FIRST UNDERWRITERS INSURANCE BROKERS

Security Policy Templates

8 Customizable Policies for Small Business Cybersecurity

This collection provides ready-to-use cybersecurity policy templates designed for small and mid-sized businesses. Each policy covers purpose, scope, key requirements, responsibilities, and enforcement. Customize the bracketed [fields] to match your organization.

A strong set of written security policies is increasingly required by cyber insurance carriers, regulatory bodies, and business partners. These templates give you a professional foundation to build on.

Part of: Cyber Security Essentials for Small Business

Free resource series from First Underwriters Insurance Brokers
www.firstunderwriters.com

These templates are for informational purposes only and do not constitute legal or cybersecurity advice.

How to Use This Document

Each policy in this collection follows a consistent structure to make customization straightforward. Replace all bracketed [fields] with your organization's specific information. Have each policy reviewed by legal counsel before formal adoption.

- Review each policy and determine which are applicable to your organization
- Replace all [bracketed placeholders] with your company-specific details
- Adjust policy statements to reflect your actual practices and risk tolerance
- Have legal counsel review the finalized policies before adoption
- Obtain executive sign-off and distribute to all employees
- Schedule annual reviews and update policies as your business evolves

Policy Templates Included

1. **Acceptable Use Policy (AUP)**
   Rules for appropriate use of company technology and systems
2. **Password & Authentication Policy**
   Requirements for passwords, MFA, and credential management
3. **Data Classification & Handling Policy**
   How to categorize, store, transmit, and dispose of data
4. **Remote Work & BYOD Security Policy**
   Security requirements for remote workers and personal devices
5. **Email & Communication Security Policy**
   Safe email practices, phishing prevention, and communication rules
6. **Vendor & Third-Party Risk Policy**
   Managing security risks from suppliers and service providers
7. **Data Breach Notification Policy**
   Procedures and timelines for breach response and notification
8. **Security Awareness Training Policy**
   Requirements for ongoing employee cybersecurity education

These templates are for informational purposes only and do not constitute legal or cybersecurity advice.

POLICY 1

Acceptable Use Policy (AUP)

1.1 Purpose

This policy defines acceptable use of [Company Name]'s information technology resources, including computers, networks, email, internet access, software, and data. It establishes baseline expectations for all users to protect the organization from security threats, legal liability, and reputational harm.

1.2 Scope

This policy applies to all employees, contractors, temporary staff, interns, and any third party granted access to [Company Name]'s technology resources, regardless of location or device.

1.3 Policy Statements

- Company technology resources are provided primarily for business purposes. Limited personal use is permitted provided it does not interfere with job duties, consume excessive resources, or violate any policy.
- Users must not attempt to access systems, files, or data they are not authorized to use. Sharing login credentials with others is strictly prohibited.
- Users must not install unauthorized software, browser extensions, or hardware on company systems without IT approval.
- Internet use must not include accessing, downloading, or distributing illegal, offensive, discriminatory, or sexually explicit material.
- Users must not use company resources for personal commercial activities, political campaigning, gambling, or any illegal purpose.
- All data created, stored, or transmitted on company systems is the property of [Company Name]. The company reserves the right to monitor, access, and review all usage without prior notice.
- Users must report any suspected security incident, unauthorized access, or policy violation to [IT Contact / Help Desk] immediately.
- Use of removable media (USB drives, external hard drives) is restricted to approved devices. Data transfers to personal storage require management approval.

1.4 Enforcement

Violations may result in disciplinary action up to and including termination of employment or contract, and may be referred for legal action. [Company Name] reserves the right to revoke access privileges at any time.

These templates are for informational purposes only and do not constitute legal or cybersecurity advice.

POLICY 2

Password & Authentication Policy

2.1 Purpose

This policy establishes requirements for creating, managing, and protecting passwords and authentication credentials to prevent unauthorized access to [Company Name]'s systems and data.

2.2 Scope

This policy applies to all users who access [Company Name]'s systems, applications, and data, including employees, contractors, and third-party vendors. It covers all passwords, PINs, tokens, and authentication methods.

2.3 Password Requirements

- Minimum length: 12 characters for standard users; 16 characters for administrative and privileged accounts.
- Passwords must include a mix of uppercase letters, lowercase letters, numbers, and special characters. Passphrases of 16+ characters are encouraged.
- Passwords must not contain the user's name, username, company name, or common dictionary words used alone.
- Passwords must be unique across all company systems. Reusing passwords from personal accounts is prohibited.
- Approved password managers (such as [Approved Tool]) must be used. Writing passwords on paper or in unencrypted files is prohibited.
- Passwords must be changed immediately if compromise is suspected. Routine forced rotation is not required if MFA is enabled.

2.4 Multi-Factor Authentication (MFA)

- MFA is required for: email, VPN, cloud services (Microsoft 365, Google Workspace), financial systems, remote desktop, and any system containing sensitive data.
- Approved MFA methods: authenticator apps (preferred), hardware security keys, and push notifications. SMS is permitted only as a temporary fallback.
- Administrative accounts must use phishing-resistant MFA (hardware keys or FIDO2) wherever supported.
- Users must register at least two MFA methods. MFA recovery codes must be stored securely in the approved password manager.

2.5 Enforcement

Accounts with weak, shared, or compromised passwords will be locked until credentials are reset. IT will conduct periodic audits of password strength and MFA enrollment across all accounts.

These templates are for informational purposes only and do not constitute legal or cybersecurity advice.

POLICY 3

Data Classification & Handling Policy

3.1 Purpose

This policy establishes a framework for classifying data based on sensitivity and defines handling, storage, transmission, and disposal requirements for each classification level.

3.2 Classification Levels

Confidential

Highest sensitivity. PII, PHI, financial records, trade secrets, credentials, legal documents.

Handling:

Encrypted at rest and in transit. Access restricted to named individuals. No external sharing without executive and legal approval.

Internal

Business-sensitive information. Internal reports, strategies, employee directories, contracts, pricing.

Handling:

Stored on company systems only. Shared internally on need-to-know basis. External sharing requires manager approval and NDA.

Public

Approved for public distribution. Marketing materials, published content, public filings.

Handling:

No distribution restrictions. Ensure accuracy before publication.

3.3 Data Handling Requirements

- All data must be classified upon creation or receipt. When in doubt, apply the higher classification level.
- Confidential data must be encrypted using AES-256 (or equivalent) at rest and TLS 1.2+ in transit.
- Confidential data must not be stored on personal devices, removable media, or unauthorized cloud services.
- Data disposal: digital files permanently deleted with approved tools; physical media shredded or degaussed.
- Data shared with third parties must be governed by a written agreement (NDA, DPA, or BAA as applicable).
- Employees must not send Confidential data via personal email, consumer messaging apps, or unencrypted channels.

© First Underwriters Insurance Brokers | www.firstunderwriters.com

These templates are for informational purposes only and do not constitute legal or cybersecurity advice.

POLICY 4

Remote Work & BYOD Security Policy

4.1 Purpose

This policy defines security requirements for employees who work remotely or use personal devices (BYOD) to access [Company Name]'s systems and data.

4.2 Remote Work Requirements

- Remote workers must connect through the approved VPN or secure access solution. Public Wi-Fi must not be used without an active VPN.
- Home networks must use WPA3 (or WPA2 minimum) encryption, a unique password, and current router firmware.
- Company devices must have full-disk encryption, automatic screen lock (5 min max), and current endpoint protection.
- Screens must not be visible to unauthorized individuals. Devices must not be left unattended in public locations.
- Critical security patches must be applied within 48 hours of release.
- Lost or stolen devices must be reported to [IT Contact] within 1 hour so remote wipe can be initiated.

4.3 BYOD Requirements

- Personal devices must be registered with IT and enrolled in MDM before accessing company data.
- Minimum requirements: current OS, device encryption, screen lock with biometric or PIN, no jailbreaking or rooting.
- Company data must be stored within managed applications only. Data must not be copied to personal apps or storage.
- [Company Name] may remotely wipe company data from personal devices upon termination, loss, or policy violation.
- BYOD access may be revoked if the device fails to meet security requirements.

4.4 Enforcement

Devices found non-compliant will have access suspended until brought into compliance. Repeated violations may result in permanent revocation of remote work or BYOD privileges and disciplinary action.

© First Underwriters Insurance Brokers | www.firstunderwriters.com

These templates are for informational purposes only and do not constitute legal or cybersecurity advice.

POLICY 5

Email & Communication Security Policy

5.1 Purpose

This policy establishes requirements for the secure use of email and business communication tools to protect [Company Name] from phishing, business email compromise, data leakage, and social engineering attacks.

5.2 General Email Security

- Company email accounts must be used for all business communications. Personal email must not be used for company data.
- Verify sender identity before responding to requests for sensitive information, wire transfers, or payment detail changes. Verify through a separate channel (phone call to a known number).
- Report suspicious emails to [IT/Security Contact] using the report phishing button. Do not forward to other employees.
- Do not open attachments from unknown senders. Verify unexpected attachments from known senders before opening.
- Confidential data must not be sent via unencrypted email. Use approved secure file-sharing tools.
- Automatic email forwarding to external addresses is prohibited without IT and management approval.
- Out-of-office replies to external senders should contain minimal information.

5.3 Communication Tools

- Approved tools: [Teams / Slack / etc.]. Consumer messaging apps must not be used for company data.
- Video meetings with sensitive content must use waiting rooms and participant authentication.
- Chat messages are subject to the same data handling requirements as email.

Wire Transfer & Payment Verification

Any request to change payment details, wire money, or redirect payments must be verified through a separate phone call to a known number. This is the #1 way businesses lose money to cybercrime.

These templates are for informational purposes only and do not constitute legal or cybersecurity advice.

POLICY 6

Vendor & Third-Party Risk Policy

6.1 Purpose

This policy governs how [Company Name] evaluates, monitors, and manages cybersecurity risks introduced by vendors, suppliers, contractors, and other third parties who access company data or systems.

6.2 Vendor Assessment Requirements

- All vendors accessing company data must complete a security assessment before onboarding, proportional to data sensitivity and access level.
- High-risk vendors must provide: current SOC 2 report (or equivalent), cyber insurance, incident response plan, encryption practices, and employee training evidence.
- Medium-risk vendors must complete a security questionnaire and provide evidence of basic security controls.
- Assessments refreshed annually for high-risk vendors, every two years for medium-risk.

6.3 Contractual Requirements

- Vendor agreements must include: security requirements, data handling obligations, breach notification within 24 hours, and right-to-audit provisions.
- Vendors must agree to DPA, BAA (where HIPAA applies), and NDA as appropriate.
- Vendors must limit data access to the minimum necessary and must not share with sub-processors without written approval.
- Agreements must specify data return and secure deletion upon contract termination.

6.4 Ongoing Monitoring

- Maintain current inventory of all vendors with data or system access, including data classification and access method.
- Revoke vendor access promptly when the business relationship ends.
- Escalate any vendor security incident affecting company data to the Incident Response Team immediately.

These templates are for informational purposes only and do not constitute legal or cybersecurity advice.

POLICY 7

Data Breach Notification Policy

7.1 Purpose

This policy establishes procedures for notifying affected individuals, regulators, law enforcement, and business partners in the event of a data breach involving personal or sensitive information.

7.2 Definition of a Data Breach

A data breach is any unauthorized acquisition, access, use, or disclosure of unencrypted personal information that compromises its security, confidentiality, or integrity. This includes lost/stolen unencrypted devices, unauthorized email access, ransomware with suspected exfiltration, and accidental disclosure.

7.3 Notification Timeline

Notify	Deadline	Method
Cyber Insurance Carrier	Within 24 hours	Phone + written
Breach Coach / Legal	Within 24 hours	Phone
Affected Individuals	30–60 days (per state law)	Written notice
State Attorney General	Per state statute	Per state req.
HHS (HIPAA breaches)	Within 60 days	HHS portal
FBI / IC3 (ransomware)	Within 72 hours	ic3.gov
Business Partners	Per contract	Written notice

7.4 Notification Content

- General description of the breach including approximate date and nature of incident.
- Types of personal information involved (names, SSN, financial accounts, health info, etc.).
- Steps [Company Name] is taking to investigate, mitigate, and prevent future occurrences.
- Actions affected individuals can take to protect themselves (credit monitoring, password changes).
- Dedicated contact information for questions.

Insurance Coordination Required

Contact your cyber insurance carrier BEFORE engaging forensics, legal, or notification vendors. Most policies provide panel providers. Using non-panel providers without approval may result in costs not being covered.

These templates are for informational purposes only and do not constitute legal or cybersecurity advice.

POLICY 8

Security Awareness Training Policy

8.1 Purpose

This policy requires all [Company Name] personnel to participate in ongoing cybersecurity awareness training. Employees are both the greatest vulnerability and the strongest defense against cyber threats.

8.2 Training Requirements

- New employees must complete cybersecurity training within 30 days, before receiving full system access.
- All employees must complete annual refresher training covering current threats, updated policies, and best practices.
- Targeted role-based training required for: IT administrators, finance/accounting staff, executives, and Confidential data handlers.
- Phishing simulations must be conducted quarterly. Employees who repeatedly fail must complete additional training within 14 days.

8.3 Required Training Topics

- Recognizing phishing emails, social engineering, and business email compromise attempts
- Password security, MFA usage, and credential hygiene
- Safe internet and email practices, file download and USB drive risks
- Data classification, handling procedures, and reporting requirements
- Physical security: clean desk policy, visitor management, secure printing
- Incident reporting: how to recognize and report a potential security incident
- Remote work security including home network and public Wi-Fi risks
- Social media security: protecting company information in public forums

8.4 Tracking & Compliance

[IT / HR Department] maintains training records. Compliance rates reported to management quarterly. Employees who fail to complete training may have access restricted. Records retained for minimum [3 years].

© First Underwriters Insurance Brokers | www.firstunderwriters.com

These templates are for informational purposes only and do not constitute legal or cybersecurity advice.

Policy Adoption Checklist

Use this checklist to track your progress in customizing and implementing each security policy.

- [ ] Identify which policies apply to your organization based on size, industry, and regulatory requirements
- [ ] Replace all [bracketed fields] with your company-specific details
- [ ] Adjust policy statements to reflect your actual technology environment and risk tolerance
- [ ] Have legal counsel review all policies for compliance with applicable laws
- [ ] Obtain executive approval and formal sign-off on each policy
- [ ] Distribute policies to all employees and require written acknowledgment
- [ ] Conduct initial training on all new policies within 30 days of adoption
- [ ] Publish policies in a central, accessible location (intranet, shared drive, handbook)
- [ ] Schedule annual policy reviews and assign a policy owner for each document
- [ ] Share relevant policies with your insurance broker for cyber insurance applications
- [ ] Include policy compliance verification in regular security audits
- [ ] Update policies when significant changes occur (new systems, regulations, incidents)

Need Cyber Insurance That Recognizes Your Security Efforts?

First Underwriters helps small businesses get the right coverage at the right price.
Strong security policies can improve your insurability and reduce premiums.

www.firstunderwriters.com

These templates are for informational purposes only and do not constitute legal or cybersecurity advice.