example

Policy Owner:	IT Manager / Security Lead
Effective Date:	January 1, 2025
Version:	1.0
Classification:	Internal Use Only

Information Security Policy

Small/Medium Business Edition

Information Security Policy

Part 1: Core Policy

0.1 How to Use This Policy

This policy is your guide to keeping our company's information safe. Whether you're handling customer data, working on financial records, or just sending emails, security is everyone's job.

Start here if you're:- New to the company → Read sections 1.1-1.3 first
- Looking for specific guidance → Use the table of contents or Quick Help section
- Not sure if something is secure → Contact your IT Manager or Security Lead

What you'll find in this policy:- What information security means for our business (Section 1.1)
- Your security responsibilities (Section 1.3)
- How to protect our data and systems (Sections 1.4-1.9)
- Where to get help (Throughout, plus Part 2)

Need help?Contact your IT Manager or Security Lead. Security questions are always welcome—it's better to ask than to guess.

1.1 What This Covers

What is information security?Information security means protecting our company's data, systems, and reputation from theft, damage, or misuse. It's about making sure:
- Our data stays confidential (only the right people can see it)
- Our data stays accurate and complete (integrity)
- Our systems work when we need them (availability)

Why do we need this policy?-Protect our business: Data breaches are expensive and damage our reputation
-**Protect our customers:**They trust us with their information
-**Meet legal requirements:**Laws like HIPAA, PCI DSS, and privacy regulations require security
-**Qualify for contracts:**Many customers require proof of security practices
-**Enable growth:**Good security practices help us scale safely

Who does this apply to?Everyone who works with our information or systems:
- All employees (full-time, part-time)
- Contractors and consultants
- Vendors and partners who access our systems
- Anyone using company equipment or data

What does this cover?- All company information (digital and physical)
- All systems and devices (computers, phones, servers, cloud services)
- All locations (office, home, client sites, anywhere you work)
- All communication (email, messaging, video calls)

What's out of scope?Personal use of company equipment outside work hours is covered by our Acceptable Use Policy. This policy focuses on protecting business information and systems.

1.2 Key Terms

Information Security: Protecting our data, systems, and business from threats like hackers, accidents, or theft.

Confidentiality: Keeping sensitive information private and only accessible to authorized people.

Integrity: Making sure data is accurate, complete, and hasn't been tampered with.

Availability: Ensuring systems and data are accessible when needed for business operations.

Information Asset: Anything that has value to our business—customer data, financial records, employee information, intellectual property, systems, etc.

Risk: The possibility that something bad could happen to our information or systems (like a data breach or system failure).

Security Control:A safeguard or countermeasure we put in place to reduce risk (like passwords, firewalls, or locked doors).

Security Incident: Any event that could harm our information security—suspicious emails, lost devices, unauthorized access, system breaches, etc.

Data Classification: Categorizing information based on sensitivity (Public, Internal, or Confidential) to determine how to protect it.

1.3 Roles: Who Does What

Everyone has a role in keeping our company secure. Here's who does what:

Leadership Team (CEO, Owners)- Set the tone that security matters
- Provide resources for security (budget, tools, training)
- Review security status quarterly
- Make decisions on major security investments

IT Manager / Security Lead- Manage day-to-day security
- Implement security tools and controls

- Respond to security incidents
- Provide security guidance and training
- Keep this policy up to date

Managers and Team Leads- Enforce security policies with your team
- Make sure your team completes security training
- Report security concerns promptly
- Model good security behavior

All Employees (That's You!)- Follow security policies and procedures
- Use strong passwords and protect your login
- Lock your screen when you step away
- Report suspicious emails or activity immediately
- Complete required security training
- Think before you click or share information
- Ask questions if you're unsure

Vendors and Contractors- Follow our security requirements
- Protect any company information you access
- Report security issues immediately
- Sign vendor security agreements

Role	Key Responsibilities	What This Means for You
Everyone	Basic security hygiene	Strong passwords, lock screen, report incidents
Managers	Team security oversight	Ensure team follows policies, address violations
IT/Security Lead	Security program management	Implement controls, respond to incidents, provide guidance
Leadership	Security investment & accountability	Fund security, review risks, support culture

1.4 Security Governance and Organization

How security fits into our business Security isn't just IT's job—it's built into how we run our business. We take a practical, risk-based approach:
- Identify what needs protection (customer data, financial records, intellectual property)
- Assess realistic risks we face
- Implement reasonable protections
- Monitor and improve over time

Who's in charge?-IT Manager/Security Lead: Runs our day-to-day security program
-**Leadership Team:**Reviews security status quarterly and approves major decisions
-**Everyone:**Responsible for following policies and reporting issues

Our security policies This Information Security Policy is our master policy. We also have supporting policies for specific areas:
- Access Control Policy (who can access what)
- Data Management Policy (handling sensitive data)
- Acceptable Use Policy (using company resources appropriately)
- Incident Response Plan (what to do when something goes wrong)
- Business Continuity Plan (keeping the business running during disruptions)

All policies work together to create a comprehensive security framework.

Staying compliant We follow security requirements from:
- Industry regulations (HIPAA if healthcare, PCI DSS if processing payments)
- Customer contracts (many customers require security practices)
- SOC 2 compliance (demonstrates security to customers and partners)
- Privacy laws (protecting personal information)

Our IT Manager tracks compliance requirements and conducts internal reviews to ensure we're meeting our obligations.

Measuring our security We track key metrics to know if our security is working:
- Security training completion rates
- Number and severity of security incidents
- Time to respond to and resolve incidents
- Vulnerabilities found and fixed
- Compliance audit results

Leadership reviews these metrics quarterly to make informed decisions about security investments.

1.5 Risk Management Basics

What is risk management?Risk management means understanding what could go wrong and taking reasonable steps to prevent it. We don't need to eliminate every possible risk—that's impossible—but we need to manage risks to acceptable levels.

How we assess risks At least once a year, we:
1.**Identify assets:**What do we need to protect? (customer data, financial systems, intellectual property)
2.**Identify threats:**What could go wrong? (hackers, malware, lost devices, employee mistakes)
3.**Assess impact:**How bad would it be if something happened?
4.**Evaluate likelihood:**How likely is this to happen?
5.**Prioritize risks:**Focus on the biggest risks first

How we handle risks For each significant risk, we choose an approach:
-**Mitigate:**Implement controls to reduce the risk (most common)
-**Accept:**Acknowledge the risk but don't take additional action (for low risks)

-**Avoid:**Stop the risky activity (rare, but sometimes necessary)
-**Transfer:**Use insurance or contracts to share the risk

Your role in risk management-**Report risks you see:**If something seems unsafe or insecure, speak up
-**Follow security controls:**Controls exist for a reason—use them
-**Don't take unnecessary risks:**If you're unsure whether something is safe, ask first
-**Learn from incidents:**When something goes wrong, help us understand why so we can prevent it next time

Example: Risk-based thinking in action-**High Risk:**Customer credit card data → Strong encryption, limited access, regular audits
-**Medium Risk:**Internal project plans → Standard access controls, regular backups
-**Low Risk:**General company news → Basic access controls, available to all employees

1.6 Asset Management

What are information assets?Anything valuable to our business:
-**Data:**Customer information, financial records, employee data, business plans, trade secrets
-**Systems:**Servers, cloud services, databases, applications
-**Devices:**Laptops, phones, tablets, USB drives
-**Physical assets:**Paper documents, backup tapes, locked cabinets

Tracking our assets We maintain an inventory of critical assets including:
- What it is (system, device, data type)
- Where it is (location, owner, department)
- How sensitive it is (data classification)
- How we protect it (security controls in place)

Data classification simplified We classify information into three levels:

Classification	What It Means	Examples	How to Protect
Public	Anyone can see it	Marketing materials, job postings, public website content	No special protection needed
Internal	For employees only	Internal policies, company news, project plans	Don't share outside company
Confidential	Restricted access	Customer data, financial records, trade secrets, employee personal info	Encrypt, limit access, extra protections

How to classify data When creating or receiving information, ask yourself:
1. Would it harm our business if this got out? → Probably Confidential
2. Is this only for internal use? → Probably Internal
3. Is this okay for anyone to see? → Probably Public

When in doubt, classify higher and ask your manager or IT.

Protecting physical assets- Lock confidential documents in secure areas
- Shred sensitive documents before disposal
- Don't leave devices unattended
- Return company equipment when you leave

Your responsibilities- Classify data appropriately
- Handle information according to its classification
- Report lost or stolen devices immediately
- Don't store company data on personal devices without approval

1.7 Security Controls

Security controls are the safeguards we use to protect our information and systems. Here are the key controls everyone needs to know:

Access Controls: Who Gets In-**Strong passwords:**Use at least 12 characters, mix letters, numbers, and symbols
-**Multi-factor authentication (MFA):**Required for remote access and sensitive systems
-**Unique accounts:**Never share passwords or accounts
-**Least privilege:**You get access to what you need for your job, nothing more
-**Access reviews:**We review who has access regularly and remove unnecessary access

What you need to do:- Create strong, unique passwords for each account
- Enable MFA when prompted
- Never share your password
- Request access through proper channels
- Tell IT immediately if you don't need access anymore

Endpoint Security: Protecting Devices-**Antivirus/anti-malware:**Required on all devices accessing company systems
-**Automatic updates:**Keep your devices updated with security patches
-**Encryption:**Confidential data must be encrypted
-**Screen lock:**Set your device to lock after 10 minutes of inactivity
-**Lost device protocol:**Report lost devices immediately for remote wipe

What you need to do:- Don't disable security software
- Install updates when prompted
- Lock your screen when you step away
- Report lost or stolen devices immediately

Network Security: Safe Connections-**Secure Wi-Fi:**Use company VPN on public Wi-Fi
-**Firewall protection:**Protects our network from external threats
-**Network segmentation:**Critical systems are separated for additional protection
-**Safe browsing:**Be cautious about websites you visit on company devices

What you need to do:- Use company VPN when working remotely
- Don't connect to untrusted networks without VPN
- Be cautious on public Wi-Fi
- Report suspicious network activity

Data Protection: Keeping Information Safe-**Encryption:**Confidential data is encrypted at rest and in transit
-**Secure transmission:**Use approved tools for sharing sensitive information
-**Backup and recovery:**Critical data is backed up regularly
-**Data retention:**We keep data only as long as needed
-**Secure disposal:**Confidential data is securely deleted when no longer needed

What you need to do:- Don't email confidential data without encryption
- Use approved file sharing tools
- Don't store confidential data on personal devices
- Contact IT for secure data disposal

Physical Security: Protecting Physical Assets-**Building access:**Secure doors, visitor management
-**Clean desk policy:**Don't leave confidential documents out
-**Visitor escorts:**Visitors must be escorted in secure areas
-**Secure disposal:**Shred confidential documents

What you need to do:- Don't let unauthorized people follow you through secure doors
- Lock confidential documents when not in use
- Escort visitors in your area
- Use shred bins for confidential paper

Third-Party Security: Vendor Management-**Vendor assessments:**We assess vendors before they access our systems
-**Contracts:**Vendors sign security agreements
-**Limited access:**Vendors get only the access they need
-**Monitoring:**We monitor vendor access

What you need to do:- Involve IT before giving vendor access to systems
- Don't share company data with vendors without approval
- Report concerns about vendor security practices

1.8 Security Monitoring

Why we monitor We monitor our systems to:
- Detect security incidents quickly
- Identify suspicious activity
- Ensure security controls are working
- Meet compliance requirements

What we monitor- System logs and activity
- Network traffic
- Failed login attempts
- Antivirus alerts
- Changes to sensitive data
- User access and activities

Security incident response If something goes wrong, we have a plan:

1. **Detect:**Identify potential security incident
2. **Report:**Report immediately to IT Manager/Security Lead
3. **Contain:**Stop the incident from spreading
4. **Investigate:**Understand what happened and why
5. **Recover:**Restore normal operations
6. **Learn:**Improve controls to prevent recurrence

What counts as a security incident?- Suspicious emails (phishing attempts)
- Malware or virus detections
- Unauthorized access attempts
- Lost or stolen devices
- Data breaches or leaks
- Unusual system behavior
- Accidental disclosure of confidential information

What to do if you spot something suspicious1.**Don't panic**– most issues can be resolved quickly
2.**Stop what you're doing**– don't make it worse
3.**Don't click on suspicious links or attachments**4.**Report immediately**to IT Manager/Security Lead
5.**Document what happened**– when, what, how
6.**Preserve evidence**– don't delete emails or files
7.**Follow instructions**from IT on next steps

Contact information for incidents:- IT Manager: [Contact Information]
- Security Lead: [Contact Information]
- After hours: [Emergency Contact]

Remember: Reporting quickly helps us minimize damage. You won't get in trouble for reporting suspicious activity—even if it turns out to be nothing.

1.9 Security Awareness

Why security awareness matters Most security breaches start with human error—a clicked phishing link, a weak password, or a lost device. Security awareness training helps you recognize and avoid these threats.

Required training All employees must complete:
- Security awareness training upon hire
- Annual refresher training
- Specialized training for your role (if applicable)
- Training on policy updates when changes occur

What you'll learn- How to recognize phishing and social engineering
- Password best practices
- Safe browsing and email habits
- How to protect confidential data
- What to do if something goes wrong
- Current security threats and trends

Practical security tips-Think before you click: Hover over links before clicking, verify sender identity
-**Be skeptical:**If something seems too good to be true or urgent, it probably is
-**Verify requests:**If someone asks for sensitive information, verify through another channel
-**Protect passwords:**Don't write them down, don't share them, don't reuse them
-**Lock your screen:**Every time you walk away, even for a minute
-**Report suspicious activity:**See something, say something

Phishing red flags Watch out for:
- Urgent requests for action ("Your account will be suspended!")
- Requests for sensitive information (passwords, financial data)
- Generic greetings ("Dear Customer")
- Suspicious sender addresses (close but not quite right)
- Spelling and grammar errors
- Suspicious links or attachments

When in doubt:- Don't click
- Don't provide information
- Don't download attachments
- Forward to IT and delete

1.10 What Happens If Violated

We take security seriously Security policies exist to protect our business, our customers, and you. Violations can have serious consequences.

Types of violations- Using weak or shared passwords
- Sharing confidential information inappropriately
- Ignoring security warnings or alerts
- Disabling security software
- Not reporting security incidents
- Intentionally bypassing security controls
- Misusing access privileges

Progressive discipline approach We handle violations fairly and proportionally:

Minor violations (first offense, no harm):- Verbal or written warning
- Required retraining
- Closer supervision

Moderate violations (repeated or reckless):- Written warning in personnel file
- Temporary access restrictions
- Mandatory additional training
- Performance improvement plan

Serious violations (intentional or causing harm):- Suspension
- Termination of employment
- Legal action (for illegal activities)
- Reporting to authorities (if required by law)

Investigating violations If we suspect a policy violation:
- We'll investigate fairly and confidentially
- You'll have a chance to explain your side
- We'll consider intent, circumstances, and impact
- Decisions will be documented

If you make a mistake:-**Report it immediately**– we can often minimize the damage
-**Be honest**– trying to hide mistakes makes things worse
-**Learn from it**– mistakes happen, but don't repeat them
-**Cooperate**– help us understand what happened and why

Remember: Most security incidents happen by accident, not malice. If you report mistakes quickly and honestly, we'll work with you to fix them and prevent recurrence.

Part 2: Quick Help

FAQ

1. What is information security and why does it matter?Information security means protecting our company's data, systems, and reputation from theft, damage, or misuse. It matters because:
- Data breaches are expensive and damage our reputation

- We're legally required to protect certain information
- Our customers trust us with their data
- Good security enables business growth

2. What are my security responsibilities?Every employee is responsible for:
- Following security policies and procedures
- Using strong passwords and protecting your login credentials
- Locking your screen when away from your desk
- Reporting security incidents or suspicious activity immediately
- Completing required security training
- Handling confidential information appropriately
- Asking questions when you're unsure

3. How do I classify data?Use this quick guide:
-**Public:**Anyone can see it (marketing materials, public website content)
-**Internal:**For employees only (internal policies, project plans)
-**Confidential:**Restricted access (customer data, financial records, trade secrets)

When in doubt, classify higher and ask your manager or IT.

4. Can I work on my personal laptop or use personal devices?Generally no. Company work should be done on company-provided devices that have proper security controls. If you need to use a personal device:
- Get approval from your manager and IT
- Install required security software
- Follow all security policies
- Understand that company data on personal devices may need to be wiped if the device is lost

5. What's the most important thing I can do for security?Be aware and cautious. Think before you click on links or open attachments. If something seems suspicious or too good to be true, it probably is. Report suspicious activity immediately. Most security breaches start with a simple mistake—your awareness is our best defense.

6. What if I accidentally click a phishing link or make a security mistake?Don't panic and don't be embarrassed. Report it to IT immediately:
1. Stop what you're doing
2. Don't click anything else
3. Contact IT Manager or Security Lead right away
4. Change your password if you entered credentials
5. Follow IT's instructions

The faster you report it, the less damage it can cause. You won't get in trouble for reporting an honest mistake.

7. Who do I contact for security questions?- General questions: IT Manager [Contact]
- Security incidents: Security Lead [Contact]

- After hours emergencies: [Emergency Contact]
- HIPAA questions (if applicable): Privacy Officer [Contact]
- PCI questions (if applicable): Compliance Lead [Contact]

Common Situations

Situation: You receive an email that looks suspicious-Don't clickon any links or attachments
-**Check the sender:**Is the email address legitimate? Hover over links without clicking.
-**Look for red flags:**Urgency, generic greetings, requests for sensitive information
-**Action:**Forward the email to IT and then delete it. If it claims to be from a coworker, verify through another channel (call or instant message them).

Situation: You need to share confidential information with a coworker-**Use approved tools:**Company email or secure file sharing (ask IT which tools are approved)
-**Verify recipient:**Make sure you're sending to the right person
-**Encrypt if necessary:**For highly sensitive data, ask IT about encryption
-**Action:**Don't email confidential information without encryption. Use secure file sharing tools. When in doubt, ask IT.

Situation: Working from home or traveling-**Use company VPN:**Always connect through VPN when accessing company systems remotely
-**Secure your workspace:**Work in a private area where others can't see your screen
-**Public Wi-Fi:**Avoid if possible. If you must use it, always use VPN.
-**Action:**Before working remotely, make sure you have VPN installed and configured. Contact IT for help.

Situation: Lost or stolen device (laptop, phone, tablet)-**Time is critical:**The faster we act, the better we can protect company data
-**Contact IT immediately:**Don't wait, even if it's after hours. Call emergency contact.
-**Remote wipe:**IT can remotely wipe company data from the device
-**Action:**Report immediately to IT Manager or Security Lead. Provide device details (type, last location, what was on it). File a police report if stolen.

Situation: A vendor or contractor asks for access to company systems-**Don't provide access yourself:**Involve IT first
-**Proper approval needed:**Vendor access requires security assessment and approval
-**Limited access:**Vendors should only get access they need, for as long as they need it
-**Action:**Contact IT Manager to initiate vendor access request. IT will assess security and set up appropriate access.

Quick Reference Checklist

Daily Security Habits:- ☐ Use strong, unique passwords (12+ characters)
- ☐ Enable multi-factor authentication (MFA) where required

- ☐ Lock your screen every time you step away
- ☐ Think before you click on links or attachments
- ☐ Verify sender identity for sensitive requests
- ☐ Keep your devices updated with security patches

Handling Confidential Data:- ☐ Classify data appropriately (Public, Internal, Confidential)
- ☐ Encrypt confidential data when sharing
- ☐ Don't store company data on personal devices
- ☐ Use approved file sharing tools
- ☐ Shred confidential paper documents

Incident Response:- ☐ Report security incidents immediately
- ☐ Don't try to fix it yourself – call IT
- ☐ Preserve evidence (don't delete emails or files)
- ☐ Document what happened
- ☐ Follow IT's instructions

Training and Awareness:- ☐ Complete required security training
- ☐ Stay informed about current threats
- ☐ Ask questions when unsure
- ☐ Report suspicious activity

Remember: When in doubt, ask. Security questions are always welcome!

Part 3: Framework Addendums

HIPAA Quick Guide

What's Different for HIPAA

If we handle patient health information (PHI), HIPAA requires comprehensive security measures:

Key HIPAA requirements:-**Risk Analysis:**Conduct annual risk analysis specifically for systems that store, process, or transmit PHI
-**Security Safeguards:**Implement administrative, physical, and technical safeguards to protect PHI
-**Policies and Procedures:**Document all security policies and procedures (keep for 6 years)
-**Workforce Training:**All workforce members who handle PHI must receive HIPAA security training
-**Business Associate Agreements:**Sign agreements with any vendors who access PHI

-**Breach Notification:**Report breaches of unsecured PHI to HHS and affected individuals

What this means for you:- PHI gets extra protection beyond our normal "Confidential" classification
- You need specific training before accessing PHI
- You must follow strict access controls for PHI
- You must report any potential PHI breach immediately
- No personal devices for PHI without approval and encryption

Quick Compliance Checklist- ☐ Conduct annual risk analysis for all systems with PHI
- ☐ Implement required safeguards (administrative, physical, technical)
- ☐ Document all security policies and procedures
- ☐ Provide HIPAA security training to all workforce members
- ☐ Execute Business Associate Agreements with vendors accessing PHI
- ☐ Establish breach notification procedures
- ☐ Review and update HIPAA security policies annually
- ☐ Maintain documentation for at least 6 years

When to Get Help Contact your Privacy Officer or HIPAA Compliance Lead if:
- You're handling patient health information for the first time
- You need to conduct HIPAA risk analysis
- A vendor needs access to PHI (need Business Associate Agreement)
- You suspect a PHI breach or security incident
- You have questions about HIPAA requirements

ISO 27001 Quick Guide

What's Different for ISO 27001

ISO 27001 requires a formal Information Security Management System (ISMS):

Key ISO 27001 requirements:-**Information Security Policy:**Documented policy (this document) communicated to all stakeholders
-**Risk Assessment:**Formal risk assessment methodology and regular assessments
-**Statement of Applicability:**Document which ISO controls apply to your organization
-**Internal Audits:**Conduct regular internal audits of your ISMS
-**Management Review:**Leadership reviews ISMS performance at planned intervals
-**Continual Improvement:**Ongoing process to improve security effectiveness

What this means for you:- More formal documentation and record-keeping
- Regular audits and reviews of security practices
- Structured approach to risk management
- Continuous improvement mindset
- Evidence collection for certification audits

Quick Compliance Checklist- ☐ Information security policy documented and approved by management
- ☐ Policy communicated to all relevant parties
- ☐ Risk assessment conducted and documented
- ☐ Statement of Applicability created and maintained
- ☐ Security controls implemented based on risk assessment
- ☐ Internal audits conducted at planned intervals
- ☐ Management reviews ISMS performance regularly
- ☐ Nonconformities tracked and corrective actions taken
- ☐ Evidence maintained for certification audits

When to Get Help Contact your CISO or Information Security Manager if:
- You're implementing an ISMS for the first time
- You're preparing for ISO 27001 certification audit
- You need guidance on ISO 27001 controls
- You're conducting internal audits
- You need help with Statement of Applicability

PCI DSS Quick Guide

What's Different for PCI DSS

If we process, store, or transmit credit card data, PCI DSS requires:

Key PCI DSS requirements:-**Security Policy:**Comprehensive information security policy addressing all PCI requirements (Requirement 12.1)
-**Annual Risk Assessment:**Conduct annual risk assessment for the cardholder data environment
-**Usage Policies:**Document acceptable use policies for all technologies and critical systems
-**Annual Review:**Review and update all security policies at least annually
-**Security Awareness:**Maintain ongoing security awareness program for all personnel
-**Policy Dissemination:**Ensure all policies are disseminated to relevant personnel
-**Acknowledgment:**Obtain acknowledgment from personnel that they've read and understood policies

What this means for you:- Extra protections for credit card data (never store full card numbers or CVV codes)
- Strict access controls for cardholder data environment (CDE)
- Additional training if you access credit card systems
- Regular compliance assessments
- Extensive documentation requirements

Quick Compliance Checklist- ☐ Security policy covers all PCI DSS requirements
- ☐ Annual risk assessment for cardholder data environment completed

- ☐ Usage policies documented for all critical technologies
- ☐ Annual policy review and update conducted
- ☐ Security awareness training provided to all personnel with CDE access
- ☐ Policies disseminated to all relevant personnel
- ☐ Policy acknowledgment forms collected and maintained
- ☐ Quarterly PCI compliance monitoring
- ☐ Annual PCI assessment (SAQ or audit) completed

When to Get Help Contact your PCI Compliance Lead or IT Manager if:
- You're processing credit card payments for the first time
- You have questions about PCI compliance requirements
- You need to conduct annual PCI risk assessment
- You're preparing for PCI audit or SAQ completion
- You need guidance on cardholder data security

Appendices

Evidence Checklist

Auditors will look for:
- This Information Security Policy (current version, approved)
- Annual risk assessment report
- Security training completion records for all employees
- Policy acknowledgment forms (signed by all employees)
- Security incident reports and investigation documentation
- Access review logs
- Security metrics and reports to leadership
- Policy review and update documentation

Template List

Required templates and forms (available separately):
-**Risk Assessment Template:**For conducting annual risk assessments
-**Asset Inventory Template:**For tracking information assets
-**Security Incident Report Form:**For documenting security incidents
-**Policy Acknowledgment Form:**For employee policy acceptance
-**Access Request Form:**For requesting system access
-**Vendor Security Assessment:**For evaluating third-party security
-**Security Training Attendance Sheet:**For documenting training

Contact these templates through your IT Manager or download from our document management system.