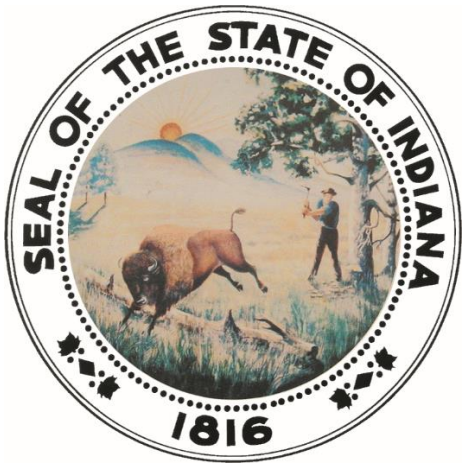
Personally Identifiable Information (PII) Guidebook 2.0



Privacy Working Group of the
Indiana Executive Council on Cybersecurity
April, 2024

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

A special thank you to members of the Indiana Executive Council on Cybersecurity's (IECC) PII Working Group, who stepped forward – from the public and private sector as leaders in privacy and cybersecurity to offer their knowledge and expertise as the foundation creating the first edition of this guide in 2021, and to the members of the IECC's Privacy Working Group, whose contributions (as subject matter experts) were instrumental in providing a meaningful update to this document in 2024.

Additionally, thank you to the leadership of the IECC and all of its members, past and present, whose dedication to cyber governance, on behalf of all Hoosiers, is greatly appreciated. Lastly, we acknowledge Governor Eric Holcomb for his leadership – expressed through the continuation of Executive Order 17-11 with the recognition that a cross-sector body of subject-matter experts is required to form an understanding of Indiana's cyber risk profile, identify priorities, establish a strategic framework of Indiana's cybersecurity initiatives, and leverage the body of talent to stay on the forefront of the cyber risk environment.

DEFINING PII

PII Guidance Sources

This section lists various regulations and standards that define PII that may require specific protections.

- Centers for Medicare and Medicaid Services (CMS) Minimum Acceptable Risk Standards for Exchanges (MARS-E)
- Department of Homeland Security (DHS) Handbook for Safeguarding Sensitive Personally Identifiable Information, March 2012
- Health Insurance Portability and Accountability Act (HIPAA)
- Indiana Code (IC) 4-1-6, Fair Information Practices; Privacy of Personal Information
- IC 4-1-11-3, Notice of Security Breach, Personal Information
- IC 35-43-5-1(i), Forgery, Fraud, and Other Deceptions; Identifying Information
- Internal Revenue Service (IRS) Publication 1075, November 2021
- National Institute for Standards and Technology (NIST) Special Publication (SP) 800-53
- Office of Management and Budget (OMB) Memorandum 06-19
- OMB Memorandum 07-16

PII Guidance Sources and Definitions

SOURCE	DEFINTION
CMS MARS-E	National Institute of Standards and Technology (NIST) Special Publication 800-122, April 2010, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, defines PII as "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, social security number, 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."
DHS	Some PII is sensitive as stand-alone data, for example, SSN, driver's license or state identification number, passport number, alien registration number, or financial account number. Other examples of sensitive PII data elements are citizenship or immigration status, medical information, ethnic, religious, sexual orientation, or lifestyle information, and account passwords, in conjunction with the identity of an individual (directly or indirectly inferred).
HIPAA	Pursuant to NIST Special Publication 800-66, Rev 2, *Individually Identifiable Health Information (IIHI)* [45 C.F.R. Sec. 160.103], PII requiring protection is a subset of health information, including demographic information collected from an individual, and: (1) Is created or received by a healthcare provider, health plan, employer, or healthcare clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of healthcare to an individual; or the past, present, or future payment for the provision of healthcare to an individual; and (i) That identifies the individual; or (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual. Protected Health Information (PHI) is a form of PII. It is IIHI that is: • Transmitted by electronic media. • Maintained in electronic media; or • Transmitted or maintained in any other form or medium.

	PHI excludes IIHI in: • In education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g. • In records described at 20 U.S.C. 1232g(a)(4)(B)(iv) • In employment records held by a covered entity in its role as employer • Regarding a person who has been deceased for more than 50 years
IC 4-1-6 Indiana Fair Information Practices Act	"Personal information" means any information that describes, locates, or indexes anything about an individual or that affords a basis for inferring personal characteristics about an individual including, but not limited to, the individual's education, financial transactions, medical history, criminal or employment records, finger and voice prints, photographs, or the individual's presence, registration, or membership in an organization or activity or admission to an institution.
IC 4-1-11-3 Notice of Security Breach (as applicable to State agencies)	"Personal information" means: (1) an individual's: (A) first name and last name; or (B) first initial and last name; and (2) at least one (1) of the following data elements: (A) Social Security number. (B) Driver's license number or identification card number. (C) Account number, credit card number, debit card number, security code, access code, or password of an individual's financial account.
IC 35-43-5-1(i) Identifying Information (as applicable to forgery, fraud, and other deceptions)	"Identifying information" means information that identifies a person, including a person's: (1) name, address, date of birth, place of employment, employer identification number, mother's maiden name, social security number, or any identification number issued by a governmental entity. (2) unique biometric data, including the person's fingerprint, voice print, or retina or iris image. (3) unique electronic identification number, address, or routing code. (4) telecommunication identifying information; or (5) telecommunication access device, including a card, a plate, a code, a telephone number, an account number, a personal identification number, an electronic serial number, a mobile identification number, or another telecommunications service or device or means of account access that may be used to: (A) obtain money, goods, services, or any other thing of value; or (B) initiate a transfer of funds.
IRS Publication 1075	Federal Tax Information (FTI) may include Personally Identifiable Information (PII). FTI may include the following PII elements: • Name of a person with respect to whom a return is filed • Taxpayer mailing address • Taxpayer identification number • E-mail addresses • Telephone numbers • Social Security Numbers • Bank account numbers • Date and place of birth • Mother's maiden name • Biometric data (e.g., height, weight, eye color, fingerprints) • Any combination of the above

NIST SP 800-122, April 2010	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, social security number, 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. Examples of PII include, but are not limited to: • Name, such as full name, maiden name, mother's maiden name, or alias • Personal identification number, such as social security number, passport number, driver's license number, taxpayer identification number, or financial account or credit card number • Address information, such as street address or email address • Personal characteristics, including photographic image (especially of face or other identifying characteristic), fingerprints, handwriting, or other biometric data (e.g., retina scan, voice signature, facial geometry) • Information about an individual that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, weight, activities, geographical indicators, employment information, medical information, education information, financial information)
OMB Memorandum 06-19	Any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual.
OMB Memorandum 07-16	Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

Observations and Analysis

The above list of PII definitions is not an exhaustive one, but it does provide relevant definitions for the purpose of this guidebook. A common element of these definitions of PII is that it can be used to distinguish or trace an individual's identity.

The next section of this guidebook discusses PII in two categories, Singularly PII – that is information that is itself a sensitive identifier, such as a Social Security Number or Passport Number – and Collectively PII – that is sensitive information that is not PII unless it contains identifiers.

Organization-specific PII, though not defined by a regulation, can be sensitive PII. For example, a unique identification number associated with an organization's customer record containing sensitive information could be considered PII if the name of the organization and system were known, such as answers to challenge questions when a user attempts to log into the organization's system without their password.

Summary of Categories of PII That Must Be Protected

Singularly PII	Collectively PII	Organization-specific PII
Any of the following single items: • Social security number • Alien registration/green card number • State identification number • Driver's license number • Passport number • Full credit card number • Full financial account number	**Contains individual's name to include full first and last name or first initial and full last name, and at least one of the following:** • Mother's maiden name • Date of birth • Place of birth • Address (street or PO Box) • Email address • Phone number • Employer or business name • Citizenship or immigration status • Ethnic affiliation • Religious affiliation • Sexual orientation • Lifestyle preferences • Employment history • Wage history • Financial transactions • Customer amount owed, received, paid, collected, withheld, intercepted, earned, fined, and garnished • The following types of information and records - Medical - Biometric - Education - Financial - Tax - Criminal/incarceration - Social welfare	**Includes:** • Login ID and password to organizational network, computing equipment, or applications hosting customer or employee data • Account numbers associated with sensitive customer or employee records • Customer or employee challenge questions and answers • Employee performance records

In some instances, it may be difficult to determine what information is considered sensitive PII and, therefore, what protections to apply, such as government agencies. Part of that challenge relates to the evolving definitions of PII, which is addressed in more detail later in this Guidebook.

NOTE: the definitions of PII and applicable protections vary from State to State, across agencies and across borders, therefore, organizations should carefully consider which jurisdictions apply to their data.

CHARACTERIZING THE CURRENT STATE OF PII

Given the fact that the definitions of PII and applicable protections are ever-changing, it is essential to stay abreast of technologies and the rules that apply to them.

In May 2013, President Obama issued an executive order, "Making Open and Machine Readable the New Default for Government Information," which created the US Government's Open Data Policy and encouraged the release of government data to the public. Newly available public data together with data amassed by private entities, increased the risks of re-identification of previously de-identified sensitive PII, termed the 'mosaic effect.'

A 2014 report by Mathematica Policy Research describes the mosaic effect as "…derived from the mosaic theory of intelligence gathering, in which disparate pieces of information become significant when combined with other types of information." This possibility of re-identification has prompted local, state, and federal governments to re-evaluate and strengthen data anonymization practices.

Regulators have responded with regulations designed to establish and protect individuals' right to information privacy. An example is the European Union's (EU) General Data Protection Regulation (GDPR) (General Data Protection Regulation (GDPR) Compliance Guidelines) one if the broadest and most protective regulatory frameworks. GDPR took effect in May 2018 and, in concert with the Data Protection Act of 2018, supersedes the Data Protection Act of 1998. It broadens the definition of PII and shifts the burden of implementing privacy measures from consumers to companies. The definition of PII under the GDPR is as follows:

> *'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;*

This broadens protections of PII for EU data subjects. California passed the California Consumer Privacy Act (CCPA) (California Consumer Privacy Act (CCPA) | State of California - Department of Justice - Office of the Attorney General) effective January 2020 and is one of the most expansive data privacy regulation in the U.S.. In November 2020, California passed the California Privacy Rights Act of 2020 (CPRA), which, among other things, creates a standalone agency to administer the state's privacy regulations, imposes new restrictions on cross-context behavioral advertising, and defines a new category of 'sensitive data' within the personal information realm.

More recently, in the 2023 session of the Indiana General Assembly, Senate Bill 5 was adopted and signed into law, establishing a new article in the Indiana Code concerning consumer data protection. It takes effect January 1, 2026.

To date, more than thirty U.S. States and Puerto Rico and Congress have passed or are working on some form of data privacy legislation. U.S. Senator Maria Cantwell introduced the "Consumer Online Privacy Rights Act" (COPRA) in the fall of 2019 which was followed in the summer of 2020 by U.S. Senator Roger Wicker's "Setting an American Framework to Ensure Data Access, Transparency, and Accountability" (SAFE DATA) Act. It should be noted that the federal negotiations are continuing (as of the time that this guide was published).

IDENTIFYING RELATED REGULATIONS

This Guidebook tries to highlight some of the relevant privacy regulations, but it is not a comprehensive list. The International Association of Privacy Professionals works to track local, national and international privacy laws: Global Comprehensive Privacy Law Mapping Chart (iapp.org).

- Indiana regulations(iga.IN.gov)
  - 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
- Federal
  - https://www.govinfo.gov/app/collection/uscode
  - https://www.govinfo.gov/app/collection/cfr)
- Educational
  - Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g
  - Protection of Pupil Rights Amendment, 20 U.S.C. § 1232h
- Financial
  - Dodd-Frank Wall Street Reform and Consumer Protection Act, P.L. 111-203
  - Fair and Accurate Credit Transactions Act, P.L. 108-159
  - Fair Credit Reporting Act, 15 U.S.C. § 1681
  - Gramm-Leach-Bliley Act, P.L. 106-102, 113 Stat. 1338
  - Protection of nonpublic personal information by financial institutions, 15 U.S.C. § 6801
  - Right to Financial Privacy Act, P.L. 95-630
- Medical
  - 21st Century Cures Act, P.L. 114-255
  - Confidentiality of Substance Use Disorder Patient Records Rule, 42 CFR Part 2
  - Genetic Information Nondiscrimination Act of 2008, P.L. 110-233
  - Health Insurance Portability and Accountability Act, P.L. No. 104-191, 110 Stat. 1938 (1996)
  - Health Information Technology for Economic and Clinical Health Act, P.L 111-5
- Telecommunications and Marketing
  - Cable Communications Policy Act, P.L. 98-549
  - Controlling the Assault of Non-Solicited Pornography and Marketing, 15 U.S.C. Ch. 103
  - Children's Online Privacy Protection Act, 15 U.S.C. § 6501-6506
  - Children's Online Privacy Protection Rule, 16 CFR Part 312
  - Telemarketing Sales Rule, 16 CFR Part 310
  - Video Privacy Protection Act, 18 U.S.C. § 2710

- Regulations and related guidance applicable to government
  - Indiana (iga.IN.gov)
    - 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 Bureau of Motor Vehicles Records, IC 9-14-13
    - State of Indiana Information Privacy Policy

- Federal
  - https://www.govinfo.gov/app/collection/uscode https://www.govinfo.gov/app/collection/cfr)
  - Drivers Privacy Protection Act, 18 U.S.C. 2721 et seq.
  - Privacy Act of 1974, 5 U.S.C. § 552a
  - E-Government Act of 2002,
  - Freedom of Information Act, 5 U.S.C. § 552
  - NIST SP 800-53, Revision 5, September 2020, *Security and Privacy Controls for Federal Information Systems and Organizations*
  - NIST SP 800-122, April 2010, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*
  - IRS Publication 1075, November 2021, *Tax Information Security Guidelines for Federal, State and Local Agencies*
  - OMB Circular No. A-130, *Managing Information as a Strategic Resource*
  - OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*
  - Right to Financial Privacy Act of 1978, 12 U.S.C. § 3401 et seq.

FUTURE DEVELOPMENTS CONSIDERED

Data De-identification

'De-identified' data may be "at risk reidentification" using combinatoric algebra and other "mosaic" data techniques. Further, data perturbation, where data is distorted by the de-identification process, can adversely impact data integrity. Therefore, a foundational understanding of what constitutes PII in the singular, collective, and organizationally specific contexts is key to mitigating associated privacy risks.

Genomics

Genomics and precision medicine raise privacy concerns tied to genomic data being even indirectly. GED match and 23andme genetic databases have been used to help identify cold case murderers, raising privacy questions. While 2008's Genetic Information Nondiscrimination Act created new protections in the health insurance and employment contexts, technological advances are outpacing data protection.

Cross-context Identification & The Mosaic Effect

Private-sector data brokers, public-sector databases, and amassing digital data create privacy risks from cross-context identification and the mosaic effect. Cross-context identification can manifest through Ad Tech's internet and app-enabled behavioral advertising apparatus, tracking and collecting data about individual users across devices and websites. Detailed individual profiles are indiscriminately created, used and traded without individual knowledge or consent. A recent data breach resulted in the publication of data on more than 120 million households, incorporating street addresses, demographics, and finances for families, as well as information on home and automobile ownership.

Cross-identification uses multiple data sets to produce detailed profiles of individual data subjects. Profiles are built using public property information, data about political and charitable donations, and organizational membership activities. The 2020 ransomware attack on Blackbaud, for example, contained such PII in its ResearchPoint application, a database used to identify high-value donors by calculating their net worth and potential ability to donate.

California recently passed the CPRA that defines cross-context behavioral advertising and imposes limitations such as do-not-sell obligations, while exempting certain analytics functions from restrictions.

Vendor Management & Data Protection

Big-data analytics technologies are the norm, and data is a strategic organizational asset and must be maintained and protected to ensure authenticity, integrity and privacy. Third party service providers often use and exchange data, potentially including PII. Businesses are responsible for ensuring appropriate data protection for their on-prem data as well as data used or stored in cloud solutions, and when used or shared with third parties. So, their contracts should contain appropriate and effective data protection provisions.

Businesses are responsible to ensure that their third party services partners IT and data-processing systems meet appropriate cybersecurity standards and requirements. The Federal Government achieves this through the Federal Risk and Authorization Management Program, or FedRAMP, and state and local governments are able to sign on to a similar program through the non-profit State Risk and Authorization Management Program, or StateRAMP. Alternatively, those contracting must ensure not only adequate data ownership, use, and protection terms, but must expend additional resources to validate the cybersecurity posture of a potential vendor.

Payment Card Industry

The payment card industry established Payment Card Industry-Data Security Standards, known as PCI DSS, to protect cardholder PII. Upcoming PCI DSS 4.0 standards expand protections to include- protection

of consumer PII in addition to credit card data to mitigate risks of potential misuse and identity theft associated with credit card-related data.

Blockchain and Distributed Ledger Technologies
Digital Distributed Ledger Technologies and Distributed Verification and Validation Techniques, more commonly referred to as Blockchain, were designed to protect data integrity, rather than privacy or security. For example, blockchain does not allow a user to delete a record, making compliance with various privacy laws difficult or impossible.

To transmit PII, one would need to utilize zero-knowledge proofs or pointers, which remove the distributed verification and validation component of Blockchain and requires both sending and receiving parties to do their own integrity checks. This consumes significantly more resources and energy by removing all PII and replacing it with pointers or zero-knowledge proofs on Blockchain.

Section Conclusion
This section shares a general perspective of this evolving intersection of the law and emerging technologies.

BEST PRACTICES

This is a brief list of some best practices to help organizations mitigate data privacy risks.

1. Create cybersecurity, internal, and external privacy policies and procedures; regularly train everyone about them.
2. Publish notices that accurately describe the organization's data privacy and security processes.
3. Customers, clients, and website visitors should be made aware of cybersecurity concerns and the efforts being made to address them. Organizations must be transparent about the collection of PII, its use, and procedures to protect privacy and security. Customers/clients must know exactly who to contact (and how) in case of a concern.
4. Conduct regular security audits and privacy impact assessments (which may be conducted by third-party contractors), to determine vulnerabilities and address them.
5. Implement a mandatory education and orientation process for all employees who have access to PII. (This may be created by third-party contractors.)
6. Know and follow applicable laws and regulations specific to your industry. In the U.S., sector-specific laws regulate PII data use and/or dissemination in various realms (health, financial, education, etc.).
7. In addition to state and federal law, international businesses may be subject to additional sets of rules. For example, the GDPR regulates the collection, use, and transfer of data pertaining to European Union citizens.
8. Take advantage of not-for-profit organizations that promote cybersecurity measures, such as the Center for Internet Security or the All Hazards Consortium.
9. Implement cybersecurity incident response policies and procedures. Best practices require prompt action and sometimes notification.
10. Collaborate with state and federal law enforcement.
11. Review all cybersecurity and privacy-related policies and procedures at least annually. Like all things pertaining to technology and the law, changes occur constantly. Sample templates for certain key polices are included with this guidebook as appendices.

CONCLUSION

This guidebook has been developed for Indiana organizations, small and large, to learn more about how to identify information in their environment that requires a heightened degree of protection. Across various sectors and individual roles, the collection of PII in systems adds operational risk, such as security incident or data breach, which can result in legal, regulatory, financial and reputational harm. These risks can be mitigated by collecting only minimally necessary PII required for the business purpose, knowing which PII is stored and used, and removing PII when it's no longer required.

It is important to understand what constitutes PII and to ensure its appropriate maintenance and use. The appendices that follow contain sample policies of the kind that may be used to help mitigate cyber threats and enhance the privacy and security of PII. However, it is important to keep in mind that there is no substitute for obtaining legal counsel and professional advice that is specific to individual circumstances.

Apple's Tim Cook is quoted as having said that "…people have entrusted us with their most personal information. We owe them nothing less than the best protections that we can possibly provide."

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].

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

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.

APPENDIX 2
[COMPANY NAME] INFORMATION TECHNOLOGY POLICY

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.

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:

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

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		
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