Personally Identifiable Information (PII)
Guidebook 3.0

Privacy Working Group of the
Indiana Executive Council on Cybersecurity
July 2026

CONTENTS

Introduction to the PII Guidebook

Formed by the Indiana Executive Council on Cybersecurity, the Privacy Working Group (PWG) (the "Privacy Working Group") is comprised of private and public sector leaders in Indiana's privacy and cybersecurity realms. Following on the work that was completed by members of the PII Working Group in 2021, the Privacy Working Group has been tasked with updating this guide for the purpose of: defining and characterizing the use and protection of PII, including:

- identifying related regulations
- addressing potential future developments; and
- describing best practices and providing sample policies that can be implemented by organizations in any sector with the aim of mitigating cyber threats to PII while enhancing the privacy, security, accuracy, availability, and integrity of digital information.

This Guidebook is intended as a free-to-download resource and to be used by Indiana organizations, small and large, about how to protect information and data assets. And the use, storage and transfer of PII creates organizational risks that can be mitigated and managed.

For example, the inadvertent disclosure of PII can cause operational, legal, regulatory and reputational risks and related expenses. However, such risks can be managed and mitigated by always knowing what PII the organization has and by using a variety of organizational strategies with the PII in mind; for example, by collecting only the minimally necessary PII required for the business purpose, deleting PII that is no longer in use, and purchasing relevant insurance coverage. This Guidebook discusses all of this in more detail.

Acknowledgements

We extend our sincere gratitude to the members of the Indiana Executive Council on Cybersecurity's (IECC) PII Working Group, whose leadership and expertise from both the public and private sectors laid the foundation for the original edition of this guide in 2021. Their commitment to advancing privacy and cybersecurity in Indiana was instrumental in shaping this important resource.

We also thank the IECC's Privacy Working Group for their subject matter expertise and valuable contributions to this 2024 update. Their insights have ensured that the guide remains relevant and responsive to today's evolving privacy landscape.

Special recognition is given to the leadership and members of the IECC—past and present—for their continued dedication to cyber governance on behalf of all Hoosiers.

Finally, we acknowledge former Governor Eric Holcomb for establishing the IECC through Executive Order 17-11, and we recognize Governor Mike Braun and his administration for continuing to support and advance Indiana's cybersecurity strategy through this updated publication.

DEFINING PII

PII Guidance Sources and Definitions

This section outlines key federal and state regulations, standards, and guidance documents that define Personally Identifiable Information (PII) and establish requirements for its protection. These sources are foundational to Indiana's approach to safeguarding PII across public and private sectors and reflect both longstanding and evolving best practices in cybersecurity and privacy.

Source	Definition	Applicability
CMS MARS-E / NIST SP 800-122	PII is any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, SSN, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.	Federal, Healthcare
DHS Handbook (2017)	Sensitive PII includes standalone data like SSN, driver's license, passport number, alien registration number, or financial account number. Also includes data like citizenship, medical info, ethnic, religious, sexual orientation, lifestyle info, and account passwords when linked to an individual.	Federal
HIPAA / NIST SP 800-66 Rev 2	Individually Identifiable Health Information (IIHI) includes demographic and health-related data that identifies or can be used to identify an individual. PHI is a subset of IIHI transmitted or maintained in any form, excluding education and employment records and data on individuals deceased for over 50 years.	Healthcare
IC 4-1-6 (Indiana Fair Information Practices Act)	Personal information includes any data describing or indexing an individual, such as education, financial transactions, medical history, criminal or employment records, biometrics, photographs, or organizational memberships.	State (Indiana)

IC 4-1-11-3 (Notice of Security Breach)	Personal information includes a person's name (first and last or initial and last) combined with one or more of the following: SSN, driver's license or ID number, financial account or card numbers, security/access codes or passwords.	State (Indiana)
IC 35-43-5-1(i) (Forgery, Fraud, Deceptions)	Identifying information includes name, address, DOB, employer info, SSN, biometric data, electronic IDs, telecom identifiers, and access devices used for financial or service transactions.	State (Indiana)
IRS Publication 1075	Federal Tax Information (FTI) includes PII such as taxpayer name, address, ID number, email, phone, SSN, bank account, DOB, biometric data, or any combination thereof.	Federal, Tax
NIST SP 800-122, SP 800 – Rev. 5 and SP 800-171 Rev. 3 (draft)	PII includes identifiers like name, SSN, passport, driver's license, financial account numbers, address, biometric data, and any linked information such as DOB, religion, employment, education, or medical data.	Federal
OMB Memorandum 06-19	PII includes education, financial, medical, criminal, or employment history and any data that can distinguish or trace an individual's identity, such as name, SSN, DOB, biometric records, etc.	Federal
OMB Memorandum 07-16, M-23-18 (federal cybersecurity strategy)	PII includes identifiers like name, SSN, biometric records, and any other data that can distinguish or trace an individual's identity, alone or when combined with other linked information.	Federal

Observations and Analysis

The definitions of Personally Identifiable Information (PII) provided above are not exhaustive but serve the purpose of this guidebook by illustrating key concepts. A consistent theme across these definitions is that PII refers to any data that can be used—alone or in combination—to identify, trace, or distinguish an individual.

This guidebook categorizes PII into three practical types:

- Singularly PII: Information that is inherently sensitive and uniquely identifies an individual (e.g., Social Security Number, Passport Number).
- Collectively PII: Information that becomes sensitive when combined with identifiers (e.g., full name plus date of birth or address).
- Organization-Specific PII: Internal identifiers or credentials that may not be regulated but can still pose privacy risks if exposed (e.g., login credentials, challenge question answers).

These categories help organizations assess risk and apply appropriate safeguards based on context and sensitivity.

🧩 **Summary of PII Categories That Require Protection**

Singularly PII	Collectively PII	Organization-Specific PII
• Social Security Number • Passport Number • Driver's License Number • State ID Number • Alien Registration Number • Full Credit Card Number • Full Financial Account Number	• Full name or initial + last name plus: – Date of birth – Place of birth – Address – Email – Phone number – Employer – Citizenship status – Ethnicity – Religion – Sexual orientation – Lifestyle preferences – Employment or wage history – Financial transactions – Medical, biometric, education, tax, criminal, or welfare records	• Login credentials to internal systems • Account numbers tied to sensitive records • Challenge questions and answers • Employee performance data

⚠️ Considerations

Determining what qualifies as sensitive PII can be complex, especially in government or regulated environments. This complexity stems from evolving definitions and varying legal standards.

Note: PII definitions and required protections differ across jurisdictions—state, federal, and international. Organizations must carefully evaluate which laws and regulations apply to their data holdings and operations.

Characterizing the Current State of PII

The definition and protection of Personally Identifiable Information (PII) continue to evolve in response to technological advances, regulatory shifts, and growing public awareness. Staying current with these changes is essential for organizations that handle sensitive data.

One of the most significant challenges today is the mosaic effect—the risk that seemingly anonymized data can be re-identified when combined with other publicly available or privately held datasets. This concept, rooted in intelligence gathering, underscores how disparate data points can collectively reveal an individual's identity. The release of open government data and the proliferation of private data sources have amplified this risk, prompting renewed focus on data minimization, contextual sensitivity, and robust anonymization techniques.

🌐 Regulatory Landscape

Governments and regulators have responded with increasingly stringent privacy laws:

- European Union (EU): The General Data Protection Regulation (GDPR), effective since 2018, remains one of the most comprehensive privacy frameworks. It defines personal data broadly and places the responsibility for data protection squarely on organizations.

- United States

    - California: The California Consumer Privacy Act (CCPA) and its successor, The California Privacy Rights Act (CRPA), introduced new rights for consumers and established a dedicated enforcement agency.
    - Indiana: The Indiana Consumer Data Protection Act (ICDPA), signed into law in 2023, EFFECTIVE on January 1, 2026, adding Indiana to the growing list of states with comprehensive privacy legislation.
    - Federal Efforts: While federal legislation remains in flux, proposals such as the Consumer Online Privacy Rights Act (COPRA) and the Safe Data Act reflect bipartisan interest in establishing national standards.

As of 2025, over 30 states and territories have enacted or are actively developing privacy laws, creating a complex and dynamic compliance environment.

Identifying Related Regulations

This guidebook highlights key privacy regulations relevant to organizations operating in Indiana and beyond. While not exhaustive, it provides a foundational overview of laws and frameworks that govern the handling of Personally Identifiable Information (PII). For a comprehensive and regularly updated reference, consult the https://iapp.org.

🏛️ Indiana State Regulations (via https://iga.in.gov)

- Indiana Consumer Data Protection Act (IC 24-15) – Effective January 1, 2026
- Persons Holding a Customer's Personal Information (IC 24-4-14)
- Disclosure of Security Breach Act (IC 24-4.9)
- Identity Deception (IC 35-43-5-3.5)
- Fair Information Practices Act (IC 4-1-6)
- Notice of Security Breach (IC 4-1-11)
- Access to Public Records Act (IC 5-14-3)
- Privacy and Disclosure of BMV Records (IC 9-14-13)
- State of Indiana Information Privacy Policy

Federal Regulations

- https://www.govinfo.gov/app/collection/uscode
- and https://www.govinfo.gov/app/collection/cfr
- Privacy Act of 1974 (5 U.S.C. § 552a)
- Freedom of Information Act (FOIA) (5 U.S.C. § 552)
- E-Government Act of 2002
- Drivers Privacy Protection Act (18 U.S.C. § 2721)
- Right to Financial Privacy Act (12 U.S.C. § 3401 et seq.)
- OMB Circular A-130 & Memorandum M-07-16
- IRS Publication 1075 (2021)
- NIST SP 800-53 Rev. 5 (2020) – Security & Privacy Controls

- NIST SP 800-122 (2010) – Guide to Protecting PII

🎓 Educational Privacy Laws

- Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g)
- Protection of Pupil Rights Amendment (PPRA) (20 U.S.C. § 1232h)

💰 Financial Privacy Laws

- Gramm-Leach-Bliley Act (GLBA)
- Fair Credit Reporting Act (FCRA)
- Fair and Accurate Credit Transactions Act (FACTA)
- Dodd-Frank Wall Street Reform Act
- Right to Financial Privacy Act

🏛️ Protection of Nonpublic Personal Information (15 U.S.C. § 6801)

🏥 Medical & Health Privacy Laws

- Health Insurance Portability and Accountability Act (HIPAA)
- Health Information Technology for Economic and Clinical Health Act (HITECH)
- 21st Century Cures Act
- Genetic Information Nondiscrimination Act (GINA)
- Confidentiality of Substance Use Disorder Patient Records (42 CFR Part 2)

📡 Telecommunications & Marketing Privacy

- Cable Communications Policy Act
- Children's Online Privacy Protection Act (COPPA)
- Children's Online Privacy Protection Rule (16 CFR Part 312)
- Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM Act)
- Telemarketing Sales Rule (16 CFR Part 310)
- Video Privacy Protection Act (18 U.S.C. § 2710)

Future Developments Considered

🧬 Data De-identification & Re-identification Risks

De-identified data is increasingly vulnerable to re-identification through advanced analytics, including combinatoric techniques and the mosaic effect—where disparate data points are combined to reconstruct identities. Additionally, data perturbation methods used in de-identification can compromise data integrity. A clear understanding of PII—whether singular, collective, or organization-specific—is essential to mitigate these risks effectively.

🧬 Genomics & Precision Medicine

Genomic data presents unique privacy challenges. Publicly accessible genetic databases (e.g., GEDmatch, 23andMe) have been used in criminal investigations, raising ethical concerns. While the Genetic Information Nondiscrimination Act (GINA) of 2008 offers protections in health and employment contexts, rapid advances in genomics and AI-driven diagnostics are outpacing current privacy safeguards.

🌐 Cross-Context Identification & the Mosaic Effect

The aggregation of data across platforms—by private data brokers, public databases, and behavioral advertising networks—enables cross-context identification. This practice builds detailed individual profiles using data from multiple sources, often without user awareness or consent. For example:

- A breach exposed data on over 120 million households, including addresses, financials, and property ownership.
- The 2020 Blackbaud ransomware attack compromised donor profiling data from its Research Point platform.

The California Privacy Rights Act (CPRA) now defines and restricts cross-context behavioral advertising, introducing do-not-sell rights and exemptions for certain analytics functions.

🤝 Vendor Management & Third-Party Risk

As data becomes a strategic asset, organizations must ensure its authenticity, integrity, and privacy—especially when shared with third-party vendors. Contracts should include robust data protection clauses, and vendors must meet cybersecurity standards. Programs like:

- FedRAMP (Federal Risk and Authorization Management Program)
- StateRAMP (State-level equivalent for local governments)

help validate vendor security postures. Where these frameworks aren't adopted, organizations must independently assess vendor compliance and risk.

💳 Payment Card Industry Standards

The Payment Card Industry Data Security Standard (PCI DSS) has expanded in version 4.0 to include broader protections for consumer PII, beyond just credit card data. These updates aim to reduce identity theft and misuse associated with payment systems.

⛓️ Blockchain & Distributed Ledger Technologies

Blockchain offers strong data integrity, but poses challenges for privacy compliance:

- Immutable records conflict with privacy laws requiring data deletion.
- Transmitting PII via blockchain requires zero-knowledge proofs or pointers, which remove the distributed validation benefits and increase resource demands.

Organizations must carefully evaluate blockchain's suitability for privacy-sensitive applications.

🧭 Section Summary

This section outlines the evolving intersection of privacy law and emerging technologies. As innovation accelerates, organizations must proactively adapt their privacy frameworks to address new risks and regulatory expectations.

Best Practices for Data Privacy & Protection

To effectively mitigate privacy risks and safeguard Personally Identifiable Information (PII), organizations should adopt the following best practices:

1. Establish and Maintain Policies
   Develop clear internal and external privacy and cybersecurity policies. Ensure they are regularly reviewed, updated, and communicated across the organization.
2. Transparency and Notice
   Publish privacy notices that accurately describe data collection, usage, and protection practices. Ensure customers and clients know how to raise concerns and who to contact.

3. Awareness and Education
   Provide mandatory training and orientation for all employees with access to PII. Include role-specific guidance and refreshers at regular intervals.

4. Conduct Audits and Assessments
   Perform routine security audits and Privacy Impact Assessments (PIAs)—internally or via third-party experts—to identify vulnerabilities and improve controls.

5. Legal and Regulatory Compliance
   Stay informed of applicable laws and regulations, including sector-specific rules (e.g., HIPAA, GLBA, FERPA) and international frameworks like GDPR and CPRA.

6. Vendor and Third-Party Oversight
   Ensure contracts with third-party service providers include robust data protection clauses. Validate their cybersecurity posture using frameworks like FedRAMP or State RAMP.

7. Incident Response Planning
   Implement and test incident response procedures. Prompt action and notification are critical in minimizing harm and meeting legal obligations.

8. Engage with Law Enforcement and Cybersecurity Networks
   Collaborate with state and federal agencies when appropriate. Leverage resources from organizations like the Center for Internet Security (CIS) and All Hazards Consortium.

9. Annual Policy Review
   Review all privacy and cybersecurity policies at least annually to reflect changes in technology, law, and organizational needs. Sample templates are included in the appendices.

📜 Conclusion

This guidebook was developed to support Indiana-based organizations—large and small—in identifying and protecting sensitive information within their environments. The collection and use of PII introduces operational risks, including data breaches and regulatory violations, which can result in financial, legal, and reputational harm.

These risks can be mitigated by:

- Collecting only the minimum necessary PII for business purposes
- Knowing what PII is stored and where
- Removing PII when it is no longer needed

Understanding what constitutes PII and applying appropriate safeguards is essential. The appendices provide sample policies to help mitigate cyber threats and enhance privacy protections. However, organizations should seek legal counsel and professional advice tailored to their specific circumstances.

“People have entrusted us with their most personal information. We owe them nothing less than the best protections that we can possibly provide.”
— Tim Cook, CEO of Apple

To the prospective user of this policy Template:

This sample policy is intended for internal use to create a culture of data stewardship.

For additional information about cybersecurity and data privacy, visit Indiana's Cybersecurity Hub at: https://www.in.gov/cybersecurity/ for the latest resources, tips and best practices.

This policy template is not legal advice and is not a substitute for consulting with a licensed attorney for any particular legal challenges or issues facing your organization.

Version No.: ___ [DRAFT]
Last Updated: [insert date]

1. Purpose of this Policy

At [Company Name], we are committed to operating the business in a manner that fosters confidence and trust. To accomplish this goal, Personally Identifiable Information entrusted to us by our customers, employees, and vendors must be properly managed. This Policy sets forth how we will govern and protect that PII.

It is critical that all employees understand that mishandling PII can result in substantial harm to our customers, employees and the business. This harm may include financial harm to our company, employees or business partners. The harm may include identity theft and fraudulent use of information, reputational harm, regulatory fines and financial loss. In addition, mishandling PII can result in serious legal consequences for our organization. Accordingly, compliance with this Policy is mandatory.

2. Scope

This Policy applies to all [Company Name] employees, agents, and representatives, including third–party contractors or third-party providers of services to our company ("Third-Party Provider") who have access to {Company's] PII.

This Policy applies to all PII collected, maintained, transmitted, stored, retained, or otherwise used by [Company Name] regardless of where that information is stored and whether it relates to employees, customers, or any other individual.

3. Definitions

"Data Subject" means the person about whom PII is collected.

"PII" means information [Company Name] has collected or otherwise has in its possession that identifies or can be used to identify or authenticate an individual, including, but not limited to:

- Name
- Address
- Telephone number
- Email address
- Employee identification number
- Certain types of particularly sensitive personal information –
  - Social security numbers
  - Driver's license numbers
  - State-issued identification numbers
  - Health insurance identification numbers, such as a Medicare ID
  - Financial account numbers
  - Credit card numbers, or debit card numbers
  - Access codes, personal identification numbers or passwords that would permit access to an individual's financial account
  - Medical or health information

If you have any questions about whether any information qualifies as PII, you should contact [CONTACT NAME].

"Security Incident" means any act, omission, event or circumstance that compromises or potentially compromises the availability, confidentiality, integrity or security of PII.

4. Using and Retaining PII

Notice and Collection. It is our company's policy that whenever we collect PII for any purpose, including for human resources or employment purposes, we will inform the Data Subject of how we will use, disclose, retain and/or discard that PII by presenting (or at least making available) a privacy policy or privacy notice to the individual at the time they provide the information.

We will only collect PII in compliance with applicable company policies, notices, and/or Data Subject consent. PII collected must be limited to that which is reasonably necessary to accomplish [Company Name]'s legitimate business purposes or as necessary to comply with law.

Access, Use and Sharing. Employees may only access PII when that information relates to and is necessary to perform their job duties. You may not use PII in a way that is incompatible with this Policy or the notice given to the Data Subject at the time the information was collected. If you are unsure about whether a specific use or disclosure is appropriate, you should consult with [Contact Name]. You may only share such information with another Company employee, agent, or representative if the recipient has a job-related need to know the information.

PII may only be shared with a Third-Party Service Provider if it has a need to know the information for the purpose of providing the contracted services and if sharing the PII complies

with any privacy notice provided to the Data Subject. You may not share PII with a Third-Party Service Provider without prior written supervisor approval and/or a fully executed written contract that provides the appropriate safeguards for the information at issue.

Accuracy. It is important that PII that the company collects, maintains, and uses is accurate, complete, and relevant to the purposes for which it was collected. Employees should report inaccurate PII to their supervisor.

Security. All employees are responsible for doing their part to help protect PII. [Company Name]'s Information Technology and/or Information Security personnel have implemented certain technical, administrative, and physical safeguards for the protection of PII. Employees must follow those security procedures at all times to protect PII from loss, unauthorized access, and unauthorized disclosure.

Retention and Disposal. PII should be kept only for the amount of time it is needed to fulfill the legitimate business purpose for which it was collected or to satisfy a legal requirement. Employees must follow the applicable records retention schedules and policies related to retention and destruction of devices and/or media containing PII.

5. Training Employees and Supervising Contractors

All [Company Name] personnel who have access to PII will be trained on this Policy and are expected to abide by it. The company also expects that employees will help ensure that PII entrusted to a Third-Party Service Provider is protected by appropriate contract provisions. Personnel with responsibility for supervising employees or managing Third-Party Service Provider relationships will be trained on how to carry out these duties.

6. Reporting a Security Incident

If you know or suspect that a Security Incident has occurred, do not attempt to investigate the matter yourself. Immediately contact [CONTACT NAME] [and/or follow the company [SECURITY INCIDENT RESPONSE PLAN/PROCEDURE].

7. Monitoring Compliance and Enforcement

[CONTACT NAME] is responsible for overseeing management and enforcement of this Policy. If you are concerned that any provision of this Policy, or any related policy, operating procedure, process, or guideline designed to protect PII, has been or is being violated, please contact [CONTACT NAME]. The company may conduct reviews or audits to assess compliance with this Policy. Employees who violate this Policy and any related guidelines, operating procedures, or processes designed to protect PII may be subject to discipline, up to and including termination.

Other [Company Name] policies also apply to the collection, use, storage, protection, and handling of PII and may be relevant to implementing this Policy. You should familiarize yourself with these policies, including: [LIST OF OTHER APPLICABLE POLICIES]

[Insert line for name, signature, and date, if organization desires that this form be signed to acknowledge receipt.]

APPENDIX 2

[COMPANY NAME] INFORMATION TECHNOLOGY POLICY

To the prospective user of this policy Template:

This is an internal policy. This policy will be but one piece of your overall strategy to protect sensitive data.

For additional information about cybersecurity and data privacy, visit Indiana's Cybersecurity Hub at: https://www.in.gov/cybersecurity/.

This policy template is not legal advice and is not a substitute for consulting with a licensed attorney for any particular legal challenges or issues facing your organization.

1.0 Overview, Purposes of this Policy, and General Provisions

[Company Name] ("Company")'s computers, computer networks, other information technology ("IT") resources, and communications systems and equipment are provided to employees to help them perform their job duties and assist the organization achieve its business objectives. However, these resources carry risks, such as loss or misuse of Confidential Information or sensitive information, and/or data breach of company data, that can result in legal consequences for [Company]. Therefore, this Policy restricts the use of all IT resources, communications systems and equipment as described below.

The [Company's] IT equipment and resources are provided for business use only, subject to the limited exceptions addressed below. Each employee is responsible for complying with this Policy and using these resources and systems in a productive, ethical, and lawful manner.

[Company's] policies prohibiting harassment apply to the use of the company's IT and communications systems. Employees may not use [Company's] IT or communications system in a manner that is harassing or offensive, especially based on race, national origin, sex, sexual orientation, age, disability, religious beliefs or any other characteristic protected by federal, state, or local law.

The use of [Company's] IT and communications systems by an employee shall signify his or her understanding of, and agreement to comply with, this Policy.

Intellectual Property

- Defining "Confidential Information"
- Defining "Intellectual Property"

1.1 Administration of this Policy

[Contact Name] has primary responsibility for administration of this Policy. If you have questions regarding this Policy, please contact [Contact Name].

APPENDIX 2

[COMPANY NAME] INFORMATION TECHNOLOGY POLICY

1.2 Resources and Systems Covered by This Policy

This Policy governs all IT resources (both hardware and software) and communications systems (both hardware and software) that are owned by or made available by a Company. All of these IT and communication resources, systems, and equipment (collectively "IT SYSTEMS") include but are not limited to:

- Email systems and accounts
- Internet and intranet access
- Telephones and voicemail systems, including wired and mobile phones, smartphones, and pagers
- Printers, photocopiers, and scanners
- Fax machines, e-fax systems, and modems
- Computers, computer networks, and communications systems, hardware, peripherals, and software, including network key fobs and other devices
- Portable storage devices
- Cloud-based accounts and software
- Closed-circuit television (CCTV) and all physical security systems and devices, including access key cards or fobs
- Electronic systems on or within company vehicles.

This Policy also applies to and governs any employee's personal computers, electronic devices, equipment, software, apps, and/or accounts if and to the extent that an employee uses them to conduct Company's business or to access [Company's] IT SYSTEMS consistent with [Company's] IT policies and procedures.

NOTE: As it regards adopting policies involving a company's IT systems, particularly as it involves an employee being discouraged or prohibited from using their personal equipment for official work, it is appropriate for a company to consider how it should address the storage of data and the use of personal devices as part of its IT policies and procedures. In doing so, it could provide an opportunity for employees to better understand the company's expectations.

1.3 No Expectation of Privacy

All IT SYSTEMS and the contents of the IT SYSTEMS, including but not limited to items listed in this Policy, are the property of [Company]. Employees should have no expectation of privacy

whatsoever in any message, file, data, document, facsimile, telephone conversation, social media post, conversation, or any other kind or form of information or communication transmitted to, received, or printed from, or stored or recorded on the company's IT SYSTEMS.

[Company's] IT SYSTEMS are solely for [Company] purposes.

1.4 Network Systems – Access Is Limited by Authorization

[Company] maintains integrated IT SYSTEMS to facilitate all aspects of its operations. No one may sign on to any [Company] network equipment using the password or username of another employee. No employees should access, attempt to access, alter or delete any file, information, document or data except in furtherance of authorized job duties.

1.5 Confidentiality and Proprietary Rights

[Company's] Confidential Information and intellectual property (including trade secrets) are extremely valuable. Use or disclosure of such Confidential Information to anyone outside our company is prohibited. Do not use Company's name, brand names, logos, taglines, slogans, or other trademarks without written permission.

1.6 Inappropriate Use of IT Resources and Communications Systems

[Company's] IT SYSTEMS may never be used for any inappropriate or unlawful purpose. This includes but is not limited to:

- Misrepresenting oneself as another individual or company
- Sending, posting, recording, or encouraging receipt of messages or information that a reasonable person would find offensive or demeaning toward an individual or group because of a protected characteristic, including but not limited to sexual, racist, or religious content
- Revealing Company's proprietary or Confidential Information, including business information that an employee does not have a right to disclose as described in this Policy, or intellectual property without authorization
- Conducting or soliciting illegal activities
- Representing your personal opinion as that of Company
- Interfering with the performance of your job or the jobs of other Company employees
- For any other purpose that violates Company policies or practices

2.0 Discipline, Civil and Criminal Liability For Violations of this Policy

Employees who violate this Policy are subject to discipline, up to and including termination of employment.

3.0 Rules and Guidance for Specific Issues, Uses, Applications or Hardware

APPENDIX 2

[COMPANY NAME] INFORMATION TECHNOLOGY POLICY

Below, the Company addresses many common concerns, risks and issues that arise in the modern workplace. If a question arises that is not addressed in this Policy, employees should seek guidance from [Contact Name].

3.1 Connecting to the IT SYSTEMS Remotely

If an employee is granted access to connect to the IT SYSTEMS from home or otherwise via a personal device, it is the employee's responsibility to maintain reasonable cybersecurity on their personal computer or other device(s) they are using to connect. At a minimum, that includes up to date antivirus/antimalware software, and maintaining all software updates as issued.

3.2 Email, Text Messaging, and Other Messaging Applications or Apps

Company provides certain employees with access to email, text messaging systems and/or other messaging applications for use in connection with performing their job duties efficiently and effectively. This Policy strives to ensure that these communication tools do not compromise security and remain in compliance with the Company's other policies.

3.2.1 Etiquette.

Proper business etiquette must be maintained when communicating via electronic means. Sarcasm, inappropriate comments and attempts at humor should be avoided. Electronic communications allow no facial expressions and voice tones to assist in determining the meaning or intent behind comments. To avoid offending a coworker or customer, be professional and respectful in correspondence.

3.2.2 Links and Attachments

Malicious links and attachments are common sources of viruses and other malicious software. Employees may not click on links or attachments that the employee was not expecting. If in doubt, employees should call the sender (not via a phone number obtained from the communication at issue) to verify if the link or attachment is legitimate. This applies to text messages and any other application to which the employee has received a link or attachment.

3.2.3 Safety

Employees may not read or send emails, text or other electronic messages related to Company while operating any motor vehicle, or read or send email, text or other electronic messages of any kind (personal or professional) while operating a Company-owned vehicle.

3.2.4 Spam.

Employees may receive unsolicited commercial or bulk messages (spam) which is a nuisance, a drain on resources, and may spread malware. Do not open unsolicited messages and report suspicious messages to [Contact Name]. Do not reply to spam messages in any way. Do not attempt to "unsubscribe" from its distribution list. For assistance blocking spam messages, contact [Contact Name].

3.2.5 Email Use and Storage Restrictions For Sensitive Information

It is common for email accounts, including corporate accounts, to be breached by outside hackers. In addition, a "regular" email sent over the internet to reach its destination generally lacks the security protections needed for sensitive information. Accordingly, to help prevent data breaches and protect both Company data and the identities of its employees, customers and others, the following rules apply.

Employees may not send a regular email that includes (in the email itself or in any attachment) more than:

- Last 4 digits of any Social Security Number
- Last 4 digits of any Driver's License Number
- Last 4 digits of any State Identification number
- Last 4 digits of any credit or debit card number
- Last 4 digits of any financial account number

Employees may not store emails in their inbox, inbox subfolders, sent or deleted mail that contain any of the types of data listed above in its full form (i.e., more digits than listed above).

If an employee needs to send any of the types of sensitive information noted above in its full form, the employee should see [Contact Name] for assistance with more secure methods.

3.2.6 Personal Use of Company-Provided Email. Company recognizes that employees may occasionally desire to use their company-provided email account for personal use while at the office or by means of the Company's IT SYSTEMS. Use of your Company email account to conduct purely personal business is discouraged, and should be done sparingly, if ever. If an employee needs to do so in unusual circumstances, it is permitted so long as it is during non-work time (for example, breaks or meal periods), does not involve unprofessional or inappropriate content and does not interfere with your employment responsibilities or productivity.

3.2.7 Use of Personal Email Accounts. Company recognizes that employees might occasionally need to access and/or use their personal email accounts for personal use while at the office via the IT SYSTEMS. Such occasional use is permitted so long as it is during non-work time (for example, breaks or meal periods), does not involve unprofessional or inappropriate content and does not interfere with your employment responsibilities or productivity. In addition, the following rules apply when accessing your personal email account:

- You may not conduct any Company business or your job duties via your personal account.
- Do not click on any unexpected links or attachments, or open files, within a personal email account, unless you have confirmed their trustworthiness.
- Never send any of the Company's information, documents or data of any kind to or from your personal email account.

3.3 Flash Drives/Portable Hard Drives

Portable electronic storage devices present a considerable risk because they can be easily lost or stolen. Accordingly, extra care is required to protect Company and therefore:

- Employees may not save any of Company's business related data to an unencrypted flash drive or portable hard drive.
- Employees may not save the types of information listed in Section 3.2.5 above to any such device.
- Employees may not use personal flash drives or personal hard drives with Company's IT SYSTEMS, as they present a risk of spreading malware.

3.4 Installation of Software or Applications / "Apps" and Disabling Software

Employees may not download or install any software, application ("app") or program to any Company-issued equipment (desktop computer, laptop, iPad, tablet, smart phone, or any other Company-issued device) unless such action is authorized in writing by [Contact Name]. Employees may not download games or any other non-work-related files to any Company-issued equipment.

Employees may not disable any software, even temporarily, without permission from [Contact Name].

3.5 Laptop Use

Laptops require additional care because they can be easily lost or stolen. All Company laptops should be set up with an encrypted hard drive. Employees may not download or install any software, applications, "apps" or programs to a Company-owned laptop without written approval by [Contact Name]. Employees are strongly discouraged from leaving laptops in motor vehicles, but if they must do so, they should be left in the locked trunk of the vehicle or, if there is no trunk, they should be kept out of sight in a locked vehicle (example, under a blanket in the back of an SUV).

Employees may not save any Company work-related information to a personal laptop.

3.6 Logging Out of the Network and Devices

Screen saver passwords, also known as "workstation timeouts" or "lock screens," secure Company's Confidential Information by protecting active computer sessions when you step away. Locking screen savers must activate after a maximum inactivity time of ___minutes. If you handle highly Confidential Information, you should lock your screen any time you leave it unattended. Employees must log out of the Company's computer network entirely at the end of each workday.

Employees should see [Contact Name] if they need assistance to comply with these requirements.

3.7 Passwords

Employees' passwords must comply with Company's requirements as to length, complexity, and periodic password change.

Employees may not share usernames, passcodes or passwords with any other person, except to the extent needed with administrative assistants and/or IT staff. Employees shall immediately inform [Contact Name] if they know or suspect that any username, pass code, or password has been improperly shared or used, or that IT security has been violated in any way.

3.8 Personal Cloud and Personal Applications

Employees may not use any personal cloud-based account of any application, "app" or service to upload, transmit, store, share or work on any of Company's business information. This includes any such account that is set up only in the employee's name, even if the employee used their Company email address with the account. If this type of service is needed, the employee must use a/the Company's approved business account.

Similarly, employees may not use personally downloaded applications ("apps"), on any device or computer, to conduct their job duties or to transmit, store, upload, share or work on any of Company's business information.

APPENDIX 2

[COMPANY NAME] INFORMATION TECHNOLOGY POLICY

3.9 Smart Phones/ Cell Phones

[Insert company-specific rules based upon whether your company allows or encourages Bring Your Own Device (BYOD), or provides company issued phones (and/or other mobile devices), or some combinations of both. Insert here specific rules for each category of use that your company permits, based upon the nature how devices will be used for work, the sensitivity of the data involved, and other pertinent factors.]

4.0 Internet Use

Company provides internet access to certain employees for use in connection with performing their job duties. The following outlines the expectations regarding internet use by employees.

Company recognizes that employees might work long hours and occasionally may desire or need to access the internet for personal activities at the office or by means of the company's IT SYSTEMS. Such occasional use is authorized so long as it is during non-work time (for example, breaks or meal periods), does not involve unprofessional or inappropriate content, does not interfere with your employment responsibilities or productivity, and does not compromise Company's Confidential Information of the proper operation of its IT SYSTEMS.

Using the internet to access pornographic, sexually explicit, or "hate" sites, or any other website that might violate law or Company policies against harassment and discrimination is never permitted.

5.0 Responding to Suspicious Computer Activity, Pop-Ups or Threats

Malicious actors are constantly creating new tricks and schemes to try to get computer users to click on links, open attachments, or do other acts that will infect their computer network with malicious code or result in the fraudulent transfer or payment of money. This may include pop-ups messages that appear to take over a user's computer, or emails that attempt to blackmail a user.

Employees should not ever engage, call or agree to pay the sender of any such trick or scheme. If an employee has any doubts about an email, pop-up ad or error message of any kind, the employee should not try to handle it themselves but should instead reach out to [Contact Name] for assistance.

[Insert line for name, signature, and date, for employee if organization desires that this form be signed to acknowledge receipt.]

APPENDIX 3

[COMPANY NAME] CYBER INCIDENT RESPONSE PROCEDURE

To the prospective user of this template procedure:

This procedure is for internal use in your organization. The potential effectiveness of this procedure will depend on the extent to which you invest the time to customize it to your business and train those involved in its use.

This procedure template, and the guidance herein, will work with and support your organization's larger data privacy and cybersecurity efforts. That is, this procedure will be one piece of your overall strategy to protect information.

For additional information about cybersecurity and data privacy, you should consult Indiana's Cybersecurity Hub found at: https://www.in.gov/cybersecurity/

This procedure template is not legal advice and is not a substitute for consulting with a licensed attorney for any particular legal challenges or issues facing your organization

---

Version No.: ___ [DRAFT]

Last Updated: [insert date]

I. Objectives and Scope

This [Company Name] Cyber Incident Response Procedure governs all employees and management on how to respond to a potential or actual cybersecurity threat or incident ("Security Incident").

This Procedure aims to prevent incidents from going unnoticed or unreported, which may result in the magnitude of harm associated with that or a future incident being significantly greater than if the activity was promptly noted and addressed.

This Procedure also aims to make responding to Security Incidents a standardized procedure, which will be beneficial for both the speed of response and will prevent costly mistakes.

All company employees, including management, must be familiar with, and abide by this Procedure.

II. Incident Response Team

The [Company Name] Incident Response Team ("IRT") is established, and certain roles and responsibilities assigned below to achieve an orderly and professional response to Security Incidents.

The IRT is composed of the following employees, who are all IRT members, whether they are listed as a Team Member or as a Designated Backup:

APPENDIX 3

[COMPANY NAME] CYBER INCIDENT RESPONSE PROCEDURE

Team Member	Designated Backup
[Team Member 1] / IT "Help Desk" - This is your internal or external computer "Help Desk" or other IT personnel you use for routine computer issues.	If the resource used as your computer "help desk" is only one person, you should designate someone else here as their backup.
[Team Member 2]	[Team Member 3]
[Team Member 4] This should be a high-ranking member of management or an owner.	[Team Member 5] This should be a high-ranking member of management or an owner.

Designated Backups are critical team members so that this Procedure will still work even when another IRT member is on vacation or otherwise not available.

All IRT members shall keep a hard copy of this Procedure with them at the office and their home for ready access during times when the computer network and/or network communication systems are down. Contact information for IRT members is listed at the end of this Procedure.

III. Definitions

It is important that all employees understand that not all potential or actual cybersecurity incidents or events are a "data breach." In general, neither employees nor management should refer to any incident as a "data breach" (unless approved by legal counsel), because use of that term carries with it legal conclusions and related legal obligations.

"Security Incident" is a very broad term for purposes of this Procedure and means any event, incident, act, omission that a company employee or member of management becomes aware of which could possibly be a threat to the company computer system, any device connected to the system, or any company information. Examples of potential "Security Incidents" include, but are not limited to:

- Unusual Error Message on Your Computer or other Electronic Device or Phone
- Suspicious Email or Email Attachment
- Unusual Computer Behavior or Performance
- Blackmail Threat Received via Email or other Electronic Means
- Unusual Pop-Up Messages, Including Ones that Claim Your Computer is "Infected"

"Data Breach" is a legal conclusion that, depending on the applicable law, certain type(s) of information have been accessed, acquired or compromised such that a legal obligation has

been triggered to notify one or more parties of the event and/or to notify a governmental authority.

IV. Reporting Security Incidents

Any employee who discovers or encounters even a potential Security Incident should contact Help Desk immediately. It is important that employees report issues, even if they believe are minor, because it will provide information to the IRT about what is happening across the Company and ensure that the IRT verifies that what looks like a minor issue is actually so. The employee reporting the issue will pass along basic information, such as:

- Their name
- Contact information
- The nature of the concern
- The equipment or persons involved along with their location
- How the issue was detected
- When the issue was first noticed

V. IRT Response Procedures

A. Initial Assessment and Instructions

1) If the Help Desk determines that the issue is a routine matter, Help Desk will proceed with guiding the employee on what to do next. This might include advice on situations such as directing an employee what they should do with a suspicious email.

2) If the Help Desk determines that the issue may be beyond a routine matter, Help Desk will contact [Team Member 2] immediately.

Once [Team Member 2] (or his/her backup - [Team Member 3]) receive the call from Help Desk, they will assess the situation, including:

- What type of threat is it?
- Is it ongoing?
- Is the affected equipment business critical?
- What is the severity of the potential impact?
- Name of system being targeted, along with operating system, IP address, and location.
- What types of information may be targeted or at risk?

3) Help Desk and [Team Member 2] (or his/her backup - [Team Member 3]) will give instructions to the employee regarding any immediate action the employee should or should not take. For example, they may instruct the employee to take actions such as to unplug the device from the network or disconnect from Wi-Fi.

If Help Desk and [Team Member 2] (or his/her backup [Team Member 3]) determine this is an issue that can be handled in-house, they will proceed to do so. If instead, they determine that the issue may require outside help, they will proceed to step B below.

B. Escalation Step 1 – Initial Meeting

If Help Desk and [Team Member 2] recognize the Security Incident as being potentially serious or beyond (or likely beyond) internal capabilities, they will immediately contact Team Member 4 (or his/her backup [Team Member 5]).

Help Desk,[Team Member 2] (or backup) and Team Member 4 (or his/her backup – [Team Member 5] will meet in person or by telephone to determine next steps, including whether it may be appropriate to contact the company's cyber insurance carrier and any other insurance carrier that might need to be put on notice. Topics for this/her discussion will include:

- Nature of the event/incident
- Is the incident still in progress?
- What data or property is threatened and how critical is it?
- What is the potential impact on the data?
- What is the potential impact on employees and customers?
- What system or systems are targeted, where are they located physically and on the network?
- Is the response urgent?
- Can the incident be contained and remediated with internal resources?
- Is there a need for professional outside help to preserve evidence?
- Is there a potential need for law enforcement to be involved?

C. Escalation Step 2 – Getting Outside Help

If the Escalation Step 1 Initial Meeting results in a determination that the situation warrants calling for outside help, the IRT shall immediately call the company's outside legal counsel who has been designated in advance to respond to cyber incidents, or the company's cyber insurance carrier, whichever has been pre-arranged as the appropriate "first call" to make.

The IRT will then coordinate with and support outside legal counsel and/or the cyber insurance carrier's breach response team.

VI. Post Incident Procedures

APPENDIX 3

[COMPANY NAME] CYBER INCIDENT RESPONSE PROCEDURE

For each event that rises beyond the initial step of being quickly resolved by Help Desk, the following information shall be documented by the IRT to help improve cyber defenses and this Procedure going forward:

1. A description of the incident, with pertinent details.
2. How the incident was discovered.
3. The category of the incident -
    a. Minor – handled easily in-house
    b. Moderate – handled in-house
    c. Severe – outside help required
4. How the incident occurred, whether through email, firewall, etc.
5. Where the attack came from, if known, such as IP addresses and other related information about the attacker.
6. What was done in response?
7. Whether the response was effective, and if not, why not.
8. Cost of the incident.

The IRT, with the assistance of legal counsel, will help ensure evidence is preserved as appropriate, such as copies of logs, emails and other communication, and metadata for any possible or anticipated insurance claims, investigations, civil claims or prosecutions.

After an incident is resolved, the IRT will update this Procedure as needed. The IRT will review and update this Procedure at least annually.

VII. Contact Information

The following phone numbers are for contacting all IRT members (including backups) away from the office in the event of an incident:

Name	Mobile Phone	Home Phone
Team Member		
Team Member		

APPENDIX 3

[COMPANY NAME] CYBER INCIDENT RESPONSE PROCEDURE

Team Member		
Team Member		
Team Member		
Team Member		
Cyber Insurance Carrier		

The following law-enforcement resources contact information may also be needed:

- FBI Field Office Cyber Task Forces: http://www.fbi.gov/contact-us/field
- FBI's Internet Crime Complaint Center (IC3): http://www.ic3.gov
- Indianapolis Field Office of Federal Bureau of Investigation (FBI): (317) 595-4000
- Indiana State Police, Cybercrime & Investigative Technologies Section. More information can be found at: https://www.in.gov/isp/3234.htm
- U.S. Secret Service, Financial Crimes Task Force (FCTF): 317-635-6420
- U.S. Secret Service Field Offices and Electronic Crimes Task Forces (ECTFs): http://www.secretservice.gov/contact/field-offices