Acceptable Use of Technology and Bring Your Own Device (BYOD) Policy

Replace each [Placeholder]. Work through it with IT and security, who own the technical controls; HR owns the people side. Add any state monitoring notice your locations require.

1. SCOPE

This policy applies to all employees, temporary workers, contractors and interns who use [Company Name] technology: computers, phones, headsets, networks, email, chat, cloud applications, customer systems and data, whether at a company site, at home or anywhere else. It also applies to personal devices used to access company email, chat or data.

2. ACCEPTABLE USE

Company systems are provided for business. Brief, occasional personal use (checking a personal email, a quick message home) is fine if it does not interfere with work, use significant bandwidth or break any other rule in this policy. Production-floor and customer-facing staff should limit personal use to breaks.

3. PROHIBITED USE

Do not use company systems to:

- Access, store or send material that is illegal, sexually explicit, or harassing or discriminatory under our [Anti-Harassment Policy]
- Share passwords, use another person's login, or let anyone else use your account
- Install software, browser extensions or apps that IT has not approved
- Copy customer, candidate or employee data to personal email, personal cloud storage, USB drives or personal devices except as this policy allows
- Take photos, screenshots or recordings of customer data or screens
- Bypass security controls, VPN, filtering or monitoring tools
- Run a personal business, mine cryptocurrency or send chain messages
- Enter confidential, customer or personal data into AI tools that IT has not approved

4. PASSWORDS, ACCESS AND SECURITY

Use a unique password for company accounts and turn on multi-factor authentication where offered. Lock your screen whenever you step away. Report lost or stolen devices, suspected phishing and any accidental data exposure to [IT or security contact] immediately, and in any case within [1 hour]. Reporting quickly will not lead to discipline for an honest mistake.

5. AI TOOLS

Approved AI tools are listed at [location]. You may use them for work within the limits IT sets. Check AI-generated output before relying on it. Do not use AI tools to make or recommend decisions about hiring, pay, discipline or termination unless HR has approved that specific use.

6. MONITORING AND PRIVACY

Company systems, accounts and devices belong to the company. To protect customers, meet legal obligations and maintain security, the company may monitor, log and review use of its systems, including email, chat, internet activity, call recordings, screen activity and system access, to the extent the law allows. Employees should not expect privacy in anything created, sent or stored on company systems. The company will not access personal accounts or personal content on a personal device except as described in section 8. [Insert any state-required notice, e.g. New York, Connecticut or Delaware electronic monitoring notice, and how employees acknowledge it.]

7. MOBILE PHONES IN WORK AREAS

Personal mobile phones and smartwatches with cameras are not permitted [on the production floor / in secure areas where customer payment data is handled]. Store them in [lockers or designated area] and use them during breaks and in [break areas]. Employees who need to be reachable for an emergency, such as childcare, can give [supervisor desk phone number] to family members. Exceptions for medical devices or disability-related needs can be requested from [HR contact].

8. BRING YOUR OWN DEVICE (BYOD)

Employees may use a personal phone, tablet or computer for work only if [IT] has approved the device and the employee has signed the BYOD agreement below. Approved devices must:

- run a supported operating system with current updates and a screen lock
- have the company's [mobile device management or work-profile app] installed, which separates company data from personal data
- not be shared with family members while logged in to company apps

The company can see and remove company apps and data in the work profile. It cannot see personal photos, messages, browsing or apps. If a device is lost or stolen, or employment ends, the company will remove company data and may, only if a full wipe is the only option and the employee has been told in advance, reset the device. [Monthly stipend or reimbursement: $[amount] per month / reimbursement of a reasonable share of the employee's plan.]

9. OFF-HOURS USE AND TIMEKEEPING

Non-exempt (hourly) employees should not check or respond to work email, chat or messages outside scheduled hours unless a manager has asked them to. Any work done outside scheduled hours, including reading and answering messages, counts as time worked and must be recorded and will be paid. Managers should not message hourly staff after hours except for schedule changes or emergencies.

10. SEPARATION AND VIOLATIONS

On the last day of employment, return all company equipment and allow removal of company data from personal devices. Violations of this policy may lead to loss of access and discipline up to termination, and serious violations may be reported to law enforcement. Effective date: [Date]. Questions: [IT contact] or [HR contact].

EMPLOYEE ACKNOWLEDGMENT AND BYOD AGREEMENT

☐ I have read and agree to follow the Acceptable Use and BYOD Policy, including the monitoring notice in section 6.

I want to use a personal device for work

☐ No ☐ Yes: phone ☐ Yes: tablet ☐ Yes: computer

Device make and model (if using BYOD)

☐ I agree to the removal of company data from my device as described in section 8.

Employee name

Employee signature

Date

Date