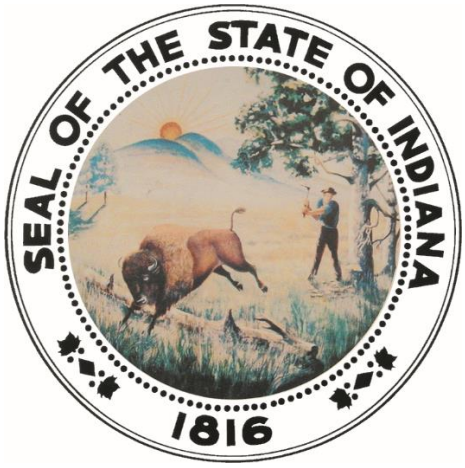
Personally Identifiable Information (PII) Guidebook



Personally Identifiable Information Working Group of the Indiana Executive Council on Cybersecurity

January, 2021

TABLE OF CONTENTS

Introduction to the PII Guidebook 1
Acknowledgements 2
Defining Personally Identifiable Information ("PII") 3
PII Guidance Sources 3
PII Guidance Sources and Definitions 3
Observations and Analysis 5
Summary of Categories of PII That Must Be Protected 6
Characterizing the Current State of PII 8
Identifying Related Regulations 10
Future Developments Considered 12
Data De-identification 12
Genomics 12
Cross-context Identification & The Mosaic Effect 12
Vendor Management & Data Protection 12
Payment Card Industry 13
Blockchain and Distributed Ledger Technologies 13
Section Conclusion 13
Best Practices 14
Conclusion 15
Appendices 1-3 16

INTRODUCTION TO THE PII GUIDEBOOK

Formed by the Indiana Executive Council on Cybersecurity, the Personally Identifiable Information Working Group (the "PII Working Group") is made up of private and public sector leaders in Indiana's privacy and cybersecurity realms. The PII Working Group has been tasked with the following:

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

This guidebook can be leveraged by Indiana businesses, small and large, to identify the information that requires a heightened degree of protection. Whether your role is to collect basic customer information at the service counter at your business in Columbia City, validating information in cargo containers at the Port of Indiana-Mount Vernon, or processing medical claims in Indianapolis, the collection and maintenance of PII in your systems adds risk to your operation. This risk can be realized by the inadvertent disclosure of PII, which can cause harm in operational, legal, and reputational contexts. These risks can be mitigated by collecting only that PII which is required to complete a given transaction. To do that, we must understand what constitutes PII in our daily lives. This guidebook intends to help you gain that understanding.

ACKNOWLEDGEMENTS

A special thank you to members of Indiana Executive Council on Cybersecurity's PII Working Group who stepped forward to offer their expertise through this document. Specific mention is warranted for John Babione, Richard Braidich, Dom Caristi, Tony Chu, Ted Cotterill, Dewand Neely, Mitch Parker, Leon Ravenna, and Ashley Schenck. Additionally, thank you to Indiana Cybersecurity Program Director Chetrice Mosely for her support throughout the drafting and review process and to members of the Indiana Executive Council on Cybersecurity for their guidance. Lastly, thank you to Governor Eric Holcomb for his leadership, without which, the State of Indiana would not be leading the charge in cyber readiness.

DEFINING PERSONALLY IDENTIFIABLE INFORMATION ("PII")

PII Guidance Sources

The purpose of this section is to identify and evaluate several definitions of PII to determine the specific data elements that should be regarded and protected as PII.

- 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
- 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	As defined by National Institute of Standards and Technology (NIST) Special Publication 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), "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 categories of PII are sensitive as stand-alone data elements. Examples include: SSN, driver's license or state identification number, passport number, alien registration number, or financial account number. Other data elements such as 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), are also Sensitive PII.
HIPAA	Pursuant to NIST Special Publication 800-66, Rev 1, "Individually Identifiable Health Information (IIHI) [45 C.F.R. Sec. 160.103], Information that 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: • Education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g; • Records described at 20 U.S.C. 1232g(a)(4)(B)(iv); and • Employment records held by a covered entity in its role as employer.
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 PUB 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	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 they reasonably represent all relevant definitions for the purpose of this guidebook. Almost all of the examined definitions start with a general description that PII is any information that can be used to distinguish or trace an individual's identity, followed by examples of PII. No source provides a comprehensive list of PII data elements.

The DHS definition specifies the difference between two different types of sensitive PII—stand-alone and if paired with another identifier. DHS gives examples of stand-alone sensitive PII as social security, driver's license, and alien registration numbers. Alone, this data can be used to access a great deal of personal information. In contrast, DHS explains that other information, like medical information, date of birth, and mother's maiden name is not sensitive PII unless combined with other identifying information like the name of the individual to which it relates.

Based on the DHS guidance, the next section of this guidebook defines data elements that are Singularly PII and Collectively PII. Singularly PII data elements will be consistent with the DHS definition of stand-alone sensitive PII. Collectively PII data elements will be consistent with the DHS definition of PII that is sensitive when paired with another identifier.

While not identified in any of the above definitions, organization-specific data can also be PII. To illustrate, a unique identification number associated with a customer's record containing sensitive information in an organization's system could be considered PII if the name of the system were known. In another case, an

organization's record of answers to normally non-sensitive questions might be PII if they are answers to challenge questions when a user attempts to log into the organization's system without their password. Consequently, the next section of this guidebook also identifies examples of organization-specific PII.

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

Most government agency definitions of PII are not specific enough to enable those responsible for protecting it to fully understand what data they are trying to protect. Part of that challenge relates to the evolving definition of PII, which is addressed in more detail later in this guidebook. To assist those wrestling with these issues, this guidebook provided (above) as comprehensive of a list of specific PII data elements as can be provided.

The table above and the other information provided in this guidebook should enable individuals, small business owners, and large industry and government organizations, who have an interest in or legal obligations to protect PII, to be more effective. It is important to understand, however, that the definition

of PII varies for different states within the Unites States and varies across the globe by nation. Accordingly, for organizations operating in multiple states and/or internationally, the definition and regulation of PII in those other jurisdictions should be carefully reviewed.

CHARACTERIZING THE CURRENT STATE OF PII

Companies, consumers, and governments alike should be prepared for ever-evolving definitions and regulations surrounding the handling and security of PII, particularly in the near-term. The development and adoption of new technologies has grown rapidly in the 21st century. Enhanced technologies allow consumers to live in a connected world with real-time access to information. Technology in the hands of consumers has also enabled the collection of an ever-growing amount of data.

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. Between the release of newly-available public data and an increasing amount of data collected from private entities, arose the possibility for re-identification 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.

The global privacy community has responded to the collection of growing amounts of data through regulations aimed at protecting individuals' information, such as the European Union's General Data Protection Regulation (GDPR). GDPR took effect in May 2018 and, in concert with the Data Protection Act of 2018, supersedes the Data Protection Act of 1998. This new regulation 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 definition broadly defines what is considered personally identifiable information in relation to EU data subjects. Following suit with the global community's posture to improve individual privacy, the California Consumer Privacy Act (CCPA) took effect in January 2020 and has quickly become the most expansive data privacy regulation in the United States. 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.

As previously discussed, increasing technological advances and a growing amount of consumer data has led to the fixed-element definition of PII becoming a thing of the past. The CCPA, CPRA, and GDPR are leading regulations in this space and lend themselves to the current state of PII, a concept currently in flux. In 2020, 30 US states and Puerto Rico considered some form of data privacy legislation, with some seeing a groundswell for likely adoption in the coming months. At the beginning of 2021, Congress is coalescing around two federal consumer privacy bills. 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 Senator Roger Wicker's "Setting an American Framework to Ensure Data Access, Transparency, and Accountability" (SAFE DATA) Act. While many fundamental privacy principles are addressed similarly in these bills, there remain specific areas where negotiations continue between interested parties. For the

purposes of this guidebook, it is important to understand that the various sides are at the table and meaningful federal consumer privacy discussions are underway. At the time of publication, these negotiations continue.

The GDPR, CCPA, CPRA, and other regulatory examples not limited to Indiana are of importance in the context of this guidebook as they impose outsized influence on continuing policy development related to privacy and data protection. Taken together, these regulations have set the standard in the European Union and, through California, across much of the US.

IDENTIFYING RELATED REGULATIONS

To ensure that users of this guidebook are fully informed, the PII Working Group has attempted to compile a list of all regulations relevant in the data privacy context. While this list relates specifically to data privacy, a more complete list of State and Federal cyber laws has been published by the Legal and Insurance Working Group and is made available via https://www.in.gov/cybersecurity/files/IECC%20Legal%20and%20Insurance%20Working%20Group%20Survey%20of%20Cyber%20Laws.pdf.

- Regulations applicable to business, health providers, and schools
  - Indiana (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, https://www.in.gov/mph/files/State-of-Indiana-Information-Privacy-Policy.pdf
    - 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 4, *Security and Privacy Controls for Federal Information Systems and Organizations*
        - NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*
        - Publication 1075, *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

As has been referenced, privacy and data protection continue to be evolving areas of study and regulation. Members of the PII Working Group maintain specialized knowledge in the field and, by discussing next steps in data privacy, hope to peer into the future on a handful of topics for the benefit of the guidebook's users.

Data De-identification

It is important to note that simply because data is labeled as having been 'de-identified' that does not rule out the possibility of reidentification. It is very easy to reidentify data by applying combinatoric algebra and there are many writings on the subject and references to those that have done this. Further, data perturbation, where data is distorted by the de-identification process, distorts the data sets. Unless de-identification is completed using a method that does not distort specific data elements, it is highly likely to occur, lessening the integrity of the data in question. Technologies that can be leveraged to reidentify previously 'deidentified' data will continue to advance. A foundational understanding of what constitutes PII in the singular, collective, and organizationally-specific contexts is key to combatting this.

Genomics

Genomics and precision medicine raise the concern of genomic data being used to identify people, even indirectly. Despite the resulting convictions, recent cases involving GEDmatch and 23andme being used to help identify cold case murderers raised numerous privacy concerns due to law enforcement access to genomics data. While 2008's Genetic Information Nondiscrimination Act created new protections in the health insurance and employment contexts, technological advances are rapidly outpacing data protection regulation in this space.

Cross-context Identification & The Mosaic Effect

There are countless data sources from private-sector brokers to public-sector records, all of which can contribute to concerns relating to cross-context identification and the mosaic effect. Cross-context identification can manifest through Ad Tech's internet and app-enabled behavioral advertising apparatus, which can track you across devices and websites. This is in addition to the voluminous number of data sets available from data brokers, which can be leveraged to form a detailed profile on a specific individual. 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. In a concerning development, this also included information on children.

Beginning with street address, cross-identification can use multiple data sets to produce a more detailed picture of the data subject. Profiles are built using public property information, data about political and charitable donations, and organizational membership activities. The 2020 ransomware attack on Blackbaud contained this information and more in its ResearchPoint application, which allowed the targeting of high-value donors by calculating their net worth and potential ability to donate.

California's recent passage of the CPRA begins to address this in specific contexts. The CPRA defines cross-context behavioral advertising and imposes limitations that target this activity to do-not-sell obligations, while exempting certain analytics functions from the restriction. This illustrates that much of the risk mitigation related to cross-context and mosaic effect identification is best addressed by policymakers. The application of broad protections across sectors of industry and society provide the most significant return when disparate data sources are involved.

Vendor Management & Data Protection

With big-data analytics technologies now the norm, data is a strategic asset for companies and government and must be maintained and protected as such. A contract for services often involves the

exchange of data and information between organizations, potentially including elements of PII. Traditional contract boilerplate documents that protect obvious PII elements like name, address phone number, and email address have become outmoded. Businesses must not only protect the information they maintain on behalf of clients in a cloud solution, but they need to protect their own information as they interact with the third party vendor. This can be achieved through vendor and cloud-specific contract boilerplate terms that explicitly protect organizational assets like data holdings from extra-contractual uses.

Third party systems should also be verified as meeting appropriate cybersecurity thresholds, depending on the type of information planned for the system in question. 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 the potential vendor. As organizations shift to a cloud-first posture for IT, programs like FedRAMP and StateRAMP will become all the more important to ensure that data protection is built into contracts and vendor management in an efficient way.

Payment Card Industry

The payment card industry continues to evolve and there are expectations that Payment Card Industry-Data Security Standards, known as PCI DSS, will be updated to address cardholder identity management and protection of personal data other than cardholder data. Current PCI standards address identity management only for those with job roles or necessity to access the data, but not for cardholders themselves. Publicly-available information leveraged in conjunction with cardholder data, even if partially redacted, can be used to build user and marketing profiles of individuals. This then can be used to re-identify the users of single-use cards, temporary cards, or virtual card numbers. Many believe that consumer data should be protected as much as credit card data due to potential for misuse and identity theft. The upcoming PCI DSS 4.0 standard makes initial inroads in this area. As the numbers themselves become ephemeral using virtual card numbers, as with the Apple Card for example, the surrounding data becomes the identifying data that can be used to re-identify and enable fraud.

Blockchain and Distributed Ledger Technologies

Recently, observers have noted an increasing volume of companies touting the use of Digital Distributed Ledger Technologies and Distributed Verification and Validation Techniques, more commonly referred to as Blockchain, as a privacy-enhancing or security-enhancing technology. This remains in dispute as Blockchain technologies were designed to achieve greater integrity, rather than privacy or security as a whole. 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 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 provides a window into the potential near-term future of data privacy. While many of the covered topics are touched on only briefly, the goal of the PII Working Group is to share a general perspective of this evolving area at the intersection of the law and emerging technologies.

BEST PRACTICES

This list offers brief insights and best practices to prepare an organization to be successful in maintaining the privacy of its customers and other stakeholders.

1. Create cybersecurity, internal, and external privacy policies and notices and make them known to all involved. As self-evident as this may appear, some entities do not have internal policies and external-facing notices in place or, if they do, they are not known by those affected.
2. 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 that are employed to protect their privacy. Customers/clients must know exactly who to contact (and how) in case of a concern.
3. Conduct regular security audits and privacy impact assessments, or contract to have these conducted, to determine vulnerabilities.
4. Implement a mandatory education and orientation process for all employees who have access to PII. This can be either created in-house or purchased from third-party providers or professionals.
5. Know and follow applicable laws and regulations specific to your industry. In the United States, sector-specific laws regulate data use and/or dissemination in various realms (health, financial, education, etc.).
6. In addition to state and federal law, those who do business internationally are subject to additional sets of rules. For example, the GDPR regulates the collection, use, and transfer of data pertaining to European citizens.
7. In order to transfer data between the European Union and U.S., organizations can join the Privacy Shield Program to self-certify compliance with data privacy regulation in the EU.
8. Monitor or participate in the activities of not-for-profit organizations that promote cybersecurity measures, such as the Center for Internet Security or the All Hazards Consortium. Whether or not their products are purchased, they provide current information via alerts, seminars, and newsletters.
9. Cybersecurity policies should include a plan for informing constituents of any security breach. Best practices require prompt notification.
10. Share information with state and federal authorities. Report not only confirmed data breaches, but possible security incidents and potential threats.
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 businesses, small and large, to identify the information in their environment that requires a heightened degree of protection. Across various sectors and individual roles, the collection of PII in systems adds risk to your operation, realized in the context of a security incident or data breach, which cause operational, legal, and reputational harm to businesses. As we've discussed, these risks can be mitigated by collecting only that PII which is required to complete a given transaction.

The PII Working Group has defined and characterized the PII realm, identified regulations related to PII, addressed potential future developments in the practice of privacy and data protection, and has identified practical best practices which organizations are encouraged to apply. After reading this guidebook, you should now be able to call on your understanding of what constitutes PII and how to ensure its appropriate maintenance and use, giving your organization a leg up in today's virtual economy. In the appendices that follow, the PII Working Group has provided sample policies that can be leveraged in the development of your own organizational policies to mitigate cyber threats and enhance the privacy and security of your digital information holdings.

For those of us in government, we serve as stewards of the peoples' information. We strive to maintain that information with an intense focus on privacy and data protection. 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." In the business environment of today and tomorrow, that isn't true only for Apple, but for businesses small and large.

APPENDICES 1-3

The appendices that follow offer templates that can be leveraged to formulate an internal privacy policy, an information technology policy, and a cyber incident response procedure. While these templates are not intended to replace counsel and guidance tailored to the user's particular challenges or issues, they can serve as a starting point and guide throughout the development process.

APPENDIX 1
[COMPANY NAME] INTERNAL PRIVACY POLICY
To the prospective user of this policy Template:

This policy is to be used internally in your organization. It is different in purpose and content from an *externally* facing privacy notice, like the type that you might post on your website.

There are several reasons you should consider taking the time to utilize this template and to customize it to your business. Chief among those reasons is that this type of policy helps create a culture and environment where your organization treats data with care. That type of culture will help your organization succeed in today's digital business world. In addition, your employees, including management, cannot be expected to understand the role and importance of privacy practices without some guidance, which this policy provides. Management/ownership must provide the policies, procedures and tools to implement the needed rules and expectations to protect data.

This policy template, and the guidance herein, will work with and support your organization's larger data privacy and cybersecurity efforts. That is, this policy 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 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. In addition, the larger your organization is in terms of number of employees and/or data handling, and/or the larger its geographic footprint of where it operates, the more likely it is that your organization needs a policy longer and/or more complex than this template, and legal counsel should be consulted.

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

1. **Purpose of this Policy**

At [Company Name], we are committed to promoting a work environment and operating the business in a manner that fosters confidence and trust. To accomplish this goal, we must properly manage and protect the Personal Information provided to us by our customers, fellow employees, vendors and suppliers. This Policy sets forth how we will govern and protect that Personal Information.

It is critical that all employees and executives understand that mishandling Personal Information can result in substantial harm to our customers, employees and others. This harm may include financial harm to our company, employees or business partners. The harm may also include identify theft and fraudulent use of information. In addition, mishandling Personal Information 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 any third–party contractors or third-party provider of services to our company ("Third-Party Provider") who have access to any Personal Information from our company.

This Policy applies to all Personal Information 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 person.

APPENDIX 1
[COMPANY NAME] INTERNAL PRIVACY POLICY

3. **Definitions**

"Data Subject" means the person about whom Personal Information is collected.

"Personal Information" 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 Personal Information ("**PI**"), 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 PI.

4. **Using and Retaining Personal Information**

Notice and Collection. It is our company's policy that whenever we collect PI 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 PI 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 PI in compliance with applicable company policies, notices, and/or Data Subject consent. PI 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 PI when that information relates to and is necessary to perform their job duties. You may not use PI 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.

PI 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 PI complies with any privacy notice provided to the Data Subject. You may not share PI 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 PI that the company collects, maintains, and uses is accurate, complete, and relevant to the purposes for which it was collected. Employees should report inaccurate PI to their supervisor.

Security. All employees are responsible for doing their part to help protect PI. [Company Name]'s Information Technology ("IT") and/or Information Security ("IS") personnel have implemented certain technical, administrative and physical safeguards for the protection of PI. Employees must follow those security procedures at all times. You must exercise particular care in protecting the types of *sensitive* PI listed above in this Policy from loss, unauthorized access and unauthorized disclosure.

Retention and Disposal. PI 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 PI.

5. **Training Employees and Supervising Contractors**

All [Company Name] personnel who have access to PI will be trained on this Policy and are expected to abide by it. The company also expects that employees will help ensure that PI 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 PI, 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 PI 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 PI 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 policy is to be used internally in your organization. There are several reasons you should consider taking the time to utilize this template and to customize it to your business. Chief among those reasons is that this type of policy helps create a culture and environment where your organization treats data with care. That type of culture will help your organization succeed in today's digital business world. In addition, your employees, including management, cannot be expected to understand the role and importance of privacy and security practices without guidance. Management/ownership must provide the policies, procedures and tools to implement the needed rules and expectations to protect data.

This policy template, and the guidance herein, will work with and support your organization's larger data privacy and cybersecurity efforts. That is, this policy 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 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. In addition, the larger your organization is in terms of number of employees and/or data handling, and/or the larger its geographic footprint of where it operates, the more likely it is that your organization needs a policy longer and/or more complex than this template, and legal counsel should be consulted.

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

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, providing these resources raises potential risks for Company, including loss or misuse of Confidential Information, and/or data breach of company data, all resulting in potential legal consequences for Company and/or its employee(s). Therefore, to protect Company and its employees, this Policy restricts the use of all IT resources, communications systems and equipment as described below.

The resources covered by this Policy 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 any IT or communications system in a manner that may be construed as harassing or offensive 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.

1.1 Administration of this Policy

APPENDIX 2
[COMPANY NAME] INFORMATION TECHNOLOGY 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 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 an employee's own 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.

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 and not the employee. 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.

Do not use the company's IT SYSTEMS for any matter that you desire to be kept private or confidential from the company.

1.4 Network Systems – Access Is Limited by Authorization

Company maintains integrated IT SYSTEMS to facilitate all aspects of its business. You may never sign on to any network equipment using the password or user name 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

You are never permitted to use the IT SYSTEMS for any inappropriate or unlawful purpose. This includes but is not limited to:

- Misrepresenting yourself 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, 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 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, in order 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 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].

APPENDIX 2
[COMPANY NAME] INFORMATION TECHNOLOGY POLICY
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 Company's computer network entirely at the end of each workday.

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

3.7 Passwords

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

Employees may not share user names, 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 user name, 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.]

APPENDIX 2
[COMPANY NAME] INFORMATION TECHNOLOGY POLICY

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. In addition, the larger your organization in terms of the number of employees and/or data handling, and/or the larger its geographic footprint of where it operates, the more likely it is that your organization needs a procedure which is more complex than this template, and legal counsel should be consulted.

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.

The 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 company 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 even issues that they believe are minor, because it will provide information to the IRT of 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 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 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