PENNROSE

Bricks & Mortar | Heart & Soul

Data Protection & Cybersecurity Policy

This policy serves as a guide to the data protection and cybersecurity practices employed at Pennrose. Developed by the Information Technology Department in house, this code represents our ongoing commitment to technological safety.

Updated August 2024

Pennrose

Data Protection & Cybersecurity Policy

Introduction

Pennrose acknowledges the paramount importance of safeguarding sensitive data, preserving user privacy, and mitigating data security risks. This policy delineates our unwavering commitment to upholding the most stringent standards of data protection, privacy, and security in all facets of our operations and interactions.

Scope

This policy applies comprehensively to all personnel, including employees, contractors, third-party vendors, and affiliates entrusted with handling sensitive data or granted access to systems housing such information on behalf of Pennrose.

Definitions

Sensitive Data: Refers to any information whose unauthorized disclosure could engender harm to individuals or the organization. This encompasses personally identifiable information (PII), financial data, health records, intellectual property, and any other confidential information.

User Privacy: Denotes the entitlement of individuals to govern the collection, utilization, and dissemination of their personal data.

Data Security Risks: Encompasses any prospective threats or vulnerabilities capable of compromising the confidentiality, integrity, or availability of sensitive data.

Principles

Data Minimization: Advocate for the collection and retention of only the minimal requisite volume of sensitive data essential for legitimate business objectives.

Lawfulness, Fairness, and Transparency: Conduct the processing of sensitive data in a lawful, equitable, and transparent manner, ensuring individuals are duly informed regarding the methods of data collection, utilization, and sharing.

Purpose Limitation: Restrict the utilization of sensitive data solely to explicitly defined purposes and secure consent when mandated.

Data Accuracy: Uphold the accuracy and currency of sensitive data to preserve its reliability and pertinence.

Security Safeguards: Deploy appropriate technical and organizational measures to fortify sensitive data against unauthorized access, disclosure, tampering, or destruction.

Accountability and Governance: Entrust responsibility for data protection, privacy, and security to designated personnel and establish mechanisms for compliance oversight and enforcement.

User Rights: Respect the entitlements of individuals concerning their personal data, including the rights to access, rectify, erase, and port.

Incident Response and Notification: Execute swift responses to data breaches or security incidents, mitigate their repercussions, and promptly inform affected individuals and authorities as stipulated by pertinent laws and regulations.

Responsibilities

Management*:* Furnish leadership and allocate resources to support the enactment and enforcement of this policy.

Employees: Adhere rigorously to this policy, undergo training on data protection and security protocols, and promptly report any anomalies or infractions to designated authorities.

IT Department: Implement and sustain technical safeguards to secure sensitive data, including encryption, access controls, firewalls, and intrusion detection systems.

Legal and Compliance Team: Remain abreast of relevant legal statutes, regulations, and industry standards concerning data protection and privacy, and ensure organizational practices remain compliant.

Training and Awareness

Conduct regular training sessions for employees on data protection principles, privacy rights, security best practices, and the mandates of this policy. Foster a culture of heightened awareness and individual accountability concerning data protection and privacy matters across all stakeholders.

Compliance Monitoring and Review

Undertake periodic audits, assessments, and evaluations to gauge compliance with this policy, identify areas necessitating enhancement, and promptly address any shortcomings. Update the policy as warranted to reflect alterations in legal requirements, technological advancements, or organizational exigencies.

Enforcement

Transgressions against this policy may warrant disciplinary measures, including but not limited to termination of employment or contract, alongside legal repercussions in consonance with applicable laws and regulations.

Conclusion

By steadfastly adhering to this policy, Pennrose pledges to uphold the highest echelons of data protection, user privacy, and data security. We acknowledge the trust reposed in us by individuals entrusting us with their data and remain resolute in our commitment to preserving that trust through judicious stewardship of sensitive information.