POLICY

Acceptable Use Policy

Clear rules for using company devices, data, tools and AI at work

Document owner	[Owner name and role]
Approved by	[Approver name and role]
Version	[1.0]
Effective date	[Date]
Next review	[Date, at least yearly]
Classification	[Internal]

Purpose

This policy sets the rules every person at [Company Name] must follow when using company devices, accounts, data and tools. It protects the company, its customers and its staff from security incidents, data loss and misuse.

Scope

This policy applies to:

- All employees, contractors, interns and temporary staff.
- All company devices, including laptops and mobile devices enrolled in the [MDM, e.g. Jamf, Kandji or Intune].
- Personal devices used to access company email, chat or applications.
- All company accounts, SaaS applications, cloud services, data and networks, wherever staff work.

Roles and responsibilities

Role	Responsibilities
[Security Lead]	Owns this policy. Maintains the list of approved tools and AI tools. Answers questions and handles reported issues.

Role	Responsibilities
[IT Manager]	Configures and monitors devices through the [MDM]. Provides approved software and the password manager.
Managers	Make sure their team members know and follow this policy. Report concerns to the [Security Lead].
[People Operations Lead]	Collects policy acknowledgments at onboarding and every year.
All users	Follow this policy, protect company data and report incidents and suspicious activity.

Policy statements

General use

1. Users must use company systems mainly for business purposes. Limited personal use is allowed if it does not affect work, security or other people, and does not break any law or company policy.
2. Users must not use company systems to harass others, access illegal content, run a personal business or mine cryptocurrency.
3. Users must not try to bypass, disable or test security controls unless authorized in writing by the [Security Lead].
4. Users must protect their accounts, never share passwords or MFA devices, and follow the [Access Control Policy].

Company devices and MDM

5. Company laptops must be enrolled in the [MDM] before they are used for company work.
6. Users must not remove the MDM profile, disable endpoint protection, or change security settings managed by the [MDM].
7. Devices must keep these settings, enforced by the [MDM]:
    - Full disk encryption ([FileVault / BitLocker]) turned on.
    - Screen lock after no more than [5] minutes of inactivity.
    - Operating system and browser updates installed within [14] days of release, or [72 hours] for critical security updates.
    - Endpoint protection ([EDR tool]) installed and running.
    - Firewall turned on.
8. Users must not leave devices unattended and unlocked in public places, and must keep them out of sight in vehicles.

9. Lost or stolen devices must be reported to [IT channel or email] within [1 hour] of discovery so they can be locked or wiped remotely.
10. Only software from the [MDM self-service catalog] or approved by the [IT Manager] may be installed. Users must not use pirated or unlicensed software.
11. Users must return all company devices and accessories on or before their last working day.

Personal devices

12. Personal phones may access company email, chat and approved apps only through [MDM work profile / approved app protection], with a screen lock and a supported OS version.
13. Personal computers must not be used to access confidential data or production systems.
14. [Company Name] may remove company data from personal devices when the user leaves or the device is lost. It must not access personal data on the device.

Data handling

15. Users must handle information according to its classification in the [Data Classification and Handling Policy]: [Public, Internal, Confidential, Restricted].
16. Confidential and restricted data, including customer data, must be stored only in approved company systems, such as [Google Drive / SharePoint, the production database, Jira].
17. Users must not copy customer data to personal accounts, personal devices, USB drives or unapproved SaaS tools.
18. Customer data must not be used in development or test environments unless it is masked or the [Engineering Lead] has approved it.
19. Files must be shared with specific people or groups. Public links to confidential data must not be created.
20. Before sending data outside the company, users must confirm that the recipient is authorized and that the channel is approved.
21. Printed confidential information must be kept secure and shredded when no longer needed.

Email, chat and collaboration

22. Users must treat unexpected links, attachments, payment requests and requests for credentials as suspicious and verify them through another channel.
23. Changes to payment details or urgent payment requests must be confirmed by a phone or video call with a known contact before acting.
24. Credentials, secrets and restricted data must not be sent in email or chat messages, including [Slack / Microsoft Teams].
25. Only approved SaaS tools may be used for company data. New tools must be requested through [ticketing tool] and reviewed by the [Security Lead] before use.

AI tools

26. Only AI tools listed in the [approved AI tools list] may be used with company data. The list states which data classification each tool is approved for.
27. Users must not enter confidential or restricted data, customer data, personal data, credentials or source code into AI tools that are not approved for that data.
28. Approved AI tools must be used with company accounts, with settings that prevent the provider from training on company data where available.
29. Users are responsible for checking AI output before using it. AI generated code must go through the normal code review and security checks.
30. AI tools and agents that can act on company systems, such as code assistants with repository or cloud access, must be approved by the [Security Lead] and must use the least access needed.
31. Browser extensions and plugins that read page content or connect to AI services must be approved before installation.

Remote work

32. Users must work from locations where screens and conversations cannot easily be seen or heard by others when handling confidential information.
33. Home Wi-Fi must use WPA2 or WPA3 with a strong password, and the router default admin password must be changed.
34. On public Wi-Fi, users must use [company VPN / zero trust access tool] or a phone hotspot.
35. Users who plan to work from another country for more than [number] days must get approval from [People Operations and the Security Lead] first.

Monitoring

36. [Company Name] monitors company devices, accounts and networks for security purposes, such as MDM compliance, login activity and threat detection, as allowed by applicable law. Users should not expect privacy for activity on company systems beyond what the law provides.

Reporting

37. Users must report immediately, through [#security channel / security@company email], any of the following:

- Suspicious emails, messages or calls.
- Lost or stolen devices.
- Data sent to the wrong person or shared by mistake.
- Malware warnings or unusual device behavior.
- Any suspected breach of this policy.

38. Users must not investigate incidents themselves or delete evidence. They must follow the instructions of the [Security Lead].
39. Reports made in good faith will not lead to disciplinary action, even if the report turns out to be a false alarm or the user made a mistake.

Acknowledgment

40. Users must acknowledge this policy before receiving access and at least once every [12 months].

Exceptions

Exceptions must be requested in [ticketing tool] with the business reason and the risk. The [Security Lead] must approve them, set an end date no later than [12 months] and record them in the [exceptions register].

Enforcement

Violations may lead to removal of access and disciplinary action, up to and including termination of employment or contract, in line with [Company Name]'s HR procedures and applicable law. Compliance is checked through MDM reports, SaaS discovery, data loss prevention alerts and internal audits.

Related documents

- Information Security Policy
- Access Control Policy
- Incident Response Plan
- [Data Classification and Handling Policy]
- [Approved AI tools list]
- [Approved software and SaaS list]

Annex A mapping

Annex A control	Section that covers it
5.9 Inventory of information and other associated assets	Company devices and MDM
5.10 Acceptable use of information and other associated assets	General use, Data handling, AI tools
5.11 Return of assets	Company devices and MDM (statement 11)

Annex A control	Section that covers it
5.13 Labelling of information	Data handling
5.14 Information transfer	Data handling, Email, chat and collaboration
6.6 Confidentiality or non-disclosure agreements	Data handling
6.7 Remote working	Remote work
6.8 Information security event reporting	Reporting
7.7 Clear desk and clear screen	Company devices and MDM, Remote work
7.9 Security of assets off-premises	Company devices and MDM, Remote work
7.10 Storage media	Data handling (statement 17)
8.1 User endpoint devices	Company devices and MDM, Personal devices
8.7 Protection against malware	Company devices and MDM
8.12 Data leakage prevention	Data handling, AI tools
8.19 Installation of software on operational systems	Company devices and MDM (statement 10)

Review and approval

The [Security Lead] must review this policy at least once every [12 months], and sooner when new tools such as AI services change how staff work. Changes are approved by [Security Committee], recorded in the document control table and communicated to all staff, who must acknowledge the new version within [30] days.