|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Information Security Policies | | | | | |
| Employee Privacy Management Policy | | | | | |
| Policy # | CPL-16-01 | Effective Date | MM/DD/YYYY | Email | policy@companyx.com |
| Version | 1.0 | Contact | Policy Author | Phone | 888-641-0500 |

Table of Contents

[Purpose 1](#_Toc393402992)

[Scope 1](#_Toc393402993)

[Policy 2](#_Toc393402994)

[Management Responsibilities 2](#_Toc393402995)

[Prior to Employment 2](#_Toc393402996)

[During Employment – Protection of PII 2](#_Toc393402997)

[After Employment 3](#_Toc393402998)

[Violations 4](#_Toc393402999)

[Definitions 4](#_Toc393403000)

[References 4](#_Toc393403001)

[Related Documents 5](#_Toc393403002)

[Approval and Ownership 5](#_Toc393403003)

[Revision History 5](#_Toc393403004)

Purpose

A wide variety of state-level data protection laws require the protection of sensitive personal information of employees via written policies and procedures. While most of the laws specifically address Social Security Numbers, many of the newer laws (such as those of New York and Texas) are taking a broader definition of sensitive employee data. Thus, this sample policy is written to refer to a generic class of sensitive personal identifying information which can be refined within the definitions section based on the specific organizational requirements. This sample policy addresses some of the high-level requirements of these data protection laws and can be used as a framework for a more comprehensive policy document. This document is based on the general employee protection requirements of The New York Social Security Number Protection Law and The New York Employee Personal Identifying Law.

As part of ongoing business operations, Company X periodically collects personal identifying information (PII) from its employees and contractors. Examples may include social security numbers (SSN), driver’s license number, and personal address details. This information is required for proper screening, management and reporting of human resource activities, as well as the facilitation of information security policies and procedures.

In recognition of the fact that improper disclosure of an employee’s personal information may subject the individual to various privacy concerns, including the possibility of identity theft, Company X has adopted this Employee Personal Information Privacy Policy to protect the confidentially of all employee data.

Scope

This policy applies to employees, contractors, consultants, temporaries, and other workers at Company X, including all personnel affiliated with third parties.

Policy

### Management Responsibilities

**Inventory of Employee Personal Information Data Types** – Company X must perform an annual inventory of all data elements collected, stored or transmitted within company records which may constitute Personal Identifying Information under this policy. Any information which may contribute the possible theft of an individual’s identity may be considered sensitive personal information and fall under this definition.

**Classification of Employee Personal Identifying Information** – All data records that contain one or more elements of PII must be classified as “CONFIDENTIAL” data according to the Company X data classification scheme.

**Personnel Training Required** – All Company X personnel who handle sensitive PII must be given specific notice and training on the contents of this policy and on specific Company X business processes that prohibit the disclosure of PII to external parties.

### Prior to Employment

**Prospective Employee Personal Information** – Sensitive personal information about a prospective employee may not be gathered unless it is necessary to make an employment decision and relevant to the job. This policy addresses social security numbers, marital status, family planning objectives, off-hours activities, political affiliations, performance on previous jobs, previous employers, credit history, education, and other personal details.

### During Employment – Protection of PII

[Sensitive employee data must be protecting throughout its lifecycle, including gathering, storage, transmission and disposal.]

**Limited Collection of Employee Personal Information** – Company X must limit the amount of sensitive personal information gathered for each employee to only the data necessary for managing the business requirements of employment.

**Surreptitious Collection Of Private Information** - Company X computer and communications systems must not collect sensitive private data from employees without having obtained their clear and unambiguous consent.

**Biometric Information Collection** - Personal biometric information may not be captured by any Company X information systems unless the individual described has been previously notified of and has consented to the capture.

**Prohibited Use of Social Security Numbers** – Company X will not use employee PII, such as social security numbers, in the creation and issuing of computer userids, email addresses or other system access controls.

**Encoding of Social Security Numbers** – Company X will not encode sensitive employee data such as social security numbers in any format that disguises the SSN but can be easily read. Examples include bar codes, RFID tags or magnetic strips.

**Display of Employees PII** – Company X must not display an employee’s personal information on any printed document used for public display, such as company access badges or ID cards.

**Prohibited Disclosure of Employee’s Personal Information** – Company X employees must never disclosure the sensitive personal information of any other employee to the general public, or to another employee of Company X without a legitimate need-to-know. Questions about this policy should be directed immediately to a supervisor and/or to the *Director of Human Resources*.

**Filing Paper or Electronic Documents** – Company X must not file any documents containing employee PII that may be subject to public disclosure via public inspection and third-party filings. (Examples include external licensing boards or certification authorities.)

**Physical Protection of PII** – All files containing printed copies of employee PII must be kept in locked file cabinets, secure rooms, or otherwise secured from physical access by personnel not authorized to view these records.

**Transmission of Electronic Information** – All transmission of electronic employee PII outside of Company X networks must be encrypted using Company X standard encryption tools authorized by the Information Security Department.

[Organizations may wish to change the reporting channels or provide a specific tile and contact number in this policy statement.]

**Reporting Suspected Disclosures** – Employees who believe that their own PII or that of another employee may have been improperly disclosed must immediately report the disclosure to their immediate supervisor and to a member of the Human Resources Department.

### After Employment

**Destruction of Employee’s PII** – All disposal of employees’ PII must be according to established Company X data disposal policies and procedures for sensitive information.

**Limited Retention Periods** – Company X will retain the PII of employees no longer employed at the company for a period of up to one (1) year. After that time, the records of these employees will be scheduled for destruction and disposal.

Violations

Any violation of this policy may result in disciplinary action, up to and including termination of employment. Company X reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. Company X does not consider conduct in violation of this policy to be within an employee’s or partner’s course and scope of employment, or the direct consequence of the discharge of the employee’s or partner’s duties. Accordingly, to the extent permitted by law, Company X reserves the right not to defend or pay any damages awarded against employees or partners that result from violation of this policy.

Definitions

**Partner –** Any non-employee of Company X who is contractually bound to provide some form of service to Company X.

**Opt-Out Notice** **-** Notification to customers that they may choose not to permit their information shared with nonaffiliated third parties.

**Pretext Calling** **-** A method of impersonation where person poses as a customer or someone authorized to have customer information in order to obtain confidential customer data.

**Privacy Program** **-** The guidance provided that will enable Company X to maintain information about individuals while protecting the right of the individuals against unwarranted or illegal invasions of their privacy.

**Partner -** Any non-employee of Company X who is contractually bound to provide some form of service to Company X.

[This section contains the definition of the PII that your organization will use to define this policy. The type of information will vary from state to state and business to business.]

Personal identifying information (PII) - Information that alone, or when combined with other personal or identifying information can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual.. For the purpose of this policy, PII includes the following:

* Social Security numbers (“SSNs”)
* Home address or telephone numbers
* Personal e-mail addresses
* Internet user IDs and passwords
* Driver’s license numbers
* Parents’ last names prior to marriage
* Biometric Data

**User -** Any Company X employee or partner who has been authorized to access any Company X electronic information resource.

References

*At least 30 different U.S. states have laws that protect the sensitive information of employees, including social security numbers. Use this section to refer the specific state laws that impact your organization.*

At least 30 different U.S. states have laws that protect the sensitive information of employees, including social security numbers. States and territories that have enacted legislation regulating the use of SSNs include Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Georgia, Hawaii, Idaho, Illinois, Kansas, Maine, Maryland, Massachusetts, Michigan, Minnesota, Missouri, Nebraska, New Jersey, New Mexico, New York, North Carolina, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Carolina, Tennessee, Texas, Utah, Vermont, Virginia, and Puerto Rico. Although most of these state statutes generally apply to persons doing business in the state, some state laws, such as the Oklahoma and Nebraska law, apply specifically in the employment context. These state statutes have a range of effective dates.

CPL: 16.1 Employee Privacy Management

ISO 27002: 18.1.4 Privacy and protection of personally identifiable information

HIPAA: Privacy Rules

NIST: Appendix J: Privacy Controls

Related Documents

Approval and Ownership

|  |  |  |  |
| --- | --- | --- | --- |
| Owner | Title | Date | Signature |
| Policy Author | Title | MM/DD/YYYY |  |
| Approved By | Title | Date | Signature |
| Executive Sponsor | Title | MM/DD/YYYY |  |

Revision History

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Description | Revision Date | Review  Date | Reviewer/Approver Name |
| 1.0 | Initial Version | MM/DD/YYYY | MM/DD/YYYY |  |
|  |  |  |  |  |