TLP:AMBER Limited distribution — share within your organisation on a need-to-know basis. Do not share externally without authorisation. TLP: https://www.first.org/tlp/ | DK: https://www.cfcs.dk/da/handelser/traffic-light-protocol/

Defencia.dk

Acceptable Use Policy
AUP

Revision	*X.X*	**Classification**	**TLP:AMBER**
Responsible	*[Management Name]*	**Document Owner**	*[Owner]*

TEMPLATE GUIDANCE *This is a template example of a real-world AUP. Adapt all sections to your organisation's requirements and applicable local law (Denmark: Medarbejdernes brug af IT, GDPR, Databeskyttelsesloven). Have Legal Counsel review before publishing. Remove all TEMPLATE GUIDANCE boxes before distributing to employees. Update xleb@defecia.dk as contact.*

Version History

Version	Date	Author	Change Description
1.0			Initial version

1. Introduction

This Acceptable Use Policy ("AUP" or "Policy") defines the principles, rules, and guidelines governing the use of [Company Name]'s technology resources, information systems, networks, data, and connected services.

This Policy is designed to protect [Company Name], its employees, contractors, partners, and customers from illegal or damaging actions — whether intentional or unintentional — and to ensure that all users of company technology act responsibly, lawfully, and in accordance with the organisation's values and obligations.

By using [Company Name]'s technology resources, all users confirm that they have read, understood, and agree to comply with this Policy. Continued use after any revision constitutes acceptance of the updated terms.

2. Purpose

The primary purpose of this Policy is to:

- Promote the integrity, reliability, availability, and security of [Company Name]'s technology resources
- Protect company and personal information from unauthorised access, disclosure, or misuse
- Ensure compliance with applicable laws and regulations, including the EU General Data Protection Regulation (GDPR), the Danish Data Protection Act (Databeskyttelsesloven), and NIS2 obligations where applicable
- Establish clear expectations for user behaviour and the consequences of non-compliance
- Protect [Company Name]'s reputation and legal standing

3. Scope

This Policy applies to all individuals who access or use [Company Name]'s technology resources, including:

- Permanent and temporary employees
- Contractors, consultants, and freelancers
- Interns and students on placement
- Partners and third-party suppliers with access to company systems
- Board members and senior management

This Policy applies to all technology resources owned, leased, or managed by [Company Name], including but not limited to:

- Desktop computers, laptops, and workstations
- Mobile devices (smartphones and tablets) — both company-issued and personal devices used for work (BYOD)
- Servers, networks, Wi-Fi infrastructure, and VPN connections
- Cloud services, SaaS applications, and web portals
- Email, instant messaging, and collaboration platforms
- Storage media: USB drives, external hard drives, SD cards
- Any personal device used to access company systems, data, or email

LEGAL NOTE	This Policy must be read in conjunction with the employee's employment contract. In Denmark, employee monitoring and device usage is subject to the Danish Employees' Computer Use Act and applicable data protection law. This Policy does not override statutory employee rights. Consult Legal Counsel before enforcement.

4. Policy

a. Use of Technology Resources

Work-Related Use: Company technology resources are provided for legitimate business purposes. Users are expected to use these resources professionally and productively.

Personal Use: Occasional, brief personal use is permitted provided it does not: interfere with work responsibilities, consume significant bandwidth or storage, violate any provision of this Policy, or create any legal or reputational risk for [Company Name].

Prohibited Use: The following activities are strictly forbidden using company technology resources:

- Accessing, storing, or distributing illegal content of any kind
- Conducting any activity for personal financial gain that is not authorised by [Company Name]
- Excessive personal use that interferes with job performance
- Streaming or downloading large non-work media files
- Accessing online gambling or gaming platforms during working hours
- Any activity that violates applicable law or regulation

b. Security and Confidentiality

Data Confidentiality: Users must protect confidential information from unauthorised disclosure. This includes customer data, financial data, personnel records, strategic plans, and any information marked Confidential, TLP:AMBER, or TLP:RED.

Data Protection (GDPR): Users who process personal data must do so in accordance with GDPR principles: lawfully, fairly, and transparently; for specified, explicit, and legitimate purposes; and with appropriate security measures. Contact the Data Protection Officer (DPO) with any questions.

Password Management: All users must use strong, unique passwords for each system. Minimum requirements: 12+ characters, mix of uppercase, lowercase, numbers, and symbols. A company-approved password manager must be used. Passwords must never be shared. Default or manufacturer passwords must be changed immediately upon deployment.

Multi-Factor Authentication (MFA): MFA must be enabled on all systems that support it, including email, VPN, cloud services, and any system accessible from the internet. This is mandatory, not optional.

Encryption: Sensitive data must be encrypted at rest and in transit. Laptops and mobile devices must have full-disk encryption enabled (BitLocker, FileVault, or equivalent).

Screen Locking: Devices must auto-lock after a maximum of [5/10] minutes of inactivity. Users must lock their screen (Win+L / Cmd+Ctrl+Q) when leaving a device unattended.

Incident Reporting: Any security breach, suspected breach, lost device, or suspicious activity must be reported immediately to the IT department or [security contact] at [email/phone]. Do not attempt to investigate or remediate a security incident yourself.

c. Prohibited Activities

The following activities are strictly prohibited on company technology resources. This list is not exhaustive.

Hacking and Unauthorised Access: Attempting to gain unauthorised access to any system, network, or data — whether internal or external — is strictly prohibited. This includes port scanning, vulnerability testing, or use of exploitation tools without explicit written authorisation from IT Security.

Malware: Intentionally introducing, distributing, or executing malware, viruses, ransomware, spyware, or any other malicious code is a serious violation and may constitute a criminal offence.

Harassment and Offensive Material: Using technology resources to harass, bully, intimidate, or discriminate against any person is forbidden. Distributing or accessing pornographic, racist, sexist, or otherwise offensive material is not permitted.

Illegal Copying and Piracy: Copying, downloading, or distributing software, media, or content in violation of copyright or licensing agreements is prohibited.

Shadow IT / Unapproved Software: Installing or using software, applications, browser extensions, or cloud services that have not been approved by IT is prohibited. All software requests must go through the IT approval process. Unapproved tools will be subject to removal and monitoring.

Circumventing Security Controls: Using VPNs, proxies, Tor, or other tools to bypass company security controls, content filtering, or monitoring is prohibited unless explicitly approved for a specific business purpose.

Data Exfiltration: Transferring company data to unauthorised external storage, personal cloud accounts, or personal email accounts is prohibited. This includes uploading sensitive data to consumer AI tools without IT approval.

Use of AI Tools: The use of AI assistants (e.g. ChatGPT, Copilot, Gemini) for work purposes is subject to the [AI Usage Addendum / separate AI policy]. Users must not submit confidential company data, customer data, or personal data to external AI services without explicit approval.

d. Monitoring and Privacy

TEMPLATE GUIDANCE

Monitoring of employee IT activity is subject to Danish and EU law. In Denmark, monitoring must be proportionate, documented, and employees must be informed in advance. This section must be reviewed by Legal Counsel before implementation. 'No expectation of privacy' clauses must be carefully worded to comply with Danish employment law.

Rights to Monitor: [Company Name] reserves the right to monitor activity on its technology resources, including network traffic, email, device usage logs, and access records, for the purpose of ensuring compliance with this Policy, protecting company assets, and meeting legal obligations. Monitoring will be conducted in accordance with applicable law.

Privacy Expectations: Users should not have an expectation of privacy when using company-owned devices, networks, or systems for any purpose. [Company Name] may access, review, and retain data stored on or transmitted through company systems. Personal devices used to access company resources may be subject to remote management (MDM) as described in the BYOD policy.

Proportionality: Monitoring will be proportionate to the risk and purpose. Continuous detailed monitoring of all user activity is not standard practice. Targeted monitoring may be initiated in response to a specific security incident, compliance investigation, or reasonable suspicion of policy violation.

Notification: Employees are informed of this Policy and the possibility of monitoring through this document, the employment contract, and the onboarding process. Ongoing reminder notices may be posted at system login.

e. Software Licensing and Intellectual Property

Compliance with Licensing: All software used on company systems must be properly licensed. Users must not install unlicensed software. IT maintains a software asset register. Audit requests must be fulfilled promptly.

Intellectual Property: All work product created using company technology resources, or during working hours, is the intellectual property of [Company Name] unless otherwise specified in the employment contract. Users must not reproduce, distribute, or misuse third-party intellectual property.

Open Source: Use of open-source software must comply with applicable licence terms (GPL, MIT, Apache, etc.). Use of open-source components in company products must be approved by IT and Legal.

f. Personal Devices and BYOD (Bring Your Own Device)

TEMPLATE GUIDANCE

BYOD policies carry significant legal and technical complexity. The organisation must balance employee privacy with security requirements. Consider whether BYOD is appropriate or whether company-issued devices are preferable. This section should be reviewed by Legal Counsel.

Approved BYOD Use: Employees who use personal devices for work must register their device with IT and install the company Mobile Device Management (MDM) profile. Use of personal devices for work is a privilege, not a right, and is subject to this Policy.

Security Requirements: Personal devices used for work must have: full-disk encryption enabled, a PIN or biometric lock, the latest available OS updates installed, and company-approved email and VPN clients.

Separation of Data: Users must keep personal and company data separate. Company email and data must be accessed through approved applications only, not personal accounts.

Remote Wipe: If a personal device used for work is lost or stolen, [Company Name] may, with the employee's advance consent (documented at device registration), remotely wipe the company data partition. The employee will be notified unless doing so would compromise a security investigation.

g. Remote and Hybrid Working

Home Network Security: Employees working remotely must use the company VPN when accessing internal systems. Home Wi-Fi routers must use WPA2 or WPA3 encryption. Public Wi-Fi must not be used to access company systems without VPN protection.

Physical Security: Employees must ensure that company devices and data are protected from physical access by household members or others. Screens must not be visible to unauthorised persons during calls or work involving confidential information.

Video Conferencing: Employees must ensure that background environments during video calls do not expose confidential information (whiteboards, screens, documents). Use of virtual backgrounds is recommended when working from non-secure environments.

5. Compliance and Consequences

All users of [Company Name] technology resources are responsible for understanding and complying with this Policy. Ignorance of this Policy is not an acceptable defence.

Violations of this Policy may result in:

- Verbal or written warning
- Temporary or permanent suspension of access to technology resources
- Disciplinary action up to and including termination of employment or contract
- Civil legal action by [Company Name] to recover damages
- Referral to law enforcement authorities where criminal activity is suspected

PROPORTIONALITY	Disciplinary action will be proportionate to the severity of the violation. Minor, unintentional breaches may result in additional training. Serious or repeated violations, or violations involving malicious intent, data theft, or criminal activity, will be treated with the highest severity.

6. Policy Review and Modification

Review frequency	*Minimum annually. Also reviewed after: significant security incident, major technology change, new regulatory requirement, or significant organisational change.*
Review owner	*[CISO / IT Manager / Document Owner]*
Approval authority	*[C-level / Management / Board]*
Communication of changes	*All changes will be communicated to all employees via [email / intranet / team meeting] with a minimum of [14 days] notice before the revised Policy takes effect. Employees will be required to re-acknowledge the updated Policy.*

7. Acknowledgement of Understanding

All employees, contractors, and third-party users of [Company Name] technology resources must read this Policy and confirm that they have understood and agreed to comply with it.

By signing below, the individual confirms that they:

- Have read and understood the Acceptable Use Policy in full
- Agree to comply with all requirements set out in this Policy
- Understand the consequences of non-compliance
- Will report any suspected violations or security incidents to the IT department immediately

RECORD KEEPING Signed acknowledgements must be retained in the employee's HR file. For GDPR compliance, retain for the duration of employment plus [3/5] years. Digital signatures are accepted if the system provides a verifiable audit trail.

Full Name	Job Title / Department	Signature	Date	Employee ID / Ref.

References and Further Guidance

The following resources may be useful when adapting this template:

- SANS Institute Information Security Policy Templates: https://www.sans.org/information-security-policy/
- Workable AUP Template: https://resources.workable.com/acceptable-use-policy-template
- ENISA Guidelines on Cybersecurity for SMEs: https://www.enisa.europa.eu
- Danish Data Protection Agency (Datatilsynet): https://www.datatilsynet.dk
- NIS2 Directive (EU 2022/2555): https://eur-lex.europa.eu

A policy that no one has read is no policy at all. Awareness, training, and annual acknowledgement are as important as the document itself.