Remote Work & Information Security Policy

Effective: January 15, 2026 **Owner:** People Operations & IT Security
Audience: All employees and contractors

1. Purpose

This policy defines the requirements and expectations for employees and contractors who work outside of company-managed offices. Its purpose is to protect customer data, intellectual property, and company systems while supporting flexible, productive remote work.

2. Scope

This policy applies to anyone who accesses company systems, applications, or data from any location that is not a company-managed office. It applies regardless of device ownership (company-issued or personal) and regardless of whether the work is full-time, part-time, or occasional.

3. Approved Work Environments

3.1 Physical environment

- You must work from a location with reliable internet (minimum 25 Mbps down / 5 Mbps up).
- Your workspace must offer a reasonable degree of privacy. Confidential calls and screens must not be visible or audible to non-employees, including family members and roommates.
- Public spaces (cafés, airports, co-working drop-ins) are permitted only for non-confidential work. Customer data and source code must never be accessed in public on screen.

3.2 International work

Working from outside your country of employment for more than 14 consecutive days requires written approval from People Ops and Tax. Some countries are restricted entirely for legal and security reasons; consult the current Restricted Locations list before travel.

4. Device Standards

- **Company-issued laptops** are the only approved devices for accessing source code, production systems, customer data, and internal financial systems.
- **Full-disk encryption** must be enabled and verified by the IT Mobile Device Management agent.
- **Screen lock** must engage after no more than 5 minutes of inactivity.

- **Operating system updates** must be installed within 14 days of release. Critical security patches must be installed within 72 hours.
- **Personal devices** may be used only for email, calendar, and chat, and only when enrolled in the company MDM in approved-personal-device mode.

5. Network & Connectivity

- You must use the company VPN any time you access internal systems from a network you do not personally own and control.
- Home Wi-Fi must use WPA2 or WPA3 with a unique password (not the manufacturer default).
- Do not connect company devices to public USB charging ports.
- Do not enable tethering or hotspots that share the company VPN connection with third parties.

> **Reminder:** If you suspect that any company device, account, or credential has been lost, stolen, or compromised, you must notify `security@company.com` within 1 hour, regardless of time zone or working hours.

6. Data Handling

6.1 Customer data

- Customer data may only be accessed through approved company applications. It may not be copied to personal cloud storage, personal email, or removable media.
- Local downloads of customer data are permitted only for an active business need, must be stored in the encrypted `~/Work` folder, and must be deleted within 7 days.

6.2 Printing

Printing customer data or other confidential information from a home printer is prohibited unless explicitly authorized in writing for a specific task. Printed material must be shredded after use; it must not be placed in household recycling.

7. Authentication & Access

- Multi-factor authentication (MFA) is required on every company application that supports it. Hardware security keys are required for production-access roles.
- Passwords must be stored only in the company-approved password manager. Browser-saved passwords for company accounts are prohibited.
- Sharing credentials with anyone, including teammates and contractors, is prohibited.

8. Acceptable Use

- Use of company devices and networks for unlawful activity, harassment, or unauthorized commercial activity is prohibited.
- Installation of software not approved by IT is prohibited on company devices. Submit a request via the IT Catalog if you need additional tools.
- Generative AI tools may be used in accordance with the separate *AI & Data Handling Policy*; customer or proprietary data must not be entered into unapproved third-party AI tools.

9. Incident Reporting

Any of the following must be reported immediately to `security@company.com`:

- Lost or stolen device.
- Suspicious login alerts or unexpected MFA prompts.
- Phishing attempts, even if unsuccessful.
- Inadvertent disclosure of customer data, source code, or financial information.

10. Acknowledgement

All employees and contractors must acknowledge this policy annually through the People Ops portal. Violation may result in disciplinary action up to and including termination, and may result in legal action where applicable.

Employee name:	**Signature / e-sign date:**