



SAMPLE POLICY EXCERPTS

Cybersecurity Policy Suite

A sample of clear, practical policy language—ready to be tailored, approved, published, acknowledged, and evidenced.

Cybersecurity Policy Suite

A concise, editable policy baseline for a growing organization. These excerpts demonstrate structure and tone; they are not legal advice or a substitute for organization-specific review.

How this works	Unboredly policies are customized to the organization, approved by an authorized owner, published to employees, acknowledged, versioned, and reviewed on a scheduled cadence.
----------------	---

Policy library overview

Policy	Purpose	Owner	Review cycle	Status
Information Security Policy	Sets the organization’s security objectives, governance, roles, and baseline expectations.	Executive sponsor	Annual	Published
Access Control Policy	Defines access approval, least privilege, authentication, review, and offboarding expectations.	IT / Security	Annual	Published
Acceptable Use & Data Handling	Guides responsible use of company systems, data, AI tools, remote work, and personal devices.	Operations	Annual	Pending review
Incident Response Policy	Defines reporting, escalation, leadership decisions, communications, and lessons learned.	Security lead	Annual + exercise	Published
Vendor Risk Management Policy	Sets due diligence and review expectations for vendors that process company or customer data.	Finance / Security	Annual	Published

Sample: Access Control Policy

Policy statement. Access to company systems, data, and services must be approved, appropriate to the user’s role, and limited to what is necessary to perform authorized work. Access must be removed promptly when no longer required.

1. Access approval

New access requires a documented business need and approval from the relevant system owner or delegated approver.

2. Authentication

Multi-factor authentication must be used where supported for company systems, administrative access, remote access, and services that contain sensitive information.

3. Privileged access

Administrative access is limited to authorized personnel, reviewed regularly, and not used for routine work.

4. Offboarding

Access must be reviewed and removed promptly when employment, contract work, or business need ends.

5. Review

System owners review access to material systems on a defined schedule and document exceptions or corrective actions.

Sample: Acceptable Use & Data Handling

Policy statement. Personnel must use company information and technology resources responsibly, protect information according to its sensitivity, and avoid sharing company or customer data with unapproved people, services, or artificial-intelligence tools.

Employees must report suspected phishing, misdirected data, lost devices, suspected account compromise, or other security concerns promptly through the organization’s approved reporting process. Employees must not enter company credentials into unexpected websites or disclose passwords, MFA codes, or confidential information in response to unverified requests.

Acknowledgement record	When published, each policy records its version, approval date, publication date, assigned recipients, acknowledgement status, and annual review date. This creates a simple evidence trail without turning policy management into paperwork.
-------------------------------	---