Privacy & Data Handling Policy

Version 1.0

2023-11-01

HY TECH LLC
573 Bellevue Rd, STE D, Newark, DE 19713

This policy discloses the guiding principles for information stewardship and a framework for classifying and handling confidential information and applies to all employees of HY Tech LLC.

All employees are expected to responsibly manage, handle, and use information or data for instruction, research, service, and development. While such information or data may only be accessed from, or stored on a company-owned computer or device, this expectation of responsibility remains in force. This policy is intended to ensure the integrity, availability, and protection of information and data without impeding legitimate, authorized access to, and use of information and data.

I. Data Classification

Level 1: Public Data - Information intended for the public. Information at this level will not contain regulated or confidential information. For example, press releases, publications and information posted on open websites and social media. Publicly posted information must not pose any significant harm to the company.

Level 2: Internal Data - Information limited to distribution to members of the company community to support their work. For example, internal memos and emails, licensed software, company internal documents. Improper handling or unauthorized access of level 2 data will result in financial penalty and fines, loss of access to resources and violation of agreements.

Level 3: Regulated Data - Personally Identifiable Information (PII) and information protected by law, regulation, contract, binding agreement, or industry requirements. Information intended for very limited distribution on a need-to-know basis within the company. This includes but not limited to, Social security numbers, birth dates, bank information or any personal, financial or specific information that could be used to steal identity or financial resources, Healthcare information governed by HIPAA, Credit card information governed by PCI standards, Amazon customer data, Personnel files, Promotion files, Compensation data, Accounting files. Improper handling or unauthorized access of level 3 data may incur legal sanctions, financial fines and/or reputational loss and potential lawsuits.

Only authorized IP addresses and user accounts are allowed to access any company or Amazon data. Access controls of employee, software and physical devices to different levels of data are documented and mandatorily implemented. They will be reviewed and re-evaluated in the beginning of each quarter.

II. Access Management

A unique ID will be assigned to each person with computer access to Amazon information. No default, generic nor shared user accounts & credentials are allowed. At all times, only the required user accounts can access Amazon Information. In the beginning of each quarter, the list of people and services with access to Amazon Information will be reviewed. Inactive or disqualified accounts will be deleted. Anomalous usage patterns and continuing failed log-in attempts will result in an account suspension with access removed. Any data are not allowed to be stored on personal devices.

Developers must implement fine-grained access control mechanisms to allow granting rights to any party using the application and the application's operators following the principle of least privilege. Access of PII data and non-PII data must be separated. Application sections or features that vend PII must be protected under a unique access role, and access should be granted on a "need-to-know" basis.

III. Data Encryption and Storage

All data must be stored in the private NAS server provided by the company and can only be accessed from company-owned devices. No person devices, which includes but not limited to USB drives, personal laptops and cell phones, are allowed to access any data.

All Amazon data and information, including PII data, must be encrypted when they are persisted using AES-256 for all internal and external endpoints. HTTPS is mandated while transferring data in network. The cryptographic materials and cryptographic capabilities must be limited to access by only the Developer's processes and services.

All Amazon related data will only be live for 30 days and then archived. PII data must be permanently deleted after 30 days. Any printed documents containing PII must also be securely destroyed. For other Amazon data, they may be archived offline with AES-256 encryption in company owned NAS for up to 180 days.

IV. Data Sharing

We may use outside shipping companies such as Fedex, UPS and USPS to ship orders, and a credit card processing company to bill users for goods and services. These companies do not retain, share, store or use personally identifiable information for any secondary purposes beyond filling customer orders.

V. Logging and Monitoring

Logs on all channels must be preserved to detect any possible security-related issues. All logs must have access controls to prevent any unauthorized access and tampering throughout their lifecycle. Logs themselves must not contain PII and must be retained for at least 90 days for reference in the case of a Security Incident. Developers must build mechanisms to monitor the logs and all system activities to trigger investigative alarms on suspicious actions. Developers should perform investigation when monitoring alarms are triggered and act accordingly following the Incidence Response Plan.

VI. Security Updates and Patches

Updates and patches must be applied on a timely basis on company-owned computers and devices. Updates and patches designated as critical by the software vendor must be applied as soon as reasonably possible.

VII. Antivirus Protection

The company supports and maintains antivirus software for all company-owned devices. Employees must ensure they are using current antivirus protection software on personal devices that are used for business-related work.

VIII. Policy Violation

Employees who either intentionally or unintentionally violate this policy risk loss of access to some or all information resources and may be subject to other penalties and disciplinary action, both within and outside of the company.