

12.1 Information Security Policy

COMPANY's information security policy consist of all the policies and procedures list in this manual along with our employee handbook and the below employee security policy.

Introduction

Storage of confidential or consumer protected data information on computers and transferred across the network eases use and expands functionality. Commensurate with that expansion is the need for the appropriate security measures. Security is not distinct from the functionality. The Information Security Policy (ISP) recognizes that not all departments within **COMPANY** are the same and that restricted or confidential data is used differently by various departments. The policy is intended to limit or restrict access to this data by the need to know and business purpose reason. These policies apply to all departments within **COMPANY**. Each department within **COMPANY** should apply this policy. The ISP is written to incorporate current technological advances. The technology installed in some departments may limit immediate compliance with the ISP. Instances of non-compliance **must** be reviewed and approved by the **COMPANY**. Throughout the document, the term **must** and *should* are used carefully. "**musts**" are not negotiable; "shoulds" are goals for the **COMPANY**. The terms *data* and *information* are used interchangeably in the document. The terms *system* and *network* administrator are used in this document. These terms are generic and pertain to any person who performs those duties, not just those with that title or primary job duty. Many employees, managers, contract employees and staff members are the system administrators for their own machines.

NOTE: the Policies highlight areas that **COMPANY** expect employee's to ensure they are following for security of data. Employees are still required to refer to and follow the actual polices and procedures in the company manual.

Purpose of this Policy

By information security, we mean protection of the **COMPANY** Restricted or Confidential data, consumer data any data deemed confidential by the **COMPANY** both electronic and hard copy. This includes the storage, authorized access, alteration, or destruction of any **COMPANY** data.

The purpose of the information security policy is:

- To establish a **COMPANY**-wide approach to PCI / restricted or confidential information security and protect both consumer and company data.
- To prescribe mechanisms that help identify and prevent the compromise of information security and the misuse of restricted or confidential, company or consumer data.
- To define mechanisms that protects the reputation of **COMPANY** and allows **COMPANY** to satisfy its legal and ethical responsibilities with regard to PCI Compliancy and other state and federal laws and regulations.

- To prescribe an effective mechanism for responding to external complaints and queries about real or perceived non-compliance with this policy.

Responsibility

The **COMPANY** is responsible for implementing the policy.

- The information security policy is updated on a regular basis or at a minimum of once a year and published as appropriate.
- Appropriate training and guidance will be provided to all system administrators, and users. The **COMPANY** will determine and establish who is specifically responsible for providing training and guidance.
- Each Directorate involved in restricted or confidential processing or data collection will appoint a person to be responsible for security implementation, incident response, periodic user access reviews, and education of information security policies including, but not limited to, information about virus infection risks, lack of control of data and industry awareness education.

General Policy

Required Policies

- **COMPANY** will use a layered approach of overlapping controls, monitoring and authentication to ensure overall security of **COMPANY**'s data, network and system resources.
- Security reviews of servers, firewalls, routers and monitoring platforms, employee access and storage of data **must** be conducted on a regular basis. These reviews **MUST** include monitoring access logs, user access, storage and results of intrusion detection software that has been installed.

Recommended Practices

- Vulnerability and risk assessment tests of user access, access logs, visitor logs, storage compliancy and external network connections **must** be conducted on a regular basis. At a minimum, testing should be performed weekly, but the sensitivity of the information secured may require that these tests be done more often.
- Education should be implemented to ensure that users understand data sensitivity issues, levels of confidentiality, and the mechanisms to protect the data. This should be tailored to the role of the individual. Responsibility of education lies with the person/entity designated by the **COMPANY**.
- Violation of the Information Security Policy may result in disciplinary actions as authorized by **COMPANY** in accordance with **COMPANY** disciplinary policies, procedures, and codes of conduct.

Data Classification Policy

It is essential that all **COMPANY** restricted or confidential and confidential data be protected. All restricted or confidential and confidential data is considered classified and should only be accessed by personnel that have a business purpose and a clearance or manager approval. We have specified three classes below:

Confidential - Information assets for which there are legal requirements for preventing disclosure or financial penalties for disclosure. Data covered by federal and state legislation, such as FERPA, HIPAA, PCI or the Data Protection Act, are in this class. Payroll, personnel, and financial information are also in this class because of privacy requirements. This policy recognizes that other data may need to be treated as high risk because it would cause severe damage to the **COMPANY** if disclosed or modified. It is the data owner's responsibility to implement the necessary security requirements.

Restricted - Data that would not expose **COMPANY** to loss if disclosed, but that the data owner or **COMPANY** feels should be protected to prevent unauthorized disclosure.

Public - Information that may be freely disseminated.

All information resources should be categorized and protected according to the requirements set for each classification. The data classification and its corresponding level of protection should be consistent when the data is replicated and as it flows through **COMPANY**.

- All restricted or confidential information is high risk and classified, and should always be protected.
- No **COMPANY**-owned system or network subnet can have a connection to the Internet without the means to protect the information on those systems consistent with its confidentiality classification.
- All employees are responsible for following all data repositories and data transfer procedures, which protect restricted or confidential data in the appropriate manner.
- High risk data **must** be encrypted during transmission over secure channels.
- Confidential data should be encrypted during transmission over secure channels.
- All appropriate data should be backed up, and the backups tested periodically as part of a documented, regular process.
- Backups of data **must** be handled with the same security precautions as the data itself. When systems are disposed of or repurposed, data **must** be certified deleted or disks destroyed consistent with industry best practices for the security level of the data. All paper copies of restricted or confidential data **must** be shredded once the business use is completed.
- All hard copies of restricted or confidential transactions **must** be destroyed (shredded) following the restricted or confidential retention policy.

Access Control Policy

- Data **must** have sufficient granularity to allow the appropriate authorized access. There is a delicate balance between protecting the data and permitting access to those who need to use the data for authorized purposes.
- Where possible and financially feasible, more than one person **must** have full rights to any **COMPANY** restricted or confidential data.
- Starting with the cashier or customer service representative at a **COMPANY** store location, access and control of restricted or confidential data **must** be maintained.
- If at any time offline sales occur, the **COMPANY** must be the operative that re-enters the information into the system. This is not to be done at store level.

Virus Prevention Policy

- The willful introduction of computer viruses or disruptive/destructive programs into the **COMPANY** environment is prohibited, and violators will be subject to **COMPANY** disciplinary process.
- All desktop systems that connect to the network **must** be protected with an approved licensed anti-virus software product that it is kept updated according to the **COMPANY** policy.
- All servers and workstations that connect to the network and that are vulnerable to virus or worm attack, **must** be protected with an approved licensed anti-virus software product that it is kept updated.
- Headers of all incoming data including electronic mail, **must** be scanned for viruses by the email server.
- Administrators should inform users when a virus has been detected.
- Virus-scanning logs **must** be maintained whenever email is centrally scanned for viruses.

Intrusion Detection Policy

- Intruder detection **must** be implemented on all servers and workstations containing data classified as “high risk.”
- Operating system and application software logging processes **must** be enabled on all host and server systems. Where possible, alarm and alert functions, as well as logging and monitoring systems **must** be enabled.
- Server, firewall, and critical system logs **must** be reviewed daily.

Internet Security Policy

- All connections to the Internet **must** go through a properly secured connection point and the employee **must** have management approval.

Acceptable Use Policy

- COMPANY computer resources **must** be used in a manner that complies with COMPANY policies and State and Federal laws and regulations. It is against COMPANY policy to install or run software requiring a license on any COMPANY computer without a valid license.
- Use of the COMPANY's computing and networking infrastructure by COMPANY employees unrelated to their COMPANY positions, **must** be limited in both time and resources, and **must** not interfere in any way with COMPANY functions or the employee's duties. It is the responsibility of each employee to consult their supervisor if they have any questions in this respect.
- Uses that interfere with the proper functioning or the ability of others to make use of the COMPANY's networks, computer systems, applications, and data resources are not permitted.
- Use of COMPANY computer resources for personal profit is not permitted except as addressed under other COMPANY policies.
- Decryption of passwords is not permitted except by authorized staff performing security reviews or investigations. Use of network sniffers shall be restricted to system administrators who **must** use such tools to solve network problems. Auditors or security officers in the performance of their duties may also use them. They **must not** be used to monitor or track any individual's network activity except under special authorization as defined by COMPANY policy that protects the privacy of information in electronic form.

Information Security Policy

I (Employee Name) _____ have received, read, and acknowledge all the policies of the **COMPANY** employee security policy outlined above. I fully understand the policy and acknowledge that disciplinary action can be taken up termination (per the **COMPANY** employee manual) if I don't follow these policies to the letter of the law.

Employee signature: _____

Date: _____

Manager's signature: _____

Date: _____