Data Security and Protection Policy

Furniture Pros Logistics

1. Purpose

This company strives to maintain industry standards in data protection and secure coding design and principles. The company's goal is to minimize the potential theft and loss of sensitive records through the means of physical, digital, and administrative safe guards. This document will outline the methods and security integrity established by the company to demonstrate preventative measures against data breaches or the potential loss of data.

2. Scope

This policy will apply to all forms of data deemed sensitive by the company's Data Classification found in section 4. Additionally, all physical devices, servers, databases, and computer nodes connected to the company's network fall under this guideline. All users, employees, administrators interacting with this network are also subject to this policy.

Note: all public data will not fall under this policy.

3. Policy

1. General

a. Network Protection

1. All networks and computer nodes under the company are protected with network firewalls and network access lists to deny unauthorized user access.
2. All computer nodes on the company network include Bitdefender antivirus software.

b. Network Access

1. Each user is assigned a unique ID, along with an individual user account and password, which can be used to identify a user's actions over the network.
2. User access is granted based on the least privilege principle, which means the smallest amount of privilege is granted for a user's task to be completed.
3. User accounts are reviewed on a quarterly basis, which an inactive or no longer needed account will be terminated.
4. Accounts with abnormal activities will be monitored by the company's IT Department, which may lead to temporarily or permanently disabling that account if deemed necessary.

c. Account Creation and Password Requirements

1. All company user account passwords must maintain at least a minimum of 8 characters in length, contain at least one special character, contain both uppercase and lowercase letters, and contains at least one number.
2. All company user account passwords will be changed or rotated on a quarterly basis.

d. Data Transmission

1. All connections internal and external to the company network is encrypted with TLS, SFTP, IKE and Ipsec.
2. Untrusted hardware detected on a connection will be terminated.

e. Data Breach and Loss Response

1. Upon the detection of an unauthorized access and/or data corruption, the company will follow the procedure outlined in the following:
    - Within 24 hours of detecting Security Incident or suspecting that a Security Incident has occurred. Company will investigate each Security Incident, and document the incident description, remediation actions, and associated corrective process/system controls implemented to prevent future recurrence.
    - All evidences or records collected, and such documentation are available in secured server for top security clearance personal.
    - Any involved parties such as source of data, partners of the process will be notified within 24 hours of detecting Security Incident and can request a copy of the incident report (see page 5).

f. Right to Erasure

1. Upon request, the company will delete data held in company possession if proof of data ownership is provided. However, under some circumstances the company may be required to store the data if the data is required to comply with local or federal laws and regulations.
2. All data deletion processes will go through industry standard sanitization(*1) and all live instances of data will also be destroyed within a 30-day period after receiving a deletion request.
3. A certificate of sanitization (see page 6) will be generated for each data sanitization.

2. User Responsibilities

a. Inside Company Grounds

1. All users must lock their machines upon leaving their desk or work environment to prevent unauthorized access.
2. All users must not share accounts with other employees or administrators.
3. All users must keep their workplace clear of sensitive and confidential information upon leaving their desk or work environment.

b. Outside Company Grounds

1. All users must refrain from storing company related data information on personal devices.

3. Personal Identifiable Information Protection

a. PII Storage

1. All PII information after 30 days of receiving will be encrypted and transferred to a separate local repository on company grounds.

b. PII Governance

1. All data handling processes follow the guidelines found in (*1)
2. All physical devices and software containing PII should follow the above guidelines

c. Encryption at Rest

        1. All PII information are encrypted with AES 256 and stored in an offline backup device.
        2. All encryption materials, such as encryption and decryption keys and encryption processes are prohibited for unauthorized usage.
    d. Secure Coding
        1. All sensitive keys and credential information such as passwords are not to be hardcoded into production or development code or code repositories.
        2. All internal and external connections and events occurring to the company's software systems are logged and stored into a data repository indicating but not limited to: date and time of event, user id, log messages, access attempts, and system errors.
        3. Under the circumstance of when a threshold is surpassed, based on the log monitoring tools set by the company, IT personnel will follow guidelines set on (*1).

4. Testing
    a. Software Vulnerability Testing
        1. Every 180 days, tests are run to ensure the viability and secureness of all company software systems including employee hardware and software.
5. Reporting Requirements
    a. Weekly Reports
        1. Weekly reports are to be given in written form to the Head of IT Director. High priority incidents are expected to be communicated during the company's weekly IT meetings.

4. Data Classification

Data Classification Table			
	Confidential	Restricted	Public
Description	Data that is legally regulated and bound to company. Data that would provide access to highly confidential information.	Data that is deemed private by company and not released to the public.	Data that is publicly available and released by company.
Examples	Financial records, Customer PII Data, Authentication Data	Communication records, emails, documents with no confidential data, non-identifiable personal data	Public website content, press releases.
Reputation Risk	High	Medium	Low
Legal Requirements	Required by law	Required by Company	No Requirements
Bound to Data Protection Policy	Yes	Yes	No

5. Definitions

- “Company” means Furniture Pros Logistics and any subsidiaries owned by Furniture Pros Logistics.
- *1: NIST 800-88 document published by U.S. Department of Commerce, National Institute of Standards and Technology https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf