Postal.io, Inc.

IT Security Policy

This policy provides, for Postal.io, protection to confidential corporate and Subscriber data, whether held centrally, on local storage media, or remotely. This policy reasonably adheres to industry standards and best practice and reasonably provides safeguards against accidental or unlawful destruction, loss, alteration or unauthorized disclosure or access to covered data, as indicated in the Data Security and Privacy Statement.

Protection of Postal.io proprietary software and other managed systems shall be addressed to ensure the continued availability of data and programs to all authorized parties, and to ensure the integrity and confidentiality of impacted data and configuration controls.

As with all Postal.io policies, failure to follow the policy requirement may result in disciplinary action, up to and including termination.

TABLE OF CONTENTS

1. DEFINITIONS

Term/Acronym	Definition
Access Control	The process of limiting access to the resources of a system only to authorized programs, processes or other systems.
Audit Trail	A chronological record of system activities that is sufficient to enable the reconstruction, review, and examination of the sequence of environments and activities surrounding or leading to an operation, a procedure, or an event in a transaction from its inception to final results.
Authenticate	To verify the identity of a user, device, or other entity in a computer system, often as a prerequisite to allowing access to resources in a system.

Authorization	The granting of access rights to a user, program or process.
Data Breach	*Refer to Postal.io Incident Response Process.*
De-Militarized Zone (DMZ)	A physical or logical subnetwork that contains and exposes an organization's external-facing services to a larger and untrusted network, usually the Internet.
Disaster Recovery Plan	A documented process or set of procedures to recover and protect a business IT infrastructure in the event of a disaster.
Discretionary Access Control	A means of restricting access to objects based upon the identity and need to know of the user, process, and/or groups to which they belong.
File Security	The means by which access to computer files is limited to authorized users only.
Firewall	A device and/or software that prevents unauthorized and improper transit of access and information from one network to another.
FTP or File Transfer Protocol	Protocol that allows files to be transferred using TCP/IP.
Hub	Network device for repeating network packets of information around the network.
Identification	The process that enables recognition of an entity by a system, generally by the use of unique machine-readable user names.
Internet	Worldwide information service, consisting of computers around the globe linked together.
Independent Party	An internal resource or external third-party that functions independently from the management and implementation of security policies, processes, and controls.
Information Security	Department responsible for ensuring the implementation and execution of Postal.io information security management systems (ISMS).
IT Administrator	Individual responsible for the upkeep, configuration, security, and reliable operation of computer systems.
IT Department	Departments within *Postal.io* responsible for the management of IT systems, including

	servers, workstations, mobile devices, and network infrastructure.
LAN Analyzer	Device for monitoring and analyzing network traffic. Typically used to monitor network traffic levels. Sophisticated analyzers can decode network packets to see what information has been sent.
Laptop	Small, portable computer or tablet.
Mandatory Access Control	A means of restricting access to objects based upon the sensitivity of the information contained in the objects and the formal authorization of subjects to access information of such sensitivity.
Network Time Protocol (NTP)	Used to synchronize the time of a computer client or server to another server or reference time source, such as a radio or satellite receiver or modem.
Password	A protected, private character string used to authenticate an identity.
Private Branch Exchange (PBX)	Small telephone exchange used internally within a company.
Personal Data	*Refer to Postal.io Incident Response Process*
Personal Information (PI)	*Refer to Postal.io Incident Response Process*
Principle of Least Privilege	Restricting access to systems and data based on job role or function while ensuring that no additional, unneeded access is granted.
Rlogin or Remote Login	Protocol that allows a remote host to login to a UNIX host without using a password.
Security Event	*Refer to Postal.io Incident Response Process*
Security Incident	*Refer to Postal.io Incident Response Process*
Security Incident Response Team (SIRT)	*Refer to Postal.io Incident Response Process*
Security Vulnerability	*Refer to Postal.io Incident Response Process*
Security Weakness	*Refer to Postal.io Incident Response Process*
Shareware	Software for which there is no charge, but a registration fee is payable if the user decides to use the software. Often downloaded from the Internet or available from PC magazines. Normally not that very well written and often adversely affects other software.
Sensitive Company Information (SCI)	Sensitive Company Information or SCI: any record, whether in paper, electronic, or other form, that includes any one or more of the

	following elements in relation to *Postal.io* or its Personnel: Pro-forma financials and budget details; Board meeting minutes and non-public governance documents; Capitalization table, including supporting details regarding any equity grant; Strategic planning minutes and/or presentations; Source code; Compensation for current and past Personnel; Investigation records of current and past Personnel; Current and past Personnel assessments and development plans, including specific scores and feedback; and/or Risk management non-conformities and identified risks. Sensitive Company Information shall not include (i) source code required to be disclosed as part of *Postal.io*'s registration with the U.S. Copyright Office; (ii) quarterly disclosure guidance and/or results and metrics on an individual, team, and department, and company-wide basis with respect to financials and budget details, or (iii) compensation or performance information that is anonymous as to the current or past employee/intern. For clarity, excluded compensation or performance information should be anonymous as to the current or past employee/intern, should not reasonably be linked back to a current or past employee/intern, and should not contain Personal Information.
Sensitive Personal Information (SPI)	*Refer to Postal.io Incident Response Process.*
Telnet	Protocol that allows a device to login to a UNIX host using a terminal session.
Uninterruptable Power Supply (UPS)	Device containing batteries that protects electrical equipment from surges in the main power and acts as a temporary source of power in the event of a main power failure.
Username	A unique symbol or character string that is used by a system to identify a specific user.
Virtual Private Network (VPN)	A network that extends a private network across a public network, such as the Internet.

Virus	Computer software that replicates itself and often corrupts computer programs and data.
Voice Mail	Facility which allows callers to leave voice messages for people who are not able to answer their phone. The voice messages can be played back at a later time.
Wide Area Network (WAN)	A telecommunications network or computer network that extends over a large geographical distance.

2. OWNERSHIP & ADMINISTRATION

This IT Security Policy is owned by the Postal.io Management Team and administered by Information Security.

3. APPLICABILITY

This policy applies to all IT systems, including network equipment and communication systems, supporting *Postal.io* internal and remote operations and the *Postal.io* product portfolio. These policy requirements supersede all other policies, processes, practices, and guidelines relating to the matters set forth herein, with the exception of the Data Security and Privacy Statement. However, additional policies may be put in place that document enhanced policy requirements when such policies requirements are considered confidential. These policies will be reviewed no less frequently than once per calendar year and updated to meet current best practice.

Postal.io uses reasonable efforts to protect the security and privacy of all Information received by, though or on behalf of Postal.io. In cases where a system or provider cannot meet these requirements, exceptions will be noted and documented by Information Security, and alternate controls will be implemented.

4. SECURITY POLICIES

4.1 Data Encryption

- To provide data confidentiality in the event of accidental or malicious data loss, all Personal Data, PII, SPI, SCI or Subscriber data should be encrypted at rest.
- Encryption of data at rest should use at least AES 256-bit encryption.
- Strong cryptography and security protocols, such as TLS 1.2 or IPSEC, are required to safeguard Personal Data, PII, SPI, SCI or Subscriber data during transmission.
- Key exchange must use RSA or DSA asymmetric cryptographic algorithms with a minimum modulus of 2048 bits and SHA-256 or longer for the hashing algorithm.
- Digital signatures must use RSA, DSS with a minimum modulus of 2048 bits and SHA-256 or longer for the hashing algorithm.

- Hashed data must be salted with SHA-256 or higher.
- Encryption of wireless networks should be enabled using the following encryption levels:
    - Corporate Network: At a minimum, WPA2-Enterprise with EAP-TLS (802.1x w/AES and pre-shared keys)
- Personal Data, PII, SPI, SCI or Subscriber data may not be stored on equipment not owned or managed by Postal.io.
- Data may be transferred only for the purposes determined/identified in Postal.io's Data Security & Privacy Statement.
- Documented policies and process should be implemented to ensure appropriate key management.
- If you are unsure regarding the level of required encryption, you should contact Information Security for guidance and approval.

4.2 Password Policy

- Unless otherwise specified within this IT Security Policy, the following security requirements should be adhered to when creating passwords:
    - Minimum of twelve (12) characters in length, containing characters from the following three categories:
    - English uppercase characters (A through Z)
    - English lowercase characters (a through z)
    - Base 10 digits (0 through 9)
    - 1 symbol (-!$@$%^&*()_+|~=`{}:;'<>?,.\[]"/)
- Passwords history should be kept for the previous thirteen (13) passwords and passwords should be unique across the password history.
- Maximum password age is ninety (90) days.
- Must not be the same as or include the user id or be visible when entered.
- Must not be easily guessable.
- Set first-time passwords to a unique value for each user and change immediately after the first use.
- User accounts should be locked after five consecutive (5) incorrect attempts.
- Lockout duration should be set to a minimum of sixty (60) minutes or until an administrator resets the user's account.
- If a session has been idle for more than thirty (30) minutes, the user should be required to re-enter the password to re-activate access.
- The following should be adhered to when managing user passwords:
    - Verify user identity before performing password resets.
- Access to shared network/service/system power user/root/admin passwords should be controlled and limited to no more than three administrators where possible. Usage of these accounts should be monitored.
- Role based access to all systems should be implemented, including individually assigned username and passwords.
- Usernames and passwords should not be shared, written down or stored in easily accessible areas.

- Assigning multiple usernames to users should be limited. However, when multiple usernames are assigned to users, different passwords should be used with each username.
- Group, shared, or generic accounts and passwords should not be used unless approved by Information Security and should follow associated information security standards.
- Special administrative accounts, such as root, should implement additional controls, such as alerting, to detect and/or prevent unauthorized usage.
- Administrator, superuser, and service account passwords should be stored in a secure location, for example a fire safe in a secured area. If these are stored on an electronic device, the device and/or data should be encrypted following Postal.io encryption policy and access restricted accordingly.
- Change any default passwords on systems after installation.
- Render all passwords unreadable during transmission and storage using strong cryptography as defined in Data Encryption policy.
- Remove custom application accounts, user IDs, and passwords before applications become active or are released to subscribers.
- Passwords should be protected in storage by hashing following data encryption policy.

4.3 Authorized Software

- Only authorized and properly licensed software should only be installed on Postal.io owned or managed systems.
- The use of unauthorized software is prohibited. Immediate removal of unauthorized software is required if discovered.
- A security review and approval of all software should be completed prior to production release. The review should be based on system criticality and data type. Free, shareware, and open source software as well as software as a service (SaaS) should be reviewed as well.

4.4 Physical Security

- Physical security of computer equipment should conform to standard or typical industry loss prevention practices.
- Personnel and authorized third parties should ensure that SCI, SPI, PI, and customer data are appropriately secured and follow clean desk/clean screen best practices, especially when stepping away from workspaces.
- Facility entry controls should be used to limit and monitor physical access to systems where SPI, SCI and Subscriber data are maintained, including but not limited to buildings, loading docks, holding areas, telecommunication areas, and cabling areas or media containing SPI, SCI or Subscriber data using appropriate security controls including, but not limited to:
    - Use of video cameras or other access control mechanisms to monitor individual physical access to sensitive areas. Store for at least ninety (90) days, unless otherwise required by law.
    - Restriction of unauthorized access to network jacks.
    - Restriction of physical access to wireless access points, gateways, and handheld devices.

    - Use of defined security perimeters, appropriate security barriers, entry controls and authentication controls, as appropriate.
    - Ensure that any physical access required by NKPs are supervised.
    - All visitors should log in and receive the appropriate access card, as necessary, and identifying badge.
- Any paper and electronic media that contain Subscriber data, SPI, PI, SCI or Personal Data should be physically secured.
- Doors to physically secured facilities should be kept locked at all times.

4.4.1 Power Availability

- All servers are required to use universal power supplies (UPS).
- All hubs, bridges, repeaters, routers and switches and other critical network equipment should be UPS protected.
- Sufficient power availability should be in place to keep the network and servers running until the Disaster Recovery Plan can be implemented.
- UPS software should be installed on all servers to implement an orderly shutdown in the event of a total power failure.
- All UPSs should be periodically tested.

4.4.2 Environmental Protection

- Consideration should be taken to ensure environmental concerns are addressed such as fire, flood, and natural disaster (e.g., earthquake, flood, etc.)
- Data centers owned by vendors that supply services to Postal.io shall perform SOC 1/2 or equivalent audits on an annual basis and vendors shall remediate any findings in a reasonable timeframe.

4.5 Business Continuity and Disaster Recovery

- Disaster recovery plans should support Subscriber business continuity plans and should be in place and tested on a regular basis.
- A business continuity plan that considers information security requirements should be implemented and tested no less frequently than once per calendar year.

4.6 Backups

- Regular backups of data, applications, and the configuration of servers and supporting devices should occur to enable data recovery in the event of a disaster or business continuity event and retained according to data retention policy.
- All backups should be encrypted following data encryption policy for data at rest and in transit.
- Backups should be stored in a physically and logically secure location

4.7 Virus and Malware Protection

- Up to date anti-malware software for the detecting, removing and protecting of suspected malware should be utilized on all Windows & Linux-based servers, workstations, and laptops. Mac-based systems have built in protections via the operating system.
- Anti-malware software should be updated regularly for all workstations and servers with the latest anti-malware patches and/or signatures.
- Heuristic anti-malware software (signatureless) may be used, with the approval of Information Security.
- All systems should be built from original, clean master copies to ensure that malware is not propagated.
- Users should be made aware of current anti-malware procedures and policies.
- Personnel should inform Information Security and the Help Desk immediately in the event of a possible malware infection.
- Upon notification of a malware infection, affected systems should be promptly isolated from the network, scanned, and cleaned appropriately. Any removable media or other systems to which the virus may have spread should be treated accordingly.
- If a system has been identified as potentially infected and removal/quarantine of the malware cannot be definitively proven, the system should be completely wiped and re-imaged.
- Users or Subscribers impacted by malware related security incidents should be notified as soon as reasonably possible in alignment with incident response procedures.
- Potential malware infections should be immediately reported to Information Security who will take appropriate action including execution of the Computer Incident Response Plan.

4.8 Access Control

- Confidentiality of all data, both Postal.io and Subscriber data should be maintained through discretionary and mandatory access controls.
- Establish process for linking all access to system components (especially access with administrative privileges such as root) to each individual user.
- Postal.io IT should be notified of all Personnel leaving Postal.io's employment by Human Resources prior to or at the end of their employment. As soon as possible after notification, not to exceed twenty-four (24) hours, rights to all systems should be removed unless a specific exception request is approved by Information Security.
- Administrators should only log into systems with user ids attributable to them or follow processes that would not break attribution. For example, administrators should use the su command to obtain root privileges, rather than login as root onto UNIX or Linux systems.
- Access to databases containing Subscriber data, Personal Data, PI, SPI or SCI should always be authenticated. This includes access by applications/services, administrators, and all other users or sources.
- All logins to a Postal.io Subscription should be secured through an encrypted connection (e.g., HTTPS) and appropriately authenticated.
- Ensure proper user account management for all users as follows, and as described in more detail in the User Account Management Policy:

- Ensure that the Principle of Least Privilege using role-based access control (RBAC) is followed for all users.
- Control addition, deletion, and modification of usernames, credentials, and other identifier objects.
    - Users should be given access to a standard set of applications as set forth by Postal.io based on their job responsibility. Beyond that standard set of applications, users should formally request access to systems required to perform their job functions only.
    - A manager or above should formally approve user access requests. System administrators should act as the final gatekeeper before access is granted.
- Usernames should follow a consistent naming methodology to allow for proper attribution (e.g., use of e-mail addresses, or having usernames consist of the first initial and first five letters of the user's surname).
- Inactive user accounts reviewed and disabled and/or removed no less frequently than every ninety (90) days. Exceptions should be documented, reviewed, and approved by Information Security.
- Enable accounts used by vendors for remote maintenance only during the time period needed. Ensure all vendor activity is monitored.
- Ensure minimal, controlled use of administrator, local administrator, enterprise admin, and/or schema admin profiles.
- Avoid assigning security equivalences that copy one user's rights in order to create another's.
- Performance of periodic review of users' access and access rights should be conducted to ensure that they are appropriate for the users' role.
- Remote access to Postal.io networks should only to be granted to Personnel and/or authorized third parties and must use two-factor authentication (TFA).
- Two-factor authentication (TFA) should be used for any services remotely accessible by Personnel and/or authorized third parties (e.g. Office365), unless Personnel and/or authorized third parties are connected to the protected corporate network.

- Remove external access to subscriber accounts immediately upon notification that subscriber has terminated their relationship with Postal.io. Remove subscriber database from system as prescribed by contract. Overwrite all subscriber backup materials within twelve (12) months of the termination date.
- Access to internet and other external service access should be restricted to authorized parties only.

4.9 Logging, and Monitoring

- System auditing/logging facilities should be enabled and forward to a centralized logging system.
- Monitoring systems used to record login attempts/failures, successful logins and changes made to systems should be implemented. Any exceptions must be approved by Information Security.
- Intrusion detection and logging systems should be implemented to detect unauthorized access to the networks.
- Security related monitoring tools and software should only be used as required by role, and only when authorized by Information Security. This includes sniffing, vulnerability identification, and security incident event management tools.
- Auditing features on wireless access points and controllers should be enabled, if supported, and resulting logs should be reviewed periodically Information Security.
- All external ingress/egress connections should be logged.
- Logs shall be retained for one year.
- The following automated audit trails should be implemented for all system components to reconstruct the following events:
    - All individual accesses to SPI.
    - Actions taken by any individual with root or administrative privileges.
    - Access to controlled audit trails.
    - Invalid logical access attempts.
    - Use of identification and authentication mechanisms.
    - Initialization of/changes to system logging.
    - Creation and deletion of system-level objects.
- Record at least the following audit trail entries for all system components for each event:
    - User identification.
    - Type of event.
    - Date and time.
    - Success or failure indication.
    - Identity or name of affected data, system component, or resource.
- Secure audit trails so they cannot be altered. Central repositories of security related logs should be administered and managed by Information Security.
- Limit the viewing of audit trails to those with a job-related need.
- Appropriate security monitoring tools should be implemented to ensure that knowledge of the ongoing security posture is in place and that appropriate actions can be taken to mitigate security events/incidents.
- Access logs should be periodically reviewed and immediate actions taken, as necessary, to mitigate issues found.

4.10. Vulnerability Management

- An independent third party should perform external and application penetration testing no less frequently than once a year, and after any significant infrastructure or application upgrade or modification. These penetration tests should include the following:

    - Network-layer/infrastructure penetration tests.
    - Application-layer penetration tests.
    - Attestation of successful completion, including the remediation of any findings.
- Perform internal and external vulnerability tests no less frequently than quarterly. Ensure findings are addressed in a timely manner.
- Address newly identified threats and vulnerabilities on an ongoing basis based on severity and skill level required to take advantage of the identified vulnerability.
- Ensure that the SDLC Process, as documented separately, is followed to ensure that code put into production is properly tested.

4.11 Security Weakness, Events, and Incidents

- Identified Security Weaknesses should be immediately reported to Information Security. Unless authorized by Information Security, at no time should an attempt be made to take advantage of an identified Security Weakness.
- Security Weaknesses that have been compromised could trigger a Security Event. Security Events shall be analyzed by Information Security to determine whether or not they are considered Security Incidents, which are required to be addressed in accordance with the Incident Response Procedure.
- Security awareness training should be conducted no less frequently than once per calendar year. Training should cover information security policies, as well as best practice. In addition, the following should occur:
    - Security awareness training should be given at the first onboarding session attended by new employees (usually within two weeks of employment)
    - Specialized job-specific training should be given to key stakeholders (i.e., incident management, SOC 2, security policy and process, assessment response best practice, etc.)

4.12 Auditing and Assessments

- An Independent Party should verify Postal.io's compliance with the IT Security Policy through periodic audits, no less frequently than once per calendar year.
- Postal.io will obtain SOC 2 certification, or equivalent, ensuring that Postal.io's information security management system (ISMS) continues to perform in alignment with the standard.
- Data center providers should have SOC 2, or equivalent, audits performed no less frequently than once per calendar year.
- Customers can perform reasonable security assessments no less frequently than once per calendar year, following industry best practice.
- Customer audits are generally not allowed, due to confidentiality, complexity, and resource requirements. However, attestation letters and certifications can be provided to demonstrate Postal.io's compliance with this IT Security Policy

4.13 Server Security

- Servers should be physically secured.
- All administrative access should be encrypted in adherence with Postal.io's encryption policy. Access via unencrypted protocols (i.e Telnet / FTP) should be prevented.
- Personnel or authorized third parties should log out or lock servers not accessing the server or any length of time.
- Limit the number of concurrent connections to two (2), where possible.
- Only one (1) primary function per server should be implemented, where possible.
- Limit direct root access to the system console only or if no other method of attributable accessibility is available. Information Security must be informed in cases where no other method of attributable accessibility is available.
- Define and implement server build standards that include, at a minimum, the following:
    - Hardening based on industry best practice (e.g., CIS standards);
    - Host based intrusion detection (HIDS)/ File integrity Management (FIM)
    - Anti-virus/anti-malware;
    - Centralized logging configuration

4.14. Patch Management

- Server operating systems should be patched within 48 hours of a critical and/or security patch release.
- Workstations and Laptops should be patched within 48 hours of a critical and/or security patch release.
- Network devices should be patched within 48 hours of the release of a critical security patch.
- Zero-day patches should be tested and applied on all systems immediately.
- Patches should be tested prior to rollout in the production environment. Less critical systems should be patched first.

4.15 Endpoint Security

- Users should shutdown, logout or lock workstations when leaving for any length of time.
- Workstations and laptops should be restarted periodically.
- Workstations and laptops should adhere to virus and malware protection policy.
- Define and implement endpoint build standards that include, at a minimum, the following:
    - Defined configurations based on industry best practice;
    - Authorized software
    - Anti-virus/anti-malware
    - SIEM agents
- Workstation access to the Internet should be controlled (e.g., through mechanisms such as web filtering)

4.16 Mobile Computing

- Ensure appropriate controls are in place to mitigate risks to protected information from mobile computing and remote working environments.
- Data loss prevention processes and tools should be implemented to identify and/or prevent data loss.
- Use of personally owned devices should comply to acceptable use and information security policies if used to access SPI, PI, or SCI data.
- Devices owned by personal should never be used to access customer data, unless appropriate controls approved and monitored by Information Security have been implemented.
- Personal Devices or devices not owned by Postal.io are not allowed to connect to the corporate or production networks.

4.17 Network Security

- Access to internal and external network services that contain Subscriber's data should be controlled through one or more of the following:
    - Network access control lists (NACLs), or equivalent.
    - Firewall policies, or equivalent
    - Security groups, or equivalent.
    - IP whitelists, or equivalent
    - A multi-tier architecture that prevents direct access to data stores from the internet.
    - Usage of role-based access controls (RBAC) should be implemented to ensure appropriate access to networks
    - Two-factor authentication for remote access should be implemented as a time-based token.
- Firewalls, routers, and access control lists, or equivalent access controls, should be used to regulate network traffic for connections to/from the Internet or other external networks, as follows:
    - Configuration standards should be established and implemented.
    - Access control policy should limit inbound and outbound traffic to only necessary protocols, ports, and/or destinations.
    - Internal IP address ranges should be restricted from passing from the Internet into the DMZ or internal networks.
    - All inbound internet traffic should terminate in the DMZ or an equivalent network approved by Information Security.
    - Only properly established connections should be allowed into Postal.io resources.
    - The use of all services, protocols, and ports allowed to access Postal.io resources should be reviewed on a periodic basis, no less frequently than every six (6) months, for appropriate usage and control implementation.
    - All rule set modifications should be reviewed and approved by Information Security prior to implementation.
    - Direct access between the Internet and any system containing SPI should be prohibited.

- Network equipment should be configured to close inactive sessions.
- Remote access servers should be placed in the firewall DMZs or equivalent network approved by Information Security.
- Network intrusion detection systems (IDS) should be implemented and monitored by Information Security.
- Secure, encrypted VPN connections to other networks controlled by Postal.io or outside entities, when required, must be approved by Information Security.

4.17.1 Routers, Hubs and Switches

- LAN equipment, hubs, bridges, repeaters, routers and switches should be kept in physically secured facilities.
- Network equipment access should be restricted to appropriate Personnel only. Other staff and contractors requiring access are required to be supervised.
- Network equipment access should occur over encrypted channels as defined in the data encryption policy. Access via unencrypted protocols (http, telnet, ftp, tftp) should not occur. Unused channels should be disabled.
- Wireless access points and controllers should not be allowed to connect to the production network.
- Unnecessary protocols should be disabled or removed from routers and switches.
- Configuration of routers and switches should be documented and align with industry best practice. This should include changing any vendor-supplied defaults (passwords, configurations, etc.) before installing in production.

4.17.2 Cabling

- Network cabling should be documented in physical and/or logical network diagrams.
- All unused network points should be disabled when not in use.
- Storing or placing any item on top of network cabling should be avoided.
- Redundant cabling schemes should be used whenever possible.

4.18 Wireless Network Security

- Wireless networks should be encrypted as defined by Postal.io's encryption policy
- Access to wireless networks should be restricted to only those authorized, as follows:
    - Guest Network: Accessible by guests with appropriate employee approval (no direct access to corporate network) with minimal web-filtering in place.
    - Extranet Network: Only accessible by approved employee owned devices (no direct access to corporate network) with minimal web-filtering in place
    - Corporate Network: Only accessible by Postal.io owned devices with controlled ingress/egress and web filtering.
- Personnel and authorized third parties are not allowed to install unauthorized wireless equipment.
- All wifi bridges, routers and gateways should be physically secured.
- SSIDs and default usernames and passwords must be modified prior to implementation in a production environment.

4.19 Clock Synchronization

- Clocks of information processing systems performing critical or core functions within the Postal.io environment should be synchronized to a single reference time source (i.e., external time sources synchronized to a standard reference, such as via NTP).

4.20 Test, Development and Production Environments

- Test software upgrades, security patches and system and software configuration changes before deployment, including but not limited to the following:
    - Validate proper error handling.
    - Validate secure communications.
    - Validate proper role-based access control (RBAC).
    - Check performance impact
- Development, sandbox, and production environments must be segregated.
- Separation of duties must exist between development/staging, test, and production environments.
- Use only scrubbed/anonymized data (e.g., SPI, PI or personal data removed or anonymized) for *Postal.io* testing and/or development.
- Remove test data and accounts before production systems become active.
- Follow change control procedures for all changes to system components. The procedures should include testing of operational functionality.

4.21 Development

- Manage all code through a Version Control System to allow viewing of change history and content.
- Ensure that a Quality Assurance (QA) methodology is followed using a multi-phase quality assurance release cycle that includes security testing.
- Deliver security fixes and improvements aligning to a pre-determined schedule based on identified severity levels.
- Perform vulnerability testing as a component of QA testing and address any findings prior to software release.
- Ensure that software is released only via production managed change control processes, with no access or involvement by the development and test teams.
- Develop all web applications (internal and external, including web administrative access to application(s)) based on secure coding best practice. Cover, at a minimum, prevention of common OWASP Top 10 coding vulnerabilities in software development processes, including the following:
    - Cross-site scripting (XSS).
    - Injection flaws, including SQL, LDAP and Xpath.
    - Malicious file execution.
    - Insecure direct-object references.
    - Cross-site request forgery (CSRF).
    - Information leakage and improper error handling.

    - Broken authentication and session management.
    - Insecure communications.
    - Failure to restrict URL access.
- Awareness training regarding secure coding must be conducted at least once per calendar year. The curriculum must be approved by Information Security.

4.22 Transfer of Information

- To protect the confidentiality of SPI in transit:
    - Ensure that all data in transit is either encrypted and/or the transmission channel itself is encrypted following data encryption policy.
    - Where technically possible, monitor all data exchange channels to detect unauthorized information releases.
    - Use Information Security approved security controls and data exchange channels.

4.23 Data Classification, Labeling, and Handling

- Data classification, labelling and handling polices should be put in place in order to ensure that data is appropriately handled (e.g. Data Security and Privacy Statement, etc.)
- Strict control over the storage and accessibility of media that contains SPI should be maintained.
- Properly maintain inventory logs of all media and conduct media inventories at least annually.
- Destroy media containing SPI when it is no longer needed for business or legal reasons by following procedures including, but not limited to:
    - Disposal of media containing SPI so that it is rendered unreadable or undecipherable, such as by burning, shredding, pulverizing, or overwriting. Media sanitization processes should be implemented following the NIST 800-88 standard, where possible.
    - The destruction process shall be completed within 30 days of identifying media that should be removed. A log identifying the data that was destroyed and the date/time of destruction shall also be recorded (the “Disposal Log”)
    - Disposal logs should be maintained that are secured and that provides an audit trail of disposal activities. The log will be kept for a minimum of ninety (90) days. Certificates of destruction should be maintained for at least one year.

4.24 Messaging Security

- All incoming email should be scanned for viruses, phishing attempts, and spam.
- Outgoing email should have data loss prevention (DLP) monitoring in place.
- Any messaging service must be approved by Information Security prior to usage and must include appropriate audit trails and encryption of data at rest and in transit. Data loss prevention (DLP) tools and processes should be implemented, where possible.

4.25. Removable Media

- All removable media brought in from outside Postal.io should be scanned for viruses/malware prior to use. Any identified malware/viruses should be removed with the assistance of Information Security prior to use.
- Sensitive Personal information (SPI) is prohibited on any kind of removable device, unless the device is encrypted per the data encryption policy. Notwithstanding the foregoing, if stored or cached information resides on a removable device, Personnel will follow company policies and procedures, including acceptable use requirements as defined in the Data Security and Privacy Policy, to mitigate the risk of a Data Breach.
- Individuals in sensitive positions, with access to SPI, SCI or customer data, should not store such data on removable media, unless required by their role and approved by Information Security.

4.26 Voice System Security

- Use an access pin with a minimum length of six (6) digits should be used for voice mail accounts.
- Do not match voice mail access pins to the last six (6) digits of the phone number.
- Lock out the caller to a voice mail account after three sequential failed (3) attempts at pin validation.
- If a centralized system is used, check telephone bills carefully to identify any misuse of the telephone system.

4.27 Inventory Management

- An inventory of all computer equipment and software in use throughout Postal.io should be maintained.
- Computer hardware and software audits should be periodically carried out. Audits should also be used to track:
    - Unauthorized copies of software
    - Unauthorized changes to hardware and software configurations
    - Accuracy of current inventory

4.28 Background Checks

- Postal.io will process pre-employment background check on all new hires. Employment at Postal.io shall be contingent upon a satisfactory background check, including:
    - Social Security number trace.
    - Education.
    - Work Experience.
    - Criminal Background Check.
    - Credit Check, if relevant to the position.
    - Reference Check.

- Once hired, a background check may be conducted throughout the course of employment with Postal.io. This generally will occur in circumstances involving transfer to a position of high-level security or responsibility.

4.29 Vendor/Partner Risk Management

- Vendor and partner risk management policies and process should be defined to verify that vendors comply with security policies.
- Vendor and partner contracts should include language requiring adherence to security policy requirements or their equivalent.
- Critical vendors should be reviewed no less frequently than once per calendar year, to ensure continued alignment with security policies.