# Privacy Toolkit 2026

## Introduction

Running a small business, nonprofit organization, or local government agency takes hard work and resilience. You've already overcome countless challenges to keep things running smoothly. The last thing you want to hear is that there's more to do—but if you collect or handle personal information, protecting it isn't optional. It's essential for safeguarding the privacy of your customers and employees, and for complying with modern laws.

Developed members of the Indiana Executive Council on Cybersecurity's Privacy Working Group, this toolkit is intended to provide practical steps to help you meet legal obligations, reduce risk, and maintain trust.

## Step 1: Know Your Data and Guidelines

Not only must you abide by federal and Indiana privacy laws listed below, but you also need to comply with the laws of the states your customers live in. If your organization serves a national audience, you may want to adapt your practices to California privacy laws because they have the most stringent requirements in the US. If your organization has a global customer base, consider compliance with the European Union's (EU) General Data Protection Regulation (GDPR) because it has the most stringent requirements worldwide. In addition, consider applying requirements of the following regulatory frameworks:

- If you handle **health and medical information**, the Health Insurance Portability and Accountability Act (HIPAA) and Federal Trade Commission (FTC) Health Breach Notification Rule.
- If you're a **financial institution** handling customer data, the Gramm-Leach-Bliley Act (GLBA).
- If you collect or use **consumer credit information**, the Fair Credit Reporting Act (FCRA).
- If you handle **credit and debit card information**, the Payment Card Industry Data Security Standard (PCI DSS).
- If you collect information from **children under 13**, the Children's Online Privacy Protection Act (COPPA).

- If you're doing business with **individuals in Indiana**, the Indiana Consumer Data Protection Act will be applicable and serve as a meaningful resource.

## Core Privacy Principles

- Implement Privacy by Design from the start if you haven't established your organization yet. This will make your business or nonprofit less risky and more compliant into the future.
- Implement opt-in/opt-out mechanisms on your websites so visitors and customers will know how their data will be shared and used by you and your partners. This will also enable them to decide whether to accept the risks.
- Restrict access to and encrypt sensitive personal information like financial, health, location, biometrics, and children's data.
- Use Data Processing Agreements (DPAs) and enforce notification timelines when your vendors handling your customers' data are breached.
- Follow NIST Artificial Intelligence (AI) Risk Management Framework guidance to ensure you're complying with privacy best practices while using AI and automation.

## Step 2: Implement Privacy Controls

Security and privacy controls reduce risk. Examples include:

- Limit access based on job roles. This is known as the least privilege principle.
- Use multi-factor authentication (MFA) to assure only users can log into their accounts.
- Encrypt data at rest and in transit.
- Regularly update software and apply security patches either manually, or by enabling automatic updates.
- Conduct regular staff training on phishing and social engineering risks—have fun with this and make it educational!

## Step 3: Respond to Breaches

Breaches can happen even when you comply with laws and implement best practices. Follow these steps when you experience one:

### Notification

- Notify affected individuals promptly as required by law.

- Report the breach to Indiana state authorities and regulators using this form: Microsoft Word - Indiana Data Breach Notification Form 8-4-2020
- For additional information related Indiana's Security Breach Notification Statute: https://www.in.gov/attorneygeneral/consumer-protection-division/id-theft-prevention/security-breaches/security-breach-faqs-and-notification-form-for-businesses/
- Notify law enforcement if criminal activity is suspected.
- Prepare public statements and FAQs for customers and stakeholders.

### Recovery

- Restore systems from clean backups.
- Verify integrity of restored data and systems.
- Apply security patches and strengthen defenses.
- Resume normal operations after confirming containment and recovery.
- Inform your audience and customers of what happened and what you did to protect their privacy. This can help to reassure their confidence in your organization.

## Resources

CISA Incident Response Playbook: https://www.cisa.gov/sites/default/files/2024-08/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf

Policy Templates: https://www.sans.org/information-security-policy