**PERSONAL INFORMATION PROTECTION POLICY**

**PURPOSE**

This policy outlines the requirements for handling and protecting personal information to prevent harm such as fraud, embarrassment, or inconvenience to individuals. It establishes principles for maintaining confidentiality and integrity, while defining responsibilities for safeguarding such information. Protecting personal data is essential, and compliance with this policy is required.

This policy applies to all employees, agents, and representatives, as well as any third-party service providers with access to personal information in [EMPLOYER’S NAME]’s possession. It covers all personal data collected, stored, transmitted, or processed by [EMPLOYER’S NAME], regardless of the format or medium, and includes data related to employees, customers, and other individuals.

This policy is designed to comply with Massachusetts laws governing the collection, use, and protection of personal information. However, federal or state laws may impose additional requirements that must also be followed.

**DEFINIITIONS**

Personal information

Personal information refers to any data that [EMPLOYER'S NAME] collects, maintains, or possesses that can identify or authenticate an individual. This includes, but is not limited to: names, addresses, phone numbers, email addresses, employee IDs, government-issued IDs, user credentials, financial account details, geolocation data, biometric or health information, and unique personal characteristics like habits or interests. For employees, this policy only applies to data stored in secure, restricted files.

Sensitive personal information

Sensitive personal information includes details that, if lost or improperly disclosed, could harm or inconvenience an individual. Examples include government-issued IDs, financial account numbers with or without security access codes, biometric or health data, precise geolocation, and criminal records. Additional sensitive categories may include racial or ethnic background, religious beliefs, sexual orientation, genetic information, or children's data, depending on applicable laws. If unsure whether information qualifies as sensitive, consult [CONTACT NAME OR DEPARTMENT].

Security incidents

A security incident occurs when personal information's security, confidentiality, or integrity is compromised, whether through loss, unauthorized access, or improper disclosure. This includes breaches of any safeguards implemented to protect personal information.

**COLLECTING PERSONAL INFORMATION**

When gathering personal information, [EMPLOYER'S NAME] must notify individuals of how the data will be used, processed, shared, and protected through a privacy notice at the time of collection. Personal information should only be collected in alignment with company policies, applicable notices, and when necessary, with the individual's consent. Any data collected must be limited to what is reasonably needed to fulfill legitimate business purposes or comply with legal obligations.

**ACCESS, USE AND SHARING**

Access to personal information is restricted to employees who need it to perform their job duties. Personal information may not be accessed, used, or shared for purposes unrelated to work responsibilities or in ways inconsistent with the privacy notice presented at collection. If you have doubts about the appropriateness of any use or disclosure, consult [SUPERVISOR/CONTACT NAME/DEPARTMENT]. Sharing personal information with colleagues or third parties is only permitted when there is a legitimate need to know, and sharing with third-party service providers must comply with privacy notice requirements. Prior written approval and a valid contract may be required.

**ENSURING ACCURACY**

Personal information must be accurate, complete, and relevant to the purpose for which it was collected.

**SAFEGUARDING PERSONAL INFORMATION**

Employees are responsible for safeguarding personal information at all times. [EMPLOYER'S NAME] has established an Information Security Program that outlines technical, physical, and administrative safeguards. Employees must adhere to these safeguards, exercising extra care when handling sensitive personal information to prevent unauthorized access, loss, or disclosure.

**RETENTION AND DISPOSAL**

Personal information must be retained only for as long as necessary to fulfill its business purpose or meet legal obligations. Employees must adhere to [EMPLOYER'S NAME]'s records retention schedules and disposal policies, ensuring that media containing personal information is securely destroyed when no longer needed.

**DATA SUBJECT RIGHTS**

Individuals may have rights concerning their personal information, depending on the jurisdiction. These can include the right to access, correct, delete, or know how their data is being used or shared. Additionally, they may have the right to opt out of data sales, targeted advertising, or certain uses of sensitive information. If you receive a request or complaint related to personal information rights, contact [CONTACT NAME/TITLE/DEPARTMENT] for guidance.

**CROSS-BORDER TRANSFERS OF PERSONAL INFORMATION**

When transferring personal information across international borders, [EMPLOYER'S NAME] must comply with all applicable laws and regulations governing such transfers. This includes:

* Ensuring adequate protections are in place for the transferred data through approved transfer mechanisms.
* Reviewing and complying with regional requirements, such as the European Union's General Data Protection Regulation (GDPR), applicable U.S. state privacy laws, and similar frameworks in other jurisdictions.
* Assessing risks to the privacy and security of the personal information being transferred.

Employees must consult with [the Legal Department/Privacy Office/Designated Contact] before initiating any cross-border transfer of personal information to ensure compliance with this section.

**TRAINING AND SUPERVISION**

All employees with access to personal information must undergo training on the proper handling and protection of such data as outlined in this policy. This ensures everyone understands their role in maintaining confidentiality and safeguarding information.

When sharing personal information with third-party service providers, it is essential to have proper oversight to ensure compliance with [EMPLOYER'S NAME]'s standards and applicable laws. Appropriate contracts must be in place to govern the provider's handling of personal information.

Supervisors responsible for managing employees or overseeing third-party providers must receive additional training to ensure they properly monitor compliance and enforce this policy’s requirements.

**REPORTING SECURITY INCIDENTS**

If you become aware of or suspect a security incident, you must not attempt to investigate the matter on your own. Immediately report the incident to [your supervisor, IT or security department, privacy office, legal department, or other designated contact]. Follow any procedures outlined in the Security Incident Response Plan to ensure the situation is managed appropriately.

Preserve all evidence related to the potential incident, including documents, logs, or communications, to support further investigation and resolution.

**MONITORING COMPLIANCE AND ENFORCEMENT**

[DESIGNATED CONTACT OR DEPARTMENT] is responsible for overseeing the implementation of this policy and for creating any necessary processes, procedures, and guidelines to support it. If you suspect a violation of this policy or any related measures for protecting personal information, you must report it immediately to [DESIGNATED CONTACT OR DEPARTMENT].

[EMPLOYER’S NAME] will conduct regular audits and reviews to ensure compliance with this policy. Any employee who fails to adhere to this policy or its supporting procedures may face disciplinary action, up to and including termination of employment.

**RELATED POLICIES**

Other [EMPLOYER’S NAME] policies also address the collection, use, storage, protection, and handling of personal information and are critical to ensuring compliance with this policy. You should review and adhere to these related policies, including but not limited to:

* Information Security Program
* [List other relevant policies here, such as Data Retention Policy, Acceptable Use Policy, and Incident Response Plan.]
* For further clarification or questions regarding these policies, contact [DESIGNATED CONTACT OR DEPARTMENT].

**ACKNOWLEDGEMENT OF RECEIPT AND REVIEW**

I, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (employee name), acknowledge that on \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (date), I received and reviewed a copy of [EMPLOYER'S NAME]’s [NAME OF POLICY]. I understand that it is my responsibility to familiarize myself with the policy and adhere to its terms.

I also acknowledge that this policy is not intended to create an employment contract or alter my at-will employment status, unless otherwise specified in a written agreement signed by an authorized representative of [EMPLOYER'S NAME]. Any delay or failure by [EMPLOYER'S NAME] to enforce the provisions of this policy does not constitute a waiver of its rights to enforce them in the future.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Printed Name

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date