PERSONALLY IDENTIFIABLE INFORMATION (PII)

General Overview

Personally Identifiable Information (PII) has become a notable topic in information security as organizations are spending vast resources for ensuring the safety and security of such information, much of it revolving around personal consumer financial and health data. With growing cyber security threats and the ever-increasing numbers of data breaches and security compromises, protecting PII is now more important than ever. With the widespread use of technology, PII is everywhere, being stored, processed and transmitted all over the globe, at levels of efficiency once thought unimaginable. But with hundreds of millions - and counting - of individual PII breaches, organizations are finding themselves being constantly challenged by malicious threats, lawsuits, regulators, compliance auditors, and irate customers.

What's needed for ensuring the confidentiality, integrity, and availability (CIA) of PII are well-documented policies and procedures establishing highly-formalized practices for the use and disclosure of such information. What exactly is PII - according to the National Institute of Standards and Technology (NIST) publication SP 800-122, "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), it is the following:

"Any information about an individual, 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". Additionally, as for "distinguishing", "tracing", and "linking", NIST SP 800-122 defines these attributes as the following:

- To distinguish an individual is to readily identify them.
- To trace an individual is to "process sufficient information for making a determination about a specific aspect regarding an individual's activities or status.
- As for linking, this is information that is logically associated with other information.

Additionally, numerous laws, legislative mandates and industry specific directives required the protection of PII at all times, making the challenges even greater for organizations who store, use, and disclose such information. The subsequent Personally Identifiable Information (PII) policy and procedures documents seeks to provide organizations with an extremely comprehensive, well-written, high-quality template designed for ease-of-use and customization.

Personally Identifiable Information (PII) Policy and Procedures

Title	**[company name] Personally Identifiable Information (PII) Policy and Procedures**
Version	Version 1.0
Date	TBD
Language	English
Individual and/or Department Responsible for Distribution of Document	[company name] Information Technology Department
Individual and/ or Department Responsible for Timely Update of Document	[name and title]
Developed by:	[company name]
Subject	Use of Software
Approval Date	TBD
Purpose of Document	To implement comprehensive Personally Identifiable Information (PII) policies, procedures, and practices whereby all employees and other intended parties are readily aware of the organization's PII policies.
Distribution of Document	Disbursed to all employees of [company name] and available by request to all other intended parties.

1.0 Overview

In accordance with mandated organizational security requirements set forth and approved by management, [company name] has established a formal Personally Identifiable Information (PII) policy and supporting procedures. This policy is to be implemented immediately along with all relevant and applicable procedures. Additionally, this policy is to be evaluated on a(n) [annual, semi-annual, quarterly] basis for ensuring its adequacy and relevancy regarding [company name]'s needs and goals.

1.0 Purpose

This policy and supporting procedures are designed to provide [company name] with a documented and formalized Personally Identifiable Information (PII) policy that is to be adhered to and utilized throughout the organization at all times. Compliance with the stated policy and supporting procedures helps ensure the safety and security of [company name] system resources. PII requires strict measures for ensuring unauthorized parties do not have access to such data, which can be in electronic format and/or hard copy, such as paper. Additionally, with the growing cyber security threats and the ever-increasing numbers of data breaches and security compromises, protecting PII is now more important than ever. From social security numbers, dates of birth, personal medical records, along with many other unique identifiers, companies are storing PII in record amounts. The subsequent policies and procedures relating to PII initiatives for [company name] strive to ensure the overall confidentiality, integrity, and availability (CIA) of highly sensitive and privileged information.

1.0 Scope

This policy and supporting procedures encompasses all system resources that are owned, operated, maintained, and controlled by [company name] and all other system resources, both internally and externally, that interact with these systems.

- Internal system resources are those owned, operated, maintained, and controlled by [company name] and include all network devices (firewalls, routers, switches, load balancers, other network devices), servers (both physical and virtual servers, along with the operating systems and applications that reside on them) and any other system resources deemed in scope.

- External system resources are those owned, operated, maintained, and controlled by any entity other than [company name], but for which these very resources may impact the confidentiality, integrity, and availability (CIA) and overall security of the aforementioned description of "Internal system resources".

- When referencing the term “users”, this includes any individual that has been granted access rights by [company name] and has went through all required provisioning steps. Users typically include, but may not be limited to, the following: employees, consultants, vendors, contractors, along with local, state, and federal personnel.

- For purpose of this policy, personally identifiable information (PII) is defined as the following: Any information about an individual, 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.

The main categories of the Personally Identifiable Information (PII) policy include the following:

- Personally Identifiable Information
  - Protected Health Information
  - Personally Identifiable Financial Information
- Regulatory Compliance
- PII Privacy Initiatives
- Identifying PII
- PII Impact Levels
- Protecting PII
  - Hard copy
  - Electronic Format
- Minimization of PII
- Security Awareness
- Incident Response Measure and Reporting Breaches

1.0 Policy

[Company name] is to ensure that the Personally Identifiable Information (PII) policy adheres to the following conditions for purposes of complying with the mandated organizational security requirements set forth and approved by management:

PERSONALLY IDENTIFIABLE INFORMATION

The ability to successful ensure the safety and security of PII for [company name] is highly dependent upon understanding what PII is - specifically - what are common examples of this type of information. PII, regardless of industry or business sector, generally consists of the following:

- Full name, with all middle names (especially if the name is not common).
- Any part of an individual's name that is stored or displayed in conjunction with any of the subsequent listings of data and information deemed PII.
- National Identification information, such as passports, visas, permanent residence cards, voting information, social security number (United States), or any other type of unique identifier used on a national level.
- Local and/or state, provincial, etc. information, such as drivers licenses, vehicle registration and permit documents, or any other type of unique identifier used on a local and/or state, provincial level.
- Digital Identifiers, such as IP addresses, usernames, passwords, etc.
- Facial, fingerprint, iris and all other associated biometric information.
- Date of Birth
- Place of Birth

- Medical records (i.e. protected health information (PHI) and electronically protected health information (ePHI), and all associated data and information contained (electronically or hard-copy) with the medical records. Also, genetic information, if applicable.
- Criminal records
- Financial and Accounting records, such as banking, mortgage, revolving debt and tax information, along with credit and debit cards.
- Educational information, such as classes taken, schedule, grades received, degrees confirmed, disciplinary actions, financial aid, student loans, etc.
- Professional and occupational information, such as salary, tenure, etc.
- Professional licenses, certifications, designations, etc.
- Any other information deemed PII, but not listed above

In summary, PII consists of both the ***data and information*** that is unique to an individual and the ***source*** of the applicable data and information. For example, a social security number is the "data and information" of PII and the social security card or anywhere the number is found, imprinted, stored, or kept is the "source" of PII.

Protected Health Information (PHI)

Additionally, a subset of Personally Identifiable Information (PII) is that of Protected Health Information (PHI), which actually shares many similarities towards each other as to the types of data an information. Specifically, PHI contains the following list of eighteen (18) "identifiers"; data and information that is to be treated with extreme care, thus [company name] has identified these "identifiers" as "client confidential".

- Names.
- All geographical identifiers smaller than a state.
- Dates that directly relate to an individual (other than year).
- Phone Numbers.
- Fax Numbers.
- Email Addresses.
- Social Security Numbers.
- Medical Record Numbers.
- Health Insurance Beneficiary Numbers.
- Account Numbers.
- Certificate | License Numbers.
- VIN, serial numbers, license plate numbers.
- Device Identifiers and Serial Numbers.
- Web Uniform Resource Locators (URLs)
- Internet Protocol (IP) addresses.
- Biometric Identifiers, such as finger, retinal and voice.
- Full Face Photograph Images
- Any other unique identifying number, character, code, etc.

Personally Identifiable Financial Information (PIFI)
Furthermore, yet another subset of Personally Identifiable Information (PII) is Personally Identifiable Financial Information (PIFI) as discussed within the Gramm-Leach-Bliley Act (GLBA). Specifically, PIFI is the following: Any information: A consumer provides to obtain a financial product or service; About a consumer resulting from any transaction involving a financial product or service; or Otherwise obtained about a consumer in connection with providing a financial product or service. (www.ftc.gov).

There are various other forms of legislation that define what is considered "personal" information, rights for disclosure, and protective measure to be in place. It is thus the responsibility of [company name] to determine what, if any, additional laws, regulations, and "personal" privacy requirements are to be adhered to above and beyond the aforementioned list.

REGULATORY COMPLIANCE
Growing regulatory compliance laws, legislation, and industry specific rulings call for the protection of PII, and accordingly so, [company name] is to identify all compliance mandates regarding the safety and security of sensitive and confidential information, and the applicable measures for enforcement. The following list includes all applicable compliance rulings for which [company name] should be highly familiar with, if applicable:

- The Health Information Portability and Accountability Act (HIPAA) Privacy and Security rulings.
- The Health Information Technology for Economic and Clinical Health (HITECH) Subtitle D.
- The Gramm-Leach-Bliley Act (GLBA).
- The Family Educational Rights and Privacy Act (FERPA).
- Children's Online Privacy Protection Act (COPPA).
- Freedom of Information Act (FOIA).
- The Electronic Communications Privacy Act (ECPA).
- Federal Trade Commission (FTC) Red Flag Rule (Identity Theft Regulation).
- Payment Card Industry Data Security Standards (PCI DSS) regulation.
- All other applicable local, state, and federal laws and legislation.
- All other applicable industry directives.

PII PRIVACY INITIATIVES
The Organization for Economic Co-operation and Development (OECD) Privacy Guidelines, found at http://oecdprivacy.org/, provides a list of the following highly regarded privacy principles for which [company name] is to adhere to at all times:

- Collection Limitation Principle - There should be limits to the collection of personal data.
- Data Quality Principle - Personal data should be relevant to the purposes for which it is to be used.
- Purpose Specification Principle - The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes,

- Use Limitation Principle - Personal data should not be disclosed, made available or otherwise used for purposes other than those specified, except with the consent of the applicable data subject or by law.
- Security Safeguards Principle - Personal data should be protected by reasonable security safeguards against such risks as loss or un-authorized access, destruction, use, modification or disclosure of data.
- Openness Principle - There should be a general policy of openness about developments, practices and policies with respect to personal data. Additionally, means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
- Individual Participation Principle - An individual should have the right: a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; b) to have communicated to him, data relating to him i) within a reasonable time; ii) at a charge, if any, that is not excessive; iii) in a reasonable manner; and iv) in a form that is readily intelligible to him; c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.
- Accountability Principle - data controller should be accountable for complying with measures which give effect to the principles stated above.

Source: The Organization for Economic Co-operation and Development | http://oecdprivacy.org/

IDENTIFYING PII

With a sound understanding of what constitutes PII and the applicable compliance rulings for [company name] regarding the safety and security of sensitive and confidential information, it is critically important to identify all PII, both in electronic format and hard-copy, paper-based. Authorized personnel are to undertake comprehensive measures for ensuring all PII has been identified and also classified accordingly with [company name] Data and Information Classification Policy, which provides the following classification levels:

- Unclassified | Public Information
- Proprietary
- Confidential
- Company Confidential
- Client Confidential
- Sensitive
- Trade Secret
- Top Secret

PII is to never be deemed anything less than confidential, as lower forms of data classification may expose such information to unauthorized parties.

PII IMPACT LEVELS

In accordance with the United States Federal Information Processing Standards Publication 199 (FIPS PUB 199), *"Standards for Security Categorization of Federal Information and Information Systems"*, as

published by NIST, all PII is to be assigned a category (i.e. " potential impact"). This standard, which is officially issued by the National Institute of Standards and Technology (NIST), details the following three (3) security categories (i.e. "potential impact") that correspond to each one of the respective CIA objectives (confidentiality, integrity, and availability):

- Category | Impact: LOW-The unauthorized disclosure, modification, destruction, deletion, and removal of information along with the disruption of access to information results in a LIMITED adverse effect on the organization.
- Category | Impact: MODERATE- The unauthorized disclosure, modification, destruction, deletion, and removal of information along with the disruption of access to information results in a SERIOUS adverse effect on the organization.
- Category | Impact: HIGH- The unauthorized disclosure, modification, destruction, deletion, and removal of information along with the disruption of access to information results in a SEVERE | CATASTROPHIC adverse effect on the organization.

The CIA objectives of Confidentiality, Integrity, and Availability are as follows:

- Confidentiality: Preventing the disclosure of information to unauthorized individuals and/or systems.
- Integrity: Ensuring that information cannot be modified undetectably, such as guarding against improper information modification or destruction.
- Availability: Ensuring that information is available as needed, which consists of timely and reliable access.

PROTECTING PII

Hard Copy Material | Paper Records

PII is to be protected at all times, both physical hard-copy material and in electronic format. As for hard-copy documents - even in today's world, the use of paper is still quite prevalent - protecting paper records in the following manner is a must:

- First and foremost, avoid printing any documentation containing PII if you can. If that's not possible, then limit it to the extent possible. Remember, paper records should only be generated, used, and/or retained if there's a true legitimate business need.
- For paper records containing PII, assign tracking and logging mechanisms as necessary for ensuring its use and whereabouts at any given time, along with assigning an approved data classification level (i.e., sensitive, secret, etc.) for such material.
- For paper records containing PII, they must be physically stored in a secure location at all times, such as locked file cabinets, office desks, or any other acceptable measure for ensuring their safety and security from unauthorized parties.
- When such records are no longer needed for business or compliance purposes (such as data retention laws, etc.), they are to be shredded and documented accordingly. This means having secure shredding bins strategically located throughout the facility, and it also means never throwing paper records containing PII - or any other sensitive and confidential [company name] information - into a garbage can without being shredded.

- Other acceptable means of destroying paper records containing PII may include, but are not limited to shredding, burning, pulping, or pulverizing the records so that PII is rendered essentially unreadable, indecipherable, and otherwise cannot be reconstructed.
- Do not allow paper records containing PII to be viewable or accessible in general commons areas, or in an unsupervised fashion, such as residing on your desk or any other workstation | work areas while not being present.
- The transporting of paper records containing PII is to be limited to authorized personnel only at all times.
- When transporting paper records, please keep in mind the following best practices:
    - Keep information close to you at all times.
    - When unattended, ensure information is physically secure, such as in a locked file cabinet, safe, etc.
    - Keep information away from public view as for not "broadcasting" to the general public the documentation in your possession.
    - Don't transport other hazardous or dangerous items (i.e., chemicals, etc.) when transporting PII.
- Implement physical access controls and other security safeguards for protecting paper records containing PII at all times, such as the following:
    - Use electronic access control systems (ACS), such as badge readers, and applicable biometrics identifiers.
    - Promptly remove all users from company-wide access to all system resources and facilities upon their termination.
    - Utilize security cameras, alarms, and other physical security detective and preventative solutions.
    - Include provisions for responding to issues and security breaches pertaining to paper records containing PII.
- Be alert at all times. If you see paper records being inappropriately handled, residing in secure areas, left unattended, have been subject to unauthorized access, etc., please notify