

AI Caravan Ltd. IT Acceptable Use Policy

(fictional, for training only)

Document reference: IT-POL-01, version 2, effective 1 March 2026. Owner: IT coordinator.

IT Acceptable Use Policy, section 1: Scope

This policy applies to all employees, contractors and interns of AI Caravan Ltd. who use a company laptop, a company account or the company network. It covers e-mail, chat, cloud storage and AI tools.

IT Acceptable Use Policy, section 2: Accounts and passwords

Every user has one personal company account. Accounts must not be shared. Passwords are at least 14 characters long and are stored only in the company password manager. Multi-factor authentication is required on e-mail, cloud storage and the HR portal. A lost phone used for multi-factor authentication is reported to the IT coordinator on the same working day.

Automations run under a dedicated service account (automations@aicaravan.example), never under a personal account. The IT coordinator owns all service accounts and reviews their access every quarter.

IT Acceptable Use Policy, section 3: Company laptops

Laptops are issued on the first working day and returned on the last. Disks are encrypted and the screen locks after 5 minutes without use. Users may not install software that is not on the approved software list; requests to add software are sent to the IT coordinator, who answers within five working days. A lost or stolen laptop is reported within 24 hours.

IT Acceptable Use Policy, section 4: E-mail and files

Company documents are stored in the company cloud drive, in the folder of the team that owns them. Personal cloud accounts and USB drives must not be used for company documents. Files shared outside the company use a link that expires after 30 days.

IT Acceptable Use Policy, section 5: AI tools

Only AI tools on the approved software list may be used with company data. Public and internal-general documents, such as policies and product guides, may be used with approved AI tools. Personal data about employees or customers may be used only in workflows registered in the Data register and approved by the IT coordinator. Payroll, medical records, legal documents and passwords must never be pasted into, or sent by a workflow to, an external AI tool.

Every workflow that sends data to an AI provider has one row in the Data register: workflow, data sent, provider, tier, owner.

IT Acceptable Use Policy, section 6: Monitoring

The company logs sign-ins, file sharing and workflow runs for security purposes. Logs are kept for 12 months and are reviewed only by the IT coordinator, or by a manager with written approval from the department head.

IT Acceptable Use Policy, section 7: Breaches

Suspected security incidents, including a phishing e-mail that was clicked, are reported to the IT coordinator immediately. Breaches of this policy are handled under the disciplinary procedure.