Information Security Policy

Contents

I. Policy

It is the policy of 365 RETAIL MARKETS that information, as defined hereinafter, in all its forms--written, spoken, recorded electronically or printed--will be protected from accidental or intentional unauthorized modification, destruction or disclosure throughout its life cycle. This protection includes an appropriate level of security over the equipment and software used to process, store, and transmit that information.

All policies and procedures must be documented and made available to individuals responsible for their implementation and compliance. All activities identified by the policies and procedures must also be documented. All the documentation, which may be in electronic form, must be retained for at least 5 (five) years after initial creation, or, pertaining to policies and procedures, after changes are made, unless otherwise required by law. All documentation must be periodically reviewed for appropriateness and currency, a period to be determined by each entity within 365 RETAIL MARKETS.

At each entity and/or department level, additional policies, standards, and procedures will be developed detailing the implementation of this policy and addressing any additional information systems in such entity and/or department. All departmental policies must be consistent with this policy. All systems implemented after the effective date of these policies are expected to comply with the provisions of this policy where possible. Existing systems are expected to be brought into compliance where possible and as soon as practical.

II. Scope

The scope of information security includes the protection of the confidentiality, integrity and availability of information.

The framework for managing information security in this policy applies to all 365 RETAIL MARKETS entities, subsidiaries, employees, contractors, and other involved persons, and all involved systems throughout 365 RETAIL MARKETS.

This policy and all standards apply to all protected health information and other classes of protected information in any form as defined below in INFORMATION CLASSIFICATION.

III. Information Security Responsibilities

Information Security Team: The Information Security Team (IST), either centrally coordinated across 365 Platforms or for each entity, is responsible for working with user management, owners, custodians, and users to develop and implement prudent security policies, procedures, and controls, subject to the approval of 365 RETAIL MARKETS. Specific responsibilities include:

1. Ensuring security policies, procedures, and standards are in place and adhered to by entity.
2. Providing basic security support for all systems and users.
3. Advising owners in the identification and classification of computer resources. See Section INFORMATION CLASSIFICATION.
4. Advising systems development and application owners in the implementation of security controls for information on systems, from the point of system design, through testing and production implementation.
5. Educating custodian and user management with comprehensive information about security controls affecting system users and application systems.
6. Providing on-going employee security education.
7. Performing security audits.
8. Reporting regularly to the 365 RETAIL MARKETS Management Team on entity's status with regards to information security.
9. Ensuring entities are in compliance with applicable national, federal and state laws, including, but not limited to GDPR, CCPA, CPRA, FCRA, HIPAA, BIPA, GLBA, ETC.

Information Owner: The owner of a collection of information is usually the manager responsible for the creation of that information or the primary user of that information. This role often corresponds with the management of an organizational unit. In this context, ownership does not signify proprietary interest, and ownership may be shared. The owner of information has the responsibility for:

1. Knowing the information for which she/he is responsible.
2. Determining a data retention period for the information, relying on advice from legal counsel.
3. Ensuring appropriate procedures are in effect to protect the integrity, confidentiality, and availability of the information used or created within the unit.
4. Authorizing access and assigning custodianship.
5. Specifying controls and communicating the control requirements to the custodian and users of the information.
6. Reporting promptly to the IST the loss or misuse of 365 RETAIL MARKETS information.
7. Initiating corrective actions when problems are identified.
8. Promoting employee education and awareness by utilizing programs approved by the IST, where appropriate.
9. Following existing approval processes within the respective organizational unit for the selection, budgeting, purchase, and implementation of any computer system/software to manage information.

Custodian: The custodian of information is generally responsible for the processing and storage of the information. The custodian is responsible for the administration of controls as specified by the owner. Responsibilities may include:

1. Providing and/or recommending physical safeguards.
2. Providing and/or recommending procedural safeguards.
3. Administering access to information.
4. Releasing information as authorized by the Information Owner and/or the Information Privacy/ Security Team for use and disclosure using procedures that protect the privacy of the information.
5. Evaluating the cost effectiveness of controls.
6. Maintaining information security policies, procedures and standards as appropriate and in consultation with the IST.
7. Promoting employee education and awareness by utilizing programs approved by the IST, where appropriate.
8. Reporting promptly to the IST the loss or misuse of 365 RETAIL MARKETS information.
9. Identifying and responding to security incidents and initiating appropriate actions when problems are identified.

User Management: 365 RETAIL MARKETS management who supervise users as defined below. User management is responsible for overseeing their employees' use of information, including:

1. Reviewing and approving all requests for their employee’s access authorizations.
2. Initiating security change requests to keep employees' security record current with their positions and job functions.
3. Promptly informing appropriate parties of employee terminations and transfers, in accordance with local entity termination procedures.
4. Revoking physical access to terminated employees, i.e., confiscating keys, deactivating door codes, etc.
5. Providing employees with the opportunity for training needed to properly use the computer systems.

6. Reporting promptly to the IST the loss or misuse of 365 RETAIL MARKETS information.
7. Initiating corrective actions when problems are identified.
8. Following existing approval processes within their respective organization for the selection, budgeting, purchase, and implementation of any computer system/software to manage information.

User: The user is any person who has been authorized to read, enter, or update information. A user of information is expected to:

1. Access information only in support of their authorized job responsibilities.
2. Comply with Information Security Policies and standards and with all controls established by the owner and custodian.
3. Refer all disclosures of Information (1) outside of 365 RETAIL MARKETS and (2) within 365 RETAIL MARKETS, other than for payment, to the applicable entity's Department. In certain circumstances, the Department policies may specifically delegate the disclosure process to other departments.
4. Keep personal authentication devices (e.g. passwords, PINs, etc.) confidential.
5. Report promptly to the IST the loss or misuse of 365 RETAIL MARKETS information.
6. Initiate corrective actions when problems are identified.

IV. Information Classifications

Classification is used to promote proper controls for safeguarding the confidentiality of information. Regardless of classification the integrity and accuracy of all classifications of information must be protected. The classification assigned and the related controls applied are dependent on the sensitivity of the information. Information must be classified according to the most sensitive detail it includes. Information recorded in several formats (e.g., source document, electronic record, report) must have the same classification regardless of format. The following levels are to be used when classifying information:

A. Protected Health Information (PHI)

PHI is information, whether oral or recorded in any form or medium, that:

1. is created or received by a healthcare provider, health plan, public health authority, employer, life insurer, school or university or health clearinghouse; and
2. relates to past, present or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past present or future payment for the provision of health care to an individual; and
3. includes demographic data, that permits identification of the individual or could reasonably be used to identify the individual.

Unauthorized or improper disclosure, modification, or destruction of this information could violate state and federal laws, result in civil and criminal penalties, and cause serious damage to 365 RETAIL MARKETS and its patients or research interests.

B. Personally Identifiable Information (PII)

PII is information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or

household. Examples of PII are real name, alias, postal address, unique personal identifier, online identifier, IP address, email address, account name, social security number, driver's license number, passport number, or other similar identifies. Additional examples of PII are:

- Characteristics of protected classifications
- Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies
- Biometric information
- Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an internet website, application, or advertisement.
- Geolocation data.
- Audio, electronic, visual, thermal, olfactory, or similar information
- Professional or employment-related information.
- Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act
- Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes

C. PCI

PCI information applies to all entities that store, process or transmit payment cardholder data (CHD) and/or sensitive authentication data (SAD) as defined by the Payment Card Industry.

D. Confidential Information (CI)

Confidential Information is very important and highly sensitive material that is not classified as PHI, PII or PCI. This information is private or otherwise sensitive in nature and must be restricted to those with a legitimate business need for access. Examples of CONFIDENTIAL INFORMATION may include: key financial information, proprietary information of commercial research sponsors, system access passwords and information file encryption keys.

Unauthorized disclosure of this **PHI, PII, PCI** or **CI** to people without a business need for access may violate laws and regulations, or may cause significant problems for 365 RETAIL MARKETS, its customers, or its business partners. Decisions about the provision of access to this information must always be cleared through the Information Owner.

E. Internal Information

Internal Information is intended for unrestricted use within 365 RETAIL MARKETS, and in some cases within affiliated organizations such as 365 RETAIL MARKETS business partners. This type of information is already widely-distributed within 365 RETAIL MARKETS, or it could be so distributed within the organization without advance permission from the information owner.

Examples of Internal Information may include: personnel directories, internal policies and procedures, most internal electronic mail messages.

Any information not explicitly classified as PHI, PII, PCI, CI or Public will, by default, be classified as Internal Information.

Unauthorized disclosure of this information to outsiders may not be appropriate due to legal or contractual provisions.

F. Public Information

Public Information has been specifically approved for public release by a designated authority within each entity of 365 RETAIL MARKETS. Examples of Public Information may include marketing brochures and material posted to 365 RETAIL MARKETS entity internet web pages.

This information may be disclosed outside of 365 RETAIL MARKETS.

V. Risk Management

A thorough analysis of all 365 RETAIL MARKETS information networks and systems must be conducted on a periodic basis to document the threats and vulnerabilities to stored and transmitted information. The analysis examines the types of threats – internal or external, natural or manmade, electronic and non-electronic- that affect the ability to manage the information resource. The analysis also documents the existing vulnerabilities within each entity which potentially expose the information resource to the threats. Finally, the analysis also includes an evaluation of the information assets and the technology associated with its collection, storage, dissemination, and protection

From the combination of threats, vulnerabilities, and asset values, an estimate of the risks to the confidentiality, integrity and availability of the information will be determined. The frequency of the risk analysis will be determined at the entity level.

A. Existing Systems

Systems involved in storing, processing, or transmitting information as defined in INFORMATION CLASSIFICATION are subject to regular risk assessments by a qualified third party (QSA) or member of the IST on the following schedule:

ASV Scans – Quarterly

Pen Test – Yearly

Vendor Risk Rating Service - At the time of onboarding new vendor

External Vulnerability Scans - Quarterly

Internal Vulnerability Scans - Quarterly

A risk rating will be assigned to any vulnerabilities discovered as part of the risk assessment following the CVSS and other factors as determined by the QSA.

Risk	Explanation
Critical	A vulnerability exists on a target host that can lead to the complete compromise of the system or limited compromise of critical data.
High	A vulnerability was confirmed on a target host that led to a partial compromise of systems or data.

Medium	An information disclosure vulnerability was found that could assist in further exploitation attempts or a vulnerability that under precise conditions is known to be exploitable.
Low	A minimal information disclosure vulnerability exists or a vulnerability that has no known proof of concept making this extremely difficult to successfully exploit.
Best Practice	A common flaw or misconfiguration exists that should be remediated to adhere to community best practices.

Risks identified as part of an AVS scan or pen test will be reviewed as part of the CHANGE MANAGEMENT process and ultimately run through the SDLC for remediation

In addition, existing systems may be in scope for additional audit controls as defined by their INFORMATION CLASSIFICATION.

B. New Systems

Newly developed or *changed* systems will be evaluated as part of the CHANGE MANAGEMENT process and categorized based on the INFORMATION CLASSIFICATION. Upon approval by the CAB, the proposed change will be converted to an Epic, which will be subject to the relevant guidelines as outlined in this document and defined by the INFORMATIN CLASSIFICATION of the Epic.

C. Annual Risk Assessment

The annual risk assessment is initiated by the IST and is based on 365's security baseline. The baseline contains the controls all 365 Platforms and entities are expected to have in place. The controls are compiled from established industry standards like PCI DSS, SOC2, NIST CSF, ISO-27001, and related frameworks. A risk register is also maintained that calculates the probability and the likelihood of the risk. Additionally, risks may be compiled from vulnerability scans.

VI. Computer and Information Control

All involved systems and information are assets of 365 RETAIL MARKETS and are expected to be protected from misuse, unauthorized manipulation, and destruction. These protection measures may be physical and/or software based.

A. Ownership of Software

All computer software developed by 365 RETAIL MARKETS employees or contract personnel on behalf of 365 RETAIL MARKETS or licensed for 365 RETAIL MARKETS use is the property of 365 RETAIL MARKETS and must not be copied for use at home or any other location, unless otherwise specified by the license agreement.

B. Installed Software

All software packages that reside on computers and networks within 365 RETAIL MARKETS must comply with applicable licensing agreements and restrictions and must comply with 365 RETAIL MARKETS acquisition of software policies.

C. Patch Management

All systems storing Information are to receive regular security patches as recommended by the manufacturer or comparable industry standards.

D. Malware Protection

Virus/malware checking systems approved by the IST must be deployed using a multi-layered approach (POS, desktops, servers, gateways, etc.) that ensures all electronic files are appropriately scanned for malware. Users are not authorized to turn off or disable malware checking systems. Malware definitions are to be auto updated on a scheduled deemed appropriate by the IST for the target system.

E. Access Controls

Physical and electronic access to PHI, PII, PCI, CI and Internal information and computing resources is controlled. To ensure appropriate levels of access by internal workers, a variety of security measures will be instituted as recommended by the Information Security Team and approved by 365 RETAIL MARKETS. Mechanisms to control access to PHI, PII, PCI, CI and Internal information include (but are not limited to) the following methods:

1. Authorization

Access will be granted on a "need to know" basis and must be authorized by the immediate supervisor and application owner with the assistance of the IST. Any of the following methods are acceptable for providing access under this policy:

1. Context-based access: Access control based on the context of a transaction (as opposed to being based on attributes of the initiator or target). The "external" factors might include time of day, location of the user, strength of user authentication, etc.
2. Role-based access: An alternative to traditional access control models (e.g., discretionary, or non-discretionary access control policies) that permits the specification and enforcement of enterprise-specific security policies in a way that maps more naturally to an organization's structure and business activities. Each user is assigned to one or more predefined roles, each of which has been assigned the various privileges needed to perform that role.
3. User-based access: A security mechanism used to grant users of a system access based upon the identity of the user.

2. Identification/Authentication

Unique user identification (user id) and authentication is required for all systems that maintain or access PHI, PII, PCI, CI and Internal Information. Users will be held accountable for all actions performed on the system with their user id.

At least one of the following authentication methods must be implemented:

1. strictly controlled passwords
2. biometric identification, and/or
3. tokens in conjunction with a PIN.

The user must secure his/her authentication control (e.g. password, token) such that it is known only to that user and possibly a designated security manager.

An automatic timeout re-authentication must be required after a certain period of no activity (maximum 15 minutes when technically feasible).

The user must log off or secure the system when leaving it.

Multi Factor Authentication: Whenever technically feasible, MFA is to be enabled for any user or system that stores or processes Information. MFA is a method of confirming users' claimed identities by using a combination of two different factors: 1) something they know, 2) something they have, or 3) something they are. As part of PERIODIC POLICY REVIEW, systems should be evaluated if MFA can be enabled.

Location Based Restrictions: Whenever technically feasible, access to systems that store, or process Information should be restricted to known IP addresses as whitelisted by the IST. If this is problematic for remote employees utilize the 365 VPN or see section REMOTE EMPLOYEE POLICY. As part of SYSTEMS AUDIT, systems should be evaluated if Location Based Restrictions can be enabled.

SSO (Single Sign on): Whenever technically feasible, SSO is to be enabled across the applications used by the enterprise. SSO is a secure way of logging into the application that use SAML (Security Assertion Markup Language) protocol**.**

3. Password Policy

Our password policy must be enforced for both internally developed and third-party systems used by 365 RETAIL MARKETS.

- Minimum Password Length: 9
- Require Symbols: true
- Require Numbers: true
- Require Uppercase Characters: true
- Require Lowercase Characters: true
- Expire Passwords: true
- Max Password Age: 90
- Password Reuse Prevention: 7 (changed password cannot be the same as the previous 7 passwords)
- Failed password attempt lockout: 5

4. Expiration

System audits are to be completed quarterly to ensure terminated users no longer have access to date. Additionally, accounts with longer than 90 days of inactivity will be disabled.

F. Remote Access Tool Policy

Remote access tools that provide access to systems that process or store PHI, PII, PCI or CI require special consideration. These tools are incredibly powerful and are often targeted by those with malicious intent. Therefore 365 Remote Tool Policy is strictly enforced to adhere to:

1. A least privileged model for Authorization
2. Mandatory MFA for Authentication

3. Mandatory Location Based Restrictions based on approved whitelisted IP address(s)
4. Mandatory logging and account auditing
5. Mandatory automatic timeout re-authentication

G. Data Integrity

365 RETAIL MARKETS must be able to provide corroboration that PHI, PII, PCI, CI and Internal Information has not been altered or destroyed in an unauthorized manner. Listed below are some methods that support data integrity:

1. Transaction audit
2. Disk redundancy (RAID)
3. ECC (Error Correcting Memory)
4. Checksums (file integrity)
5. Encryption of data in storage
6. Digital signatures

H. Transmission Security

Technical security mechanisms must be put in place to guard against unauthorized access to data that is transmitted over a communications network, including wireless networks. The following features must be implemented:

1. Integrity controls
2. Encryption

I. Physical Access

Access to areas in which Information processing is carried out must be restricted to only appropriately authorized individuals. The following physical controls must be in place:

Computer systems must be installed in an access-controlled area. The area in and around the computer facility must afford protection against fire, water damage, and other environmental hazards such as power outages and extreme temperature situations. The access-controlled area must also secure against theft, destruction, or access by unauthorized individuals.

Workstations or personal computers (PC) must be secured against use by unauthorized individuals. Local procedures and standards must be developed on secure and appropriate workstation use and physical safeguards which must include procedures that will:

1. Position workstations to minimize unauthorized viewing of Information.
2. Grant workstation access only to those who need it to perform their job function.
3. Establish workstation location criteria to eliminate or minimize the possibility of unauthorized access to Information.
4. Employ physical safeguards as determined by risk analysis, such as locating workstations in controlled access areas or installing covers or enclosures to preclude passerby access to Information.
5. Auto-logout workstations with passwords to protect unattended machines, enforced by group policy.

1. Building Security

Offices, warehouses, buildings, and related structures in which information is stored or processed must be secured from unauthorized physical access. Employees must uniquely identify themselves prior to entering a building through manual or electronic systems. Building visitors must sign in and out through approved systems. Employee and visitor logs must be maintained for at least 1 year or longer as defined by related policies. Visitor logs must be periodically reviewed by IT.

J. Equipment and Media Controls

The disposal of information must ensure the continued protection of PHI, PII, PCI, CI and Internal Information. Each entity must develop and implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain information into and out of a facility, and the movement of these items within the facility. The following specification must be addressed:

Information Disposal / Media Re-Use of:

- Hard copy (paper and microfilm/fiche)
- Magnetic media (floppy disks, hard drives, zip disks, etc.) and
- CD ROM Disks

Accountability: Each entity must maintain a record of the movements of hardware and electronic media and any person responsible, therefore.

Data backup and Storage: When needed, create a retrievable, exact copy of electronic PHI before movement of equipment.

K. Removable Media

By policy, PHI, PII, PCI and CI should never be stored on removable media. If an exception to this policy is explicitly granted to an entity by the IST, the rules below must be followed:

1. A clear purpose must be defined as why Information must be stored on removable media.
2. Each entity must maintain a record of the movements of removable and any person responsible, therefore.
3. Upon completion of *clear purpose* in step 1, the Information is to be deleted from the removable media.
4. When needed, create a retrievable, exact copy of electronic Information before movement of equipment.
5. Other practices as defined by the IST.

L. POS/Workstation Decommission and Reuse Policy

Workstations, POS or otherwise, that have stored or processed PHI, PII, PCI or CI are subject to 365's IT Asset End of Life Policy. If the workstation is to be decommissioned, the disk drive is to be wiped and physically destroyed. If the workstation is to be reused, the disk drive is to be wiped, reformatted and a clean OS installed. Reformatting the drive alone is not enough.

M. Other Media Controls

Mobile Computing Devices: PHI, PII, PCI or CI must never be stored on mobile computing devices (laptops, smart phones, tablet, etc.) unless the devices have the following minimum-security requirements implemented:

1. Power-on passwords
2. Auto logoff or screen saver with password
3. Encryption of stored data or other acceptable safeguards approved by Information Security Team.

Further, mobile computing devices must never be left unattended in unsecured areas.

If PHI, PII, PCI or CI is stored on external medium or mobile computing devices and there is a breach of confidentiality as a result, then the owner of the medium/device will be held personally accountable and is subject to the terms and conditions of 365 RETAIL MARKETS Information Security Policies and Confidentiality Statement signed as a condition of employment or affiliation with 365 RETAIL MARKETS.

Data Transferring and Printing: Downloading and uploading PHI, PII, PCI, CI and Internal Information between systems must be strictly controlled. Requests for mass downloads of, or individual requests for, Information for research purposes that include PHI, PII, PCI or CI must be approved through the IST. All other mass downloads of information must be approved by the Application Owner and include only the minimum amount of information necessary to fulfill the request.

Oral Communications: 365 RETAIL MARKETS staff should be aware of their surroundings when discussing PHI, PII, PCI and CI. This includes the use of cellular telephones in public areas. 365 RETAIL MARKETS staff should not discuss PHI, PII, PCI and CI in public areas if the information can be overheard. Caution should be used when conducting conversations in: semi-private rooms, waiting rooms, corridors, elevators, stairwells, cafeterias, restaurants, or on public transportation.

N. Training and Awareness

The Information Security department must provide training and awareness material to all the associates on regular intervals, at least quarterly. The training and awareness should entail practical simulation using the security awareness tool. National Cyber Security Awareness month should also be organized which should compose of multiple activities that will generate more user awareness.

VII. Network Security Policy

All networked systems that store or process PHI, PII, PCI, CI and Internal Information are subject to the Network Security Policy.

Firewall: Systems will be protected by a firewall, separating untrusted external networks from trusted internal networks. The firewall rules should be configured to control and/or limit network traffic into and out of the any environments that handle PHI, PII, PCI, CI and Internal

Information. Furthermore, inbound, and outbound traffic should be restricted to that which is necessary for the system to function properly.

Network Segmentation: Systems that store or process PHI, PII, PCI, CI or Internal Information shall be separated from other systems through network segmentation. Even on a trusted internal network, network segmentation should separate systems that do not have an approved business need to be on the same network.

Intrusion Detection System/Intrusion Protection System: All centralized systems that store or process PHI, PII, PCI, CI or Internal Information shall be protected by an IDS/IPS, accompanied by centralized logging and alerting.

Disable Unnecessary Services: Only necessary services and protocols are to be enabled on networked devices. All unnecessary functionalities such as scripts, drivers, features, subsystems, file systems, ETC are to be disabled.

Patching: Network devices such as firewalls and switches are subject to 365's Patching Policy.

Internet Access: Internet browsing and accessing email from centralized systems that store or process PHI, PII, PCI or CI is prohibited.

Wireless Network: Wireless networks transmitting PHI, PII, PCI, CI or Internal Information are to use industry best practices to implement strong encryption for authentication and transmissions. Weak encryption (WEP, SSL) is strictly prohibited.

Unauthorized Devices: Devices connecting to a network transmitting PHI, PII, PCI or CI will be strictly controlled. This includes third-party systems and software sharing a POS/CHD network. Unauthorized devices found to be in violation of this policy will have their network access revoked. Explicit approval must be granted in writing for all third-party systems sharing the POS/CHD network and included in a yearly PCI-DSS audit.

VIII. Communication Policy

When using company resources to access and use the Internet, users must realize they represent the company. Whenever employees state an affiliation to the company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the company". Questions may be addressed to the IT Department.

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone, or paging, whether through language, frequency, or size of messages
3. Unauthorized use, or forging, of email header information. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

6. Use of unsolicited email originating from within 365 Retail Market's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by 365 Retail Markets or connected via 365's network. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam). PAN information will never be shared across end-user messaging technologies, or in any other manner unless explicitly authorized by 365 Retail Market InfoSec and IT.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).
8. PAN information will never be shared across end-user messaging technologies, or in any other manner unless explicitly authorized by 365 Retail Market's InfoSec and IT
9. Forwarding or auto-forwarding communications to personal email accounts is strictly prohibited.

IX. Clean Desk Policy

1. Employees are required to ensure that all sensitive/confidential information in hardcopy or electronic form is secure in their work area at the end of the day and when they are expected to be gone for an extended period.
2. Computer workstations must be locked when workspace is unoccupied.
3. Computer workstations must be shut completely down at the end of the workday.
4. File cabinets containing Restricted or Sensitive information must be kept closed and locked when not in use or when not attended.
5. Keys used for access to Restricted or Sensitive information must not be left at an unattended desk.
6. Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.
7. Printouts containing Restricted or Sensitive information should be immediately removed from the printer.
8. Upon disposal Restricted and/or Sensitive documents should be shredded in the official shredder bins or placed in the lock confidential disposal bins.
9. Whiteboards containing Restricted and/or Sensitive information should be erased.
10. Lock away portable computing devices such as laptops and tablets.
11. Treat mass storage devices such as CDROM, DVD or USB drives as sensitive and secure them in a locked drawer
12. All printers and fax machines should be cleared of papers as soon as they are printed; this helps ensure that sensitive documents are not left in printer trays for the wrong person to pick up.

X. Vendor Management

All the Vendors onboarded by the company should go through a Vendor Management Program. The Vendor Management Program has been put in place by 365 Retail Market's information Security team. The vendor management program entails the necessary Security controls that should be abided by each department.

XI. PCI Policy

All systems that processing Card Holder Data (CHD) are subject to the PCI Policy.

- No systems shall ever store Sensitive Authentication Data (SAD). SAD includes:
  - Full track data (magnetic-stripe data or equivalent on a chip)
  - CAV2/CVC2/CVV2/CID
  - PINs/PIN blocks
- No system shall ever store the full Primary Account Number (PAN)
- All newly developed POS systems that process CHD will encrypt SAD and PAN at the moment of contact (E2EE/P2PE).
- All newly developed internet-based systems that process CHD are to use tokenization for SAD (or an equivalent industry best practice solution).
- Any system that processes CHD in an offline environment (store and forward) will only store the encrypted SAD until the environment comes back online. No unencrypted information is to be stored.
- All systems that store or process PCI information as subject to a yearly PCI-DSS assessment by an independent QSA and must comply with all accompanying standards.

All individuals that come into contact with CHD are subject to the PCI Policy. If the full PAN is needed for processing payments or refunds, never:

- Write down the full PAN
- Stored electronically
- Email or transmit through chat

XII. PHI Policy

All systems that store or process PHI and **all individuals** that come into contact with PHI are subject to the Fullcount and 365 HIPAA Privacy and Security Policies and Procedures.

XIII. Change Management

Changes to systems that handle PHI, PII, PCI, CI or Internal Information will follow a documented Change Management Process.

A. Roles and Responsibilities

- **Change Manager**: Oversees the change management process
- **Change Initiator:** Recognizes and identified the need for a change
- **Change Approval Board (CAB):** Cross-functional leadership team that reviews & approves/rejects changes
- **Roadmap Review Committee**: If the change will impact an already established roadmap, this team will negotiate commitments with the CAB and business leadership.
- **Change Implementation Team:** Implements the change

B. Change Management Steps

1. A Change Initiator requests a change. They note details like the affected systems, possible risks, and expected implementation.

2. The Change Manager determines if the change will be successful. They may ask for more information in this step.
    a. The Change Manager references *the Information Security Policy* and *Information Classifications* when reviewing the change
    b. The Change Manager reviews the Epic's *Compliance* Impact Analysis review, noting if *PII*, *GDPR*, *PCI or CI* impacts have been flagged (*note: PHI is never in scope*)
3. After review, the team plans how to put the change in place. They record details about:
    a. the expected outcomes
    b. resources
    c. timeline
    d. testing
    e. ways to roll back the change
4. Goes to CAB for approval.
5. If approved, the Epic referenced in the Change Log is set to Impact Analysis status and is worked based on priority and road map placement.
6. The Change Manager reviews and closes the Change Request with target implementation date.

XIV. Remote Employee Policy

Employees working remotely are subject to the same policy as those working in an office. Remote employees must log into 365's VPN to access Information systems, as restricted by IP address whitelisting and MFA.

XV. Application Security Architecture Policy

All systems that store or process PHI, PII, PCI, CI and Internal Information and **individuals** that plan, design, develop, test, or deploy related applications are subject to the Application Security Architecture Policy, which includes (but is not limited to):

- Application Security Architecture documents and diagrams
- Deployment and infrastructure considerations
- Input validation
- Authentication
- Authorization
- Configuration management
- Session management
- Cryptography
- Parameter manipulation
- Exception management
- Auditing and logging
- Application frameworks and libraries
- Static and dynamic code analysis

XVI. Encryption Management

365's Encryption Management strategy begins with a stringent access control policy and continuous work to define the least privilege necessary for persons or systems accessing data. In conjunction with the access control policy, a strong Encryption Management Strategy must also be implemented.

- All sensitive data including PHI, PII, PCI, CI, and some internal information must be encrypted at rest and in transit.
- Decryption keys should never be kept on the same machine/environment as the encrypted data.
- Access to data and access to encryption keys should be managed separately. For example, create one set of administrators who can only manage keys and a different set of administrators who can only manage access to the underlying encrypted data.
- Encryption key access is to be integrated into logging systems so you can audit who used which keys, for which recourses, and when.
- Always use Advanced Encryption Standard (AES) with 256-bit keys (AES-256) or stronger
- Always use a (virtualized) hardware security module like AWS Key Management Service or AWS CloudHSM to protect keys at rest.
- Always use an HSMs that has been validated under the National Institute of Standards and Technology's FIPS 140-2.

The encryption key lifecycle will be determined for each application based on the sensitivity of the data processed and must be approved by Technology leadership, and reviewed by the Information Security Team. The following should be considered when establishing the key lifecycle

- The amount/volume of information protected by a given key.
- The amount of exposure if a single key is compromised.
- The time available for attempts to penetrate physical, procedural, and logical access.
- The period within which information may be compromised by inadvertent disclosure.
- The time available for computationally intensive cryptanalytic attacks"

A general rule is, as the sensitivity of data being secured increases, the lifetime of an encryption key decreases.

XVII. Contingency Plan

Controls must ensure that 365 RETAIL MARKETS can recover from any damage to computer equipment or files within a reasonable period of time. Each entity is required to develop and maintain a plan for responding to a system emergency or other occurrence (for example, fire, vandalism, system failure and natural disaster) that damages systems that contain PHI, PII, PCI, CI or Internal Information. This will include developing policies and procedures to address the following:

Data Backup Plan

- A data backup plan must be documented and routinely updated to create and maintain, for a specific period of time, retrievable exact copies of information.
- Backup data must be stored in an off-site location and protected from physical damage.
- Backup data must be afforded the same level of protection as the original data.

Disaster Recovery Plan: A disaster recovery plan must be developed and documented which contains a process enabling the entity to restore any loss of data in the event of fire, vandalism, natural disaster, or system failure.

Emergency Mode Operation Plan: A plan must be developed and documented which contains a process enabling the entity to continue to operate in the event of fire, vandalism, natural disaster, or system failure.

Testing and Revision Procedures: Procedures should be developed and documented requiring periodic testing of written contingency plans to discover weaknesses and the subsequent process of revising the documentation, if necessary.

Applications and Data Criticality Analysis: The criticality of specific applications and data in support of other contingency plan components must be assessed and documented

XVIII. IT Asset End of Life Disposal Policy

IT assets including, but not limited to, kiosks, POS devices, card readers, employee workstations, servers, network devices, printers and other office equipment are subject to the IT Asset End of Life Disposal Policy.

XIX. Systems Audit

The IST shall perform yearly audits of all systems that store or process PHI, PII, PCI, CI or Internal Information against the 365 RETAIL MARKETS Information Security Policy. Systems found to be out of compliance shall be documented and tracked through remediation as part of CHANGE MANAGEMENT.

XX. Policy Audit

The IST shall perform a yearly audit of this policy, and make updates as deemed necessary based on emerging best practices in the InfoSec field. Changes to the policy shall be tracked as part of CHANGE MANAGEMENT and documented in DOCUMENT REVISIONS.

XXI. Document Revisions

Version	Change Log
021016	Original policy
072418	Updates to Title Page and document footer
021419	Sections Updated: Risk Management, Information Classification, Information Security Definitions, Computer and Information Control, Scope
	Sections Added: Table of Contents, Document Revisions, Remote Employee Policy, Change Management, PCI Policy, Network Security Policy, Secure Coding Policy, POS Workstation Decommission and Reuse Policy, Systems Audit, Policy Audit

02032021	Sections Updated: Policy, Information Security Responsibilities, Personally Identifiable Information, Transmission Security, Equipment Media Controls, Network Security Policy, PCI Policy, Change Management
	Sections Added: Patch Management
10082021	Added Section: Password Policy
11132021	Section XII. Secure Coding Policy renamed Application Security Architecture Policy and updated.
12202021	Section XII. Secure Coding Policy renamed Application Security Architecture Policy and updated.
09262022	Minor grammatical changes. Sections Updated: VI. Computer and Information Controls, Sections Added: N. Training and Awareness, VIII. Communication Policy, IX. Clean Desk Policy, X. Vendor Management.
10242023	Minor grammatical changes. Sections Updated: V. Risk Management, VI. Computer and Information Control, XV. Application Security Architecture Policy, XXII. Definitions and Acronyms. Sections Added: XII. PHI Policy, XVIII. IT Asset End of Life Disposal Policy,

XXII. Definitions and Acronyms

IST: Information Security Team

ASV: Approved Scanning Vendor

QSA: Qualified Security Assessor

Pen: short for Penetration *Test*

CVSS: Common Vulnerability Scoring System

SDLC: Systems Development Life Cycle

CAB: Change Approval Board

PCI: Payment Card Industry

PHI: Protected Health Information

PII: Personally Identifiable Information

CI: Confidential Information

CHD: Card Holder Data, in context of PCI-DSS

SAD: Sensitive Authentication Data, in context of PCI-DSS

PAN: Primary Account Number, in context of PCI-DSS

PCI-DSS: Payment Card Industry Data Security Standard

Epic: Changes approved as part of CHANGE MANAGEMENT will tracked as an *Epic* through the SDLC. In Agile software development, an Epic is defined as a collection of work with a common objective.

Affiliated Covered Entities: Legally separate, but affiliated, covered entities which choose to designate themselves as a single covered entity for purposes of HIPAA

Availability: Data or information is accessible and usable upon demand by an authorized person.

HIPAA: The Health Insurance Portability and Accountability Act, a federal law passed in 1996 that affects the healthcare and insurance industries. A key goal of the HIPAA regulations is to protect the privacy and confidentiality of protected health information by setting and enforcing standards.

Entity: Distinct business unit within the 365 Retail Markets organization. Typically, a department, collection of departments, or separate service.

365 Platforms: Technologies branded under 365 Retail Markets, AirVend, Company Kitchen, Stockwell, Avanti, Parlevel, Spoonfed, FullCount, CDSI, and Kafoodle.