Acceptable Use Policy

Version v1.0

PolicyPress

Last Reviewed: 2026-01-01

Contents

Purpose and Scope

This policy defines the acceptable use of PolicyPress's information systems, networks, devices, and data. It exists to protect the company, its employees, and its customers from risk - not to restrict people from doing their jobs.

This policy applies to all employees, contractors, and third parties who access PolicyPress systems or data, whether on company-owned or personal devices.

General Principles

Use company systems and data:

- **For work purposes** - personal use is tolerated when incidental and does not interfere with your work or company resources
- **With care** - treat company systems and data as you would any professional asset
- **Honestly** - do not misrepresent yourself, falsify records, or circumvent controls

When in doubt about whether a use is appropriate, ask your manager or IT.

Acceptable Use

The following uses are expected and encouraged:

- Performing your job duties and collaborating with colleagues
- Accessing systems and data you have been granted permission to use
- Installing work-required software through approved channels
- Reporting security concerns or suspicious activity to IT

Prohibited Use

The following uses are prohibited on all company systems and networks, including personal devices used to access company resources:

Data and Privacy

- Accessing, copying, or sharing data beyond what your role requires
- Sharing confidential company, customer, or employee information with unauthorized parties
- Circumventing data loss prevention controls or access restrictions

Systems and Network

- Installing unauthorized software, tools, or browser extensions on company devices
- Attempting to gain unauthorized access to any system, account, or network
- Using company systems to conduct cryptocurrency mining or run personal services
- Connecting unauthorized devices to the internal network

Communications

- Sending harassing, discriminatory, or threatening communications via company systems
- Impersonating another person or organization
- Using company email or accounts for personal commercial activity

Legal and Compliance

- Downloading, storing, or distributing copyrighted material without authorization
- Accessing or distributing illegal content of any kind
- Violating applicable laws or regulations through company systems

Passwords and Credentials

- Use a unique, strong password for every system (use a password manager)
- Enable multi-factor authentication (MFA) wherever it is offered
- Never share your credentials with anyone, including IT staff
- Report suspected credential compromise to IT immediately

Personal Devices (BYOD)

If you use a personal device to access company systems (email, Slack, cloud services):

- The device must be password or PIN protected
- Company data must not be stored permanently on personal devices unless in an approved app
- PolicyPress may require the remote wipe of company data from your personal device if it is lost, stolen, or upon your departure
- PolicyPress will not access personal data on your device beyond what is technically required to manage the company's data

Remote Work

When working remotely:

- Use the company VPN when accessing internal systems, if required by IT
- Do not conduct sensitive work on public Wi-Fi without VPN protection
- Lock your screen when stepping away from your device
- Do not allow household members or guests to use company-owned equipment

Monitoring

PolicyPress reserves the right to monitor use of company systems and networks to the extent permitted by applicable law. This includes:

- Network traffic and logs on company-managed infrastructure
- Email and communication metadata (not content, unless required for a security investigation)
- Activity on company-owned devices

Monitoring is conducted for security, legal compliance, and operational purposes. Employees should have no expectation of privacy when using company-owned systems or networks.

Reporting Violations

If you observe a violation of this policy or a security concern, report it to IT or your manager promptly. Reports made in good faith will not result in retaliation.

Enforcement

Violations of this policy may result in disciplinary action up to and including termination, and may be referred to law enforcement where criminal activity is involved.

Exceptions

Exceptions to this policy (e.g., security research requiring otherwise-prohibited tools) must be:

1. Documented with business justification
2. Approved in writing by IT/Security and the relevant manager
3. Time-limited

For questions, contact IT or your manager.

Version History

Version	Date	Description	Revised By	Approved By
1.0	2026-01-01	Initial policy.	IT / Security	CEO