Privacy Management Policy

(Last Updated April 2025)

Purpose

Our Data Privacy Policy aims to establish a comprehensive framework for protecting the privacy and confidentiality of personal and sensitive data entrusted to our organization. This policy aims to provide clear guidelines and procedures for data collection, storage, use, disclosure, and disposal in compliance with applicable privacy laws, regulations, and industry best practices. By implementing effective data privacy practices, this policy seeks to ensure the lawful and ethical handling of personal information, safeguard the rights and privacy of individuals, and maintain the trust and confidence of our customers, partners, and stakeholders. Through robust data protection measures, privacy impact assessments, and ongoing monitoring, we strive to mitigate the risks of unauthorized access, data breaches, and misuse of personal information while fostering transparency, accountability, and compliance in our data handling practices.

Scope

The Data Privacy Policy applies to all our organization's employees, contractors, vendors, and stakeholders. It encompasses the protection and responsible handling of personal and sensitive information collected and processed by the organization. This policy covers collecting, storing, accessing, transferring, and disposing of personal data in compliance with applicable data protection laws and regulations. It outlines procedures for obtaining consent, implementing security measures to safeguard data, ensuring data accuracy, and responding to data subject rights requests. The policy sets forth guidelines for data breach notification, data sharing agreements, and vendor management to protect the privacy and confidentiality of individuals' information. Compliance with this policy is mandatory for all individuals within the organization, and any deviations or exceptions require approval from the designated authority responsible for data privacy and cybersecurity governance.

Safeguards

To achieve the organization's overall mission, and the purpose of this cybersecurity policy, the organization shall:

PRV-01 Maintain a transparent, documented privacy program that documents the organization's safeguards to address data privacy.

PRV-02 Ensure that the organization's documented privacy program defines a process for performing data processing authorizations (authorizing, maintaining, and revoking).

PRV-03 Ensure that the organization's documented privacy program defines a process for reviewing, transferring, disclosing, modifying, or deleting data from the organization's information systems for privacy purposes.

PRV-04 Ensure that the organization's documented privacy program defines a process for recording and maintaining an individual's privacy preferences.

PRV-05 Ensure that the organization's documented privacy program defines a process for recording, maintaining, and reviewing stakeholder goals for data privacy.

PRV-06 Ensure that the organization's documented privacy program defines a process for evaluating the organization's use of data for bias.

PRV-07 Ensure that the organization's documented privacy program defines a process for recording and evaluating data provenance and lineage.

PRV-08 Ensure that the organization's documented privacy program defines a process for limiting the identification or inference of individuals when processing data.

PRV-09 Ensure that the organization's documented privacy program defines a process for replacing attribute values with attribute references in the organization's information systems for privacy purposes.

PRV-10 Ensure that the organization's documented privacy program defines a process for informing customers and external business partners about how their data is being used and the organization's privacy goals.

PRV-11 Ensure that the organization's documented privacy program defines a process to obtain feedback from individuals regarding the organization's use of data and the associated privacy risks.

PRV-12 Ensure that the organization's documented privacy program defines a process to allow individuals to request data corrections to their data.

PRV-13 Ensure that the organization's documented privacy program defines a process to allow individuals to request data deletions of their data (right to be forgotten).

PRV-14 Ensure that the organization's documented privacy program defines a process for sharing only appropriate data with third parties.

PRV-15 Maintain a technology platform to record the organization's efforts related to its data privacy program.

PRV-16 Ensure the organization's privacy record system tracks individuals' stated privacy preferences.

PRV-17 Ensure that the organization's privacy record system tracks data correction and deletion requests and the organization's response.

PRV-18 Ensure the organization's privacy record system tracks data disclosures or sharing personal information with third-parties.

Policy Sanctions

Non-compliance with this policy may result in disciplinary action in line with our corporation's human resources procedures. Consequences may range from mandatory refresher training and written warnings to temporary suspension of remote access privileges and, in severe cases, termination of employment or contractual obligations. Individuals could be subject to legal consequences under applicable laws if violations involve illegal activities. These sanctions emphasize the critical importance of cybersecurity, the individual's role in protecting our digital assets, and the potential risks associated with policy violations. Enforcement will be consistent and impartial, with the severity of the action corresponding directly to the seriousness of the breach.