## Scope:

### Assets that will be assessed:

● On-premises equipment for in-office business needs

● Employee equipment: end-user devices (desktops/laptops, smartphones),

remote workstations, headsets, cables, keyboards, mice, docking stations,

surveillance cameras, etc.

● Storefront products available for retail sale on site and online; stored in the

company’s adjoining warehouse

● Management of systems, software, and services: accounting,

telecommunication, database, security, ecommerce, and inventory

management

● Internet access

● Internal network

● Data retention and storage

● Legacy system maintenance: end-of-life systems that require human

Monitoring

Users SPII & PII

### How audit will help organization and goals:

* Meet compliance requirements
* Reduce fines as much as possible
* Maintain assets

### How often audits should be performed:

Once a week.

## Risk Assessment:

### Employees access to PII and SPII

Can risk fines This information if confidential to the user. As it risks GDP, NIST CSF, PCI DSS, and SOC 1 & 2. High risk

### No use of Encryption

Protect PII and SPII as it risks GDP, NIST CSF, PCI DSS, and SOC 1 & 2. And is a standard security control. high risk.

### Lack of controls used:

Violates SOC 1 & 2. At minimum Encryption, Authentication, Biometrics, Authorisation, Physical, technical and administrative should be used to comply . Medium risk.

### Lack of IDS:

Implement an SIEM such as SPLUNK or Google Chronical to detect and get rid of intrusions. Will also be useful to notify customers of breach within 72 hours. Also does not comply with NIST RMF detect. medium risk.

### Lack of recovery

Does not comply with NIST RMF Recover. Recommended to use the 1, 2, 3 method of redundancy. Medium risk.

### Lack of strong passwords

Does not comply with NIST CSF. Make employees and users follow stronger password guidelines. High risk.

### Security with deprecated systems.

Have an audit completed every week, that has made sure the CIA triad is met with these older systems. Medium risk.

### Mitigation plan.

Start by following security controls to ensure Encryption, Authentication, Biometrics, Authorization, Physical controls, and Administrative controls. Administrative controls are of utmost priority right now because employees have access to all SPII and PII which does not comply with SOC. Add a new policy by having users change their passwords once every two weeks, that meet certain requirements that are stronger than the current requirements. An IDS and SIEM need to be added such as logs, and need to be added to detect intrusions. Check on old systems and make sure they comply with the CIA triad, an audit for this should be done every week. And lastly add the 1, 2, 3 method of redundancy to keep information once a disaster occurs.

**Security law checklist if audit is not met.**

**If this audit is followed, then there will be no fines or laws broken.**

| **Yes** | **No** | **Control** |
| --- | --- | --- |
|  |  | Least Privilege |
|  |  | Disaster recovery plans |
|  |  | Password policies |
|  |  | Separation of duties |
|  |  | Firewall |
|  |  | Intrusion detection system (IDS) |
|  |  | Backups |
|  |  | Antivirus software |
|  |  | Manual monitoring, maintenance, and intervention for legacy systems |
|  |  | Encryption |
|  |  | Password management system |
|  |  | Locks (offices, storefront, warehouse) |
|  |  | Closed-circuit television (CCTV) surveillance |
|  |  | Fire detection/prevention (fire alarm, sprinkler system, etc.) |

**Compliance checklist**

Payment Card Industry Data Security Standard (PCI DSS)

| **Yes** | **No** | **Best practice** |
| --- | --- | --- |
|  |  | Only authorized users have access to customers’ credit card information. |
|  |  | Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment. |
|  |  | Implement data encryption procedures to better secure credit card transaction touchpoints and data. |
|  |  | Adopt secure password management policies. |

General Data Protection Regulation (GDPR)

| **Yes** | **No** | **Best practice** |
| --- | --- | --- |
|  |  | E.U. customers’ data is kept private/secured. |
|  |  | There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach. |
|  |  | Ensure data is properly classified and inventoried. |
|  |  | Enforce privacy policies, procedures, and processes to properly document and maintain data. |

System and Organizations Controls (SOC type 1, SOC type 2)

| **Yes** | **No** | **Best practice** |
| --- | --- | --- |
|  |  | User access policies are established. |
|  |  | Sensitive data (PII/SPII) is confidential/private. |
|  |  | Data integrity ensures the data is consistent, complete, accurate, and has been validated. |
|  |  | Data is available to individuals authorized to access it. |

**3/10 rating**