to-end encryption and personal logins. If the tool chosen for conferencing or collaboration is insecure, be extra careful with the sharing of confidential or sensitive data.
- For meetings that will address confidential or strictly confidential topics, particularly concerning Kastelo IP, it's highly recommended that the meeting invite is sent out from Kastelo to ensure the security of the meeting (accesses, confidentiality, sharing of files, etc.)
- Always be aware that digital meetings, calls, chat etc. can easily be recorded
- Ensure that there are the right approvals in place when sharing documents etc. through collaboration tools

Only use Kastelo approved file shares or collaboration tools for sharing Kastelo or Customer data

Internet access and internet usage

Open wifi should be avoided if possible and may not be used when sharing Kastelo confidential information, in such cases it's recommended to connect via mobile network if a secure internet access isn't available.

E-mail

The following applies for usage of Kastelo e-mail account or when communication Kastelo data via e-mail:

- Always use your Kastelo e-mail account for any communication performed on behalf of Kastelo
- Usage of your private e-mail account for business communication is not allowed
- You may not forward Kastelo confidential data to your private mail-address
- You may not use your Kastelo e-mail address for signing up for online services or subscriptions that aren't related to the work you're doing for Kastelo
- MFA must be applied to all Kastelo mail accounts
- Suspicious e-mail shall either be deleted or reported to the IT-department (O365 also has a button where spam and malicious e-mails can be reported directly to Microsoft)
- If you suspect that your Kastelo e-mail account has been compromised, change your password and report your suspicions immediately to the IT-department

As e-mail communication is a common attack vector always keep the following in mind:

- Check the senders e-mail address: is it correct? Does the url between the < > match the senders name?
- Don't click on emails link or open attachments if you don't recognize the sender or find the mail in any ways suspicious
- Verify via phone or other communication tools such as e.g. chat or virtual meeting if a known sender suddenly starts using private or suspicious mail-addresses
- Verify unusual requests for payment approvals, changes to bank details, or disclosure of confidential data with the sender via phone or in person

Storage of data

Data that is stored locally on your laptop and not on OneDrive, Sharepoint or other shared services is not backed up. If a document has been saved to OneDrive when it was first created, it will be saved locally and backed when you next logon to the network.

Only use Kastelo approved storage areas or collaboration tools for storage of data in order to ensure that the data is backed up and secure.

Storage on unencrypted USB sticks or removable hard drives is not allowed.

Security

General Security Requirements for accessing Kastelo resources from mobile devices:

- Applications and operative systems on mobile devices shall be updated and available security patches applied
- Antivirus shall be applied to all mobile devices
- All laptops shall have hard desk encryption enabled
- All mobile devices shall be password protected and locked when not in use
- VPN shall be used for accessing Kastelo central resources
- All mobile devices shall be backed either in the Kastelo environment or in cloud storage (primarily mobile phones)
- Where possible SSO shall be applied and MFA required for access
- User unique accounts shall be used for accessing Kastelo resources and information
- An NDA or confidentiality agreement must be signed before accessing of Kastelo resources
- Kastelo IP shall be handled in accordance with confidentiality clause or NDA and cannot be downloaded to mobile devices unless specifically approved by Kastelo (does not apply to Kastelo employees)
- Monitoring shall be applied to all central services and alarms be triggered if there are deviations to security configurations or functionality such as inactivation of AV, encryption , or other types of security events are detected
- All central services and storage solutions, as well as user devices shall be backed up

Undertaking

I hereby verify that I have read, understood and accept responsibility for complying with this policy.

I accept that noncompliance with the policy may result in disciplinary actions. I'm also aware that this policy may be updated at any one time.

Date:

Location:

Signature:

Name:

Company (if not Kastelo):

Information Security Policy

Introduction

This document is created and enacted for Kastelo Holding AB and subsidiaries, collectively “Kastelo Group” or “Kastelo”.

Kastelo provides services that affect our customers most valued and critical asset: information. Thus, both our customers, partners, and employees must be able to rely on Kastelo to conscientiously assume responsibility for conducting our business in a way that ensures the security of their data. For us, providing comprehensive security and extensive data protection is more than just an obligation to meet statutory and regulatory requirements; it is also an explicit mark of quality of our services.

To ensure a sufficiently high level of data protection Kastelo has implemented an Information Security Management System, ISMS, governed by this policy. The aim of the ISMS and policy is to provide continuous risk-based information security management encompassing processes and controls for reducing or eliminating risks and threats to ours or our customers information assets. The ISMS and the policy are based on international standards such as ISO 27002, ISO 27005 and the EU General Data Protection Regulation. Topic specific standards and best practices are also applied in the different sections of the ISMS.

The ISMS and this policy are directed at all employees, subcontractors and partners to set the standard of how security is to permeate the business and workings of Kastelo. They are also aimed at our customers and shareholders to offer a transparent testimony to how Kastelo protects their assets and interests.

Violations of the policy may lead to disciplinary actions.

Principles of Data Protection

The following principles govern all security provisions and requirements within Kastelo.

Principle: Lawful conduct

Lawful conduct provides the basis for all actions conducted within the Group.

We respect the rights of the individuals and uphold the right to freedom of opinion and freedom of speech. Any security measures controls or contractual requirements that infringe such rights shall only be implemented within the legally admissible framework, with due regard to appropriateness.

Principle: Data Protection and Data Security

We work actively to ensure a sufficient level of data protection in regards to:

- *confidentiality* – that information is not made available or disclosed to unauthorized individuals, entities or processes;
- *integrity* – that information is kept accurate and complete and not altered by unauthorized individuals or entities;
- *availability* – that information is accessible and usable by authorized individuals, entities or processes when needed; and
- *traceability* – that activities can be derived to an identifiable individual or entity.

Principle: Customer Trust

We shall provide secure and reliable products and services to our customers.

Principle: Security Culture

Integrity and security awareness shall permeate the way we act and the way we conduct ourselves and our business throughout all levels of the company.

Principle: Need to Know

Knowledge and access to information shall only granted where needed. All access authorizations are controlled, and granted accesses are reviewed on a regular basis.

Principle: Leaning on Expertise

We lean on best practices and internationally recognized standards and regulations.

Principle: Risk-based Approach

Implementation of security measures and controls are based on systematic risk management:

- *identification of threats* to security protection goals;
- *investigation and assessment* of current security situation;

- *identification of resulting risk*, including *potential consequences* and *likelihood of occurrence*;
- identification of *appropriate countermeasures* or *consciously accepted risk*;
- *documentation* of evaluation process and decisions on security controls; and
- *long term management* of risk.

Risk-based security management demands a comprehensive view of key corporate assets and their correlation to critical business processes.

Security Management

To achieve our security goals, ensure proper implementation of security measures and maintain a continuous and long-term effective management of security Kastelo has implemented an Information Security Management System, ISMS. The ISMS encompasses organizational, administrative and technical elements throughout the whole business and applies to information in all its forms.

The ISMS, and this policy, applies to all employees using the company assets or partaking in business projects and deliveries, regardless of geographical location. This includes external parties such as contractors and partners.

The ISMS and this policy will be revised continuously and at the least annually.

Security Culture

Responsibility for information security management is incorporated in the organizational structure and every member of the organization, including contractors, are responsible for compliance with policies and instructions. Ultimate responsibility for communicating and promoting the ISMS and this policy throughout their organizations, and for encouraging a security culture throughout every aspect of the business, lies with management.

Employees shall be given the required security competence and shall also be encouraged to learn about security on their own initiative. They shall question any requirements which they feel to be ambiguous or unintelligible, and are encouraged to oppose any instructions which may be considered unethical or are evidently unlawful without having to fear any negative consequences. Employees shall also notify the company of any relevant security risks and incidents of which they are aware.

Structure of Information Security Management System

The Information Security Management System is structured into several tiers.

Each tier successively expands on and concretizes the tier above. This policy defines the overarching goals and principles; the Handbook defines how these principles are

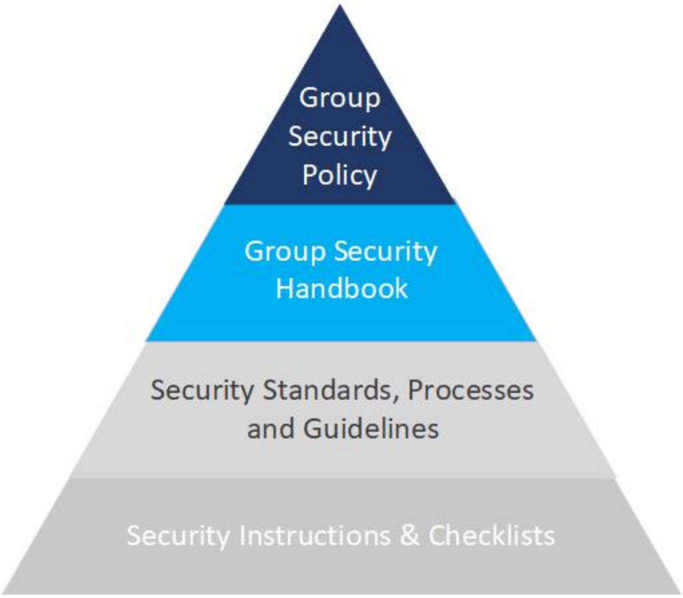
Group Security Policy
Group Security Handbook
Security Standards, Processes and Guidelines
Security Instructions & Checklists

Figure 1: ISMS Tiers

put into practice; the Standards, Processes and Guidelines describe the specifics of each practice; and finally, Instructions and Checklists define the individual steps to be taken in certain processes.

Monitoring and Reviews

Security Management shall monitor implementation of and compliance with the ISMS and Group Security Policy as well as review the applied security measures and take appropriate actions to ensure continuous improvement of the ISMS. Business units shall also perform their own reviews of compliance and implemented controls.

Password Management Policy

- All applications, systems and mobile devices shall be protected by passwords.
- Screensavers or lock screen shall be enabled on mobile devices and password protected (face or fingerprint recognition is an alternative to passwords).
- Passwords may not be reused for multiple applications or services.
- Kastelo credentials (username or passwords) may not be reused for external services.
- Sharing of passwords is not allowed.
- Password to Kastelo resources and VPN service should consist of minimum 10 characters with mixed characters from three of the four categories: English uppercase (A ... Z), English lowercase (a ... z), base ten digits (0 ... 9) or non-alphanumeric (! # % etc.), alternatively pass phrases with a minimum of 24 characters.
- It is recommended that mobile device passwords be changed every 180 days.
- Passwords shall be stored encrypted in digital form, e.g., in a password manager. If written down, they should be stored securely, i.e., in a locked cabinet. Kastelo provides a subscription to 1Password to all employees who want to use it.
- Default passwords must be changed.
- Accounts with elevated access rights (supervisor, system administrator) should be kept to a minimum. The usage of such IDs/passwords should be logged and reviewed at intervals.
- Password reset service is provided to central resources by Kastelo IT Admin. Verification of identity will be requested. No password reset service is provided for mobile devices which are not managed by Kastelo IT Admin.
- Only change password by using ctrl-alt-delete, settings, or when already logged in to a service. Never change passwords by clicking on links in e-mails unless you have requested a password reset yourself.

- Where possible multi factor authentication should be used.

Hardware Policy

Last updated for 2024.

Kastelo provides appropriate computing hardware for employees, with room for individual choice. We'll order from Dustin with delivery to your home office. The hardware policy should be reviewed yearly; if the year in the title doesn't match the current year, take the specific hardware recommendations below with a pinch of salt and perhaps file a suggested update. Generally, we expect hardware to have a life time of about three years before it should be upgraded to the policy in effect at that time.

Computer

You get a reasonably specced PC or Mac laptop with a 13" screen. Pick one of:

- PC laptop: Dell XPS 13 Plus 9320 (Core i7 32GB 1000GB SSD 13.4")
- Mac laptop: MacBook Air (2023) (M2 24GB 1000GB SSD 10-core 13.6")

By default, you'll get a Swedish keyboard layout. If you prefer something else, e.g. international English, let us know and we'll sort that out.

Additional office hardware

You also need a monitor, keyboard, etc.

- One 27" 4K monitor (UltraSharp U2723QE 27" 3840 x 2160 16:9 IPS 60Hz)
- External keyboard, mouse / trackpad / trackball, mouse pad of your choice (expense it).

Phone

If you require a phone for your work. Your choice of an iOS or Android smartphone up to 8 000 SEK (excl. VAT) with an unlimited data plan (domestic). Popular examples:

- Apple iPhone 14 128GB
- Samsung Galaxy S22 128GB Dual-SIM
- … or equivalent

If you want the most expensive phone on the market, for whatever reason, that's fine too but you get to chip in the additional cost above the limit.

Additional travel hardware

If and when it's required to travel to customers, we provide reasonable hardware for travel and presentations: laptop bag, presentation pointer/clicker, additional charger, dongles. Make reasonable choices and expense it as required.