7710 W. Sahara Ave, Suite 126, Las Vegas, NV 89117

eConnect Information Security Document

Introduction to the ISP (Information Security Policy)

1.1. eConnect provides software and solutions to hundreds of commercial enterprises around the US and the world. This policy addresses procedures and protections outlined to protect, secure, and provide access to systems, software, and subscriber data.

1.2. This policy reasonably adheres to industry standards and best practice and provides safeguards against accidental or unlawful destruction, loss, alteration or unauthorized disclosure or access to covered data. This policy is designed to provide a consistent application of security controls for eConnect and eConnect subscribers.

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

2. Scope of the ISP

2.1. This document applies to all the users in the Organization. The organization employs no temporary users or visitors with temporary access to services and when working with partners those partners have limited or access to monitored services. Compliance with policies in this document is mandatory for this constituency.

3. History of the ISP

Version	Description	From	To	Author
1.0	Initial version	10-01-2020	12-31-2021	Jack Coronel

Roles	Responsibilities
President & CEO	Accountable for all aspects of the Company's Information Security Policy.
Chief Technology Officer	Responsible for the security of the IT infrastructure. Plan against security threats, vulnerabilities, and risks. Respond to information security incidents. Help in disaster recovery plans.
Department Leaders	Help with the security requirements for their specific area.

	Determine the privileges and access rights to the resources within their areas.
IT Team Leaders	Implements and operates IT security. Implements the privileges and access rights to the resources. Implement and maintain Security Policy documents. Ensure security training programs. Ensure IT infrastructure and team supports Security Policies.
Users	Meet Security Policies. Report any attempted security breaches.

4. General Policy Definitions

4.1. All the IT services should be used in compliance with the technical and security requirements defined in the design of the services.

4.2. eConnect uses reasonable efforts to protect the security and privacy of all information received by though or on behalf of eConnect or it's customers. In cases where a system or provider cannot meet these requirements, exceptions will be noted and alternate controls will be implemented.

4.3. Infractions of the policies in this document may lead to disciplinary actions. In some serious cases they could even lead to termination, and or prosecution.

5. Data Protection & Encryption

5.1. To provide data confidentiality in the event of accidental or malicious data loss, all Personal Data, PII, SCI or Subscriber Data shall be encrypted at rest.

5.2. Encryption of data at rest shall use at least AES 256-bit encryption.

5.3. Strong cryptography and security protocols, such as TLS 1.2 or IPSEC, are required to safeguard Personal Data, PII, SCI or Subscriber Data during transmission.

5.4. Key exchange shall use RSA or DSA cryptographic algorithms with a minimum key length of 2048 bits and minimum digest length of 256.

5.5. Digital signatures shall use RSA, DSS with a minimum key length of 2048 bits and minimum digest length of 256.

5.6. Hashed data shall use bcrypt for the hashing algorithm. Bcrypt incorporates an algorithmic salt to protect against rainbow table attacks and is an adaptive function. As such, the iteration count shall be balanced to ensure an appropriate security vs. performance balance in order to resist brute-force search attacks.

5.7. Encryption of wireless networks shall be enabled using the following encryption levels:

5.7.1. Corporate Network: At a minimum, WPA2-Enterprise with PEAP (802.1x w/AES) and 2FA using domain joined machines.
5.7.2. Extranet Network (isolated from Corporate and Guest Network): WPA2-Enterprise with PEAP (802.1x w/AES)
5.7.3. Guest Network (isolated from Corporate and Extranet Network): Captive Portal (requires eConnect Personal to authorize access) with guests required to connect over secure connections (https) for encrypted transit.
5.7.4. Any additional required wireless networks that cannot be addressed by the identified wireless network types above must be approved and adhere to data protection and encryption policy.

5.8. Personal Data, PII, SCI or Subscriber Data shall not be stored on equipment not owned or managed by eConnect, Inc.
5.9. Data shall be transferred only for the purposes determined and identified as essential.
5.10. Appropriate encryption and key management is in place.
5.10.1. If you are unsure regarding the level of required encryption or specific encryption policies, you shall contact Information Security for guidance and approval.
5.11. Data loss prevention processes and tools shall be implemented to identify and/or prevent data loss.

6. Password Policy

6.1. Unless otherwise specified within this IT Security Policy, the following security requirements shall be adhered to when creating passwords:
6.1.1. Minimum of eight (8) characters in length, containing characters from the following three categories:
6.1.2. English uppercase characters (A through Z)
6.1.3. English lowercase characters (a through z)
6.1.4. Base 10 digits (0 through 9)
6.1.5. The use of non-alphabetic characters (e.g., !, $, #, %) is optional but is highly recommended.
6.1.6. Shall not be the same as or include the user id.
6.1.7. Passwords shall not be visible by default when entered.
6.1.8. Passwords shall not be easily guessable.
6.2. Maximum password age is one hundred eighty (180) days.
6.3. Set first-time passwords to a unique value for each user and change immediately after the first use.
6.4. User accounts shall be locked after seven (7) incorrect attempts.

6.5. Lockout duration shall be set to a minimum of thirty (30) minutes or until an administrator resets the user's ID upon proper user identity verification.

6.6. If a session has been idle for more than ten (10) minutes, the user shall be required to re-enter the password to re-activate access.

6.7. The following shall be adhered to when managing user passwords:

6.7.1. Verify user identity before performing password resets.

6.7.2. Where possible, these requirements shall be automatically enforced using management tools such as Active Directory Group Policy or specific system configuration(s).

6.7.3. Access to shared network/service/system power user/root/admin passwords shall be controlled and limited to no more than three administrators. Usage of these accounts shall be monitored.

6.7.4. Role based access to all systems shall be implemented, including individually assigned username and passwords.

6.7.5. Usernames and passwords shall not be shared, written down or stored in easily accessible areas.

6.7.6. Assigning multiple usernames to users shall be limited. However, when multiple usernames are assigned to personnel, different passwords shall be used with each username.

6.7.7. Group, shared, or generic accounts and passwords shall not be used unless approved (e.g., service accounts) and shall follow approved information security standards.

6.7.8. Special administrative accounts, such as root, shall implement additional controls, such as alerting, to detect and/or prevent unauthorized usage.

6.7.9. Administrator, superuser, and service account passwords shall 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 shall be encrypted following eConnect encryption policy and access restricted accordingly.

6.7.10. Change any default passwords on systems after installation.

6.7.11. Render all passwords inaccessible during transmission using encryption.

6.7.12. Passwords shall be protected in storage by hashing.

6.7.13. Remove custom application accounts, user IDs, and passwords before applications become active or are released to subscribers.

7. Authorized Software

7.1. Only authorized, supported, and properly licensed software shall only be installed on eConnect owned or managed systems.

7.2. Only IT administrators or specific personnel approved and who have been granted administrator access shall install authorized and licensed software.

7.3. The use of unauthorized software is prohibited. Immediate removal of unauthorized software is required if discovered.

7.4. Workstation configurations or build standards defined by the IT Department are required to be followed. Change of definitions is only allowed by the IT Department, or authorized parties who have been specifically granted administrator access.

7.5. A security review and approval of all software shall be completed prior to production release. The review shall be based on system criticality and data type. Free, shareware, and open source software as well as software as a service (SaaS) shall be reviewed as well.

7.6. Software that is end-of-life and no longer supported is considered unauthorized software, and shall be addressed.

8. Physical Security

8.1. Physical security of computer equipment shall conform to recognized loss prevention guidelines.

8.2. Personnel and authorized third parties shall ensure that Sensitive Compartmented Information (SCI), Personal Identifiable Information (PII), Personal Information (PI), and customer data are only recreated in hardcopy format where absolutely needed for an identified purpose and are appropriately secured. All Personnel and authorized third parties shall follow clean desk/clean screen best practices, especially when stepping away from workspaces.

8.3. Facility entry controls shall be used to limit and monitor physical access to systems where PII, SCI and Subscriber Data are maintained, including but not limited to buildings, loading docks, holding areas, telecommunication areas, and cabling areas or media containing PII, SCI or Subscriber Data using appropriate security controls including, but not limited to:

8.4. Use of video cameras or other access control mechanisms to monitor individual physical access to sensitive areas.

8.5. Store video for at least ten (10) days, unless otherwise required by law.

8.6. Restriction of unauthorized access to network access points.

8.7. Restriction of physical access to wireless access points, gateways, and handheld devices.

8.8. Use of defined security perimeters, appropriate security barriers, entry controls and authentication controls, as appropriate.

8.9. Ensuring that all personnel with physical data center access to data centers containing PII, SCI or Subscriber Data wear visible identification that identifies them as employees, contractors, visitors, etc.

8.10. Restriction of non-personnel or Need to Know Parties (NKP) from being given virtual access to the Data Center without appropriate approvals in place.

8.11. Ensure that any physical access required by NKPs is supervised.
8.12. All visitors shall log in and receive the appropriate access, as necessary.
8.13. Any paper and electronic media that contain Subscriber Data, PII, SCI or Personal Data shall be physically secured.
8.14. Doors to physically secured facilities shall be kept locked at all times.

9. Power Availability

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

10. Environmental Protection

10.1. Consideration shall be taken to ensure environmental concerns are addressed such as fire, flood, and natural disaster (e.g., earthquake, flood, etc.)
10.2. Redundant air conditioning units shall be in place to ensure maintenance of appropriate temperature and humidity in the data center.
10.3. Data centers shall be required to perform SOC 1/2 or equivalent audits on an annual basis and vendors shall be required to remediate any findings in a reasonable timeframe.

11. Business Continuity and Disaster Recovery

11.1. Disaster recovery plans shall support customers business continuity plans and shall be in place and tested on a regular basis.
11.2. A business continuity plan that considers information security requirements shall be discussed and tested at least once per calendar year.

12. Backups

12.1. Regular backups of data, applications, and the configuration of servers and supporting devices shall occur to enable data recovery in the event of a disaster or business continuity event and retained according to Data Retention Policy.
12.2. All backups shall be encrypted following Data Protection & Encryption Policy for data at rest and in transit.
12.3. Backups shall be encrypted and stored in a physically and logically secure geographically separate location

12.4. Backups for critical systems and systems that contain production Subscriber Data, Personal Data and/or PII shall be performed on at least a daily basis.

13. Virus and Malware Protection

13.1. Up to date anti-virus software for the detecting, removing and protecting of suspected viruses shall be installed on all servers, workstations, and laptops.

13.2. Anti-virus software shall be updated regularly for all workstations and servers with the latest anti-virus patches and/or signatures, where applicable.

13.3. Heuristic anti-virus software (signatureless) can be used, with the approval of Information Security.

13.4. All systems shall be built from original, clean master copies to ensure that viruses are not propagated.

13.5. Users shall be made aware of current anti-virus procedures and policies.

13.6. Personnel shall inform the IT Department immediately in the event of a possible virus infection.

13.7. Upon notification of a virus infection systems shall be isolated from the network, scanned, and cleaned appropriately. Any removable media or other systems to which the virus shall have spread shall be treated accordingly.

13.8. If a system has been identified as potentially infected and removal/quarantine of the virus/malware cannot be definitively proven, the system shall be completely wiped and re-imaged.

13.9. Users or Subscriber's impacted by virus related security incidents shall be notified as soon as reasonably possible in alignment with incident response procedures.

13.10. Potential virus and malware infections shall be immediately reported to the IT Team Leader.

14. Access Control

14.1. Confidentiality of all data, both eConnect and Subscriber Data, shall be maintained through discretionary and mandatory access controls administered by eConnect or the respective customer, as applicable.

14.2. Establish a process for linking all access to system components (especially access with administrative privileges such as root) to each individual user.

14.3. The IT Department shall be notified of all personnel leaving eConnect's employ by HR (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 shall be removed unless a specific exception request is received from Talent, Legal or Information Security.

14.4. Administrators shall only log into systems with user ids attributable to them or follow processes that would not break attribution.

14.5. Access to databases containing Subscriber Data, Personal Data, PII or SCI shall always be authenticated. This includes access by applications/services, administrators, and all other users or sources.

14.6. All access shall be removed for users who administer or operate systems and services that process Personal Data and PII where their user controls are compromised (e.g., due to corruption or compromise of passwords, or inadvertent disclosure).

14.7. The reissuance of de-activated or expired user IDs for systems or services that process Personal Data and PII shall not be permitted.

14.8. All logins to the Subscription shall be secured through an encrypted connection (e.g., HTTPS) and appropriately authenticated.

14.9. Ensure proper user management for all users as follows:

14.9.1. Ensure that the Principle of Least Privilege using role-based access control (RBAC) is followed for all users.

14.9.2. Control addition, deletion, and modification of usernames, credentials, and other identifier objects.

14.9.3. Users (including temps, consultants, and contractors) shall formally request access to systems with only the rights necessary to perform their job functions.

14.9.4. A manager or above and the system owner shall formally approve user roles and access requests. System administrators shall act as the final gatekeeper to ensure access is granted appropriate to the identified role.

14.9.5. Usernames shall follow a consistent naming methodology to allow for proper attribution (e.g., generally consisting of the first initial and first five letters of the user's surname).

14.9.6. Inactive user accounts are reviewed and disabled and/or removed at least every ninety (180) days. Exceptions shall be documented, reviewed, and approved by Information Security.

14.9.7. Enable accounts used by vendors for remote maintenance only during the time period needed. Ensure all vendor activity is monitored.

14.9.8. Ensure minimal, controlled use of administrator, local administrator, enterprise admin, and/or schema admin profiles.

14.9.9. Avoid assigning security equivalences that copy one user's rights in order to create another's.

14.9.10. Performance of periodic review of users' access and access rights shall be conducted to ensure that they are appropriate for the users' role.

14.10. Remote access to eConnect networks shall only be granted to personnel and/or authorized third parties and shall use two-factor authentication (TFA) or multi-factor (MFA) authentication.

14.11. Two-factor authentication (TFA) or multi-factor authentication (MFA) shall be used for any services remotely accessible by personnel and/or authorized third parties (e.g. Office365, VPN, etc.), unless personnel and/or authorized third parties are connected to the protected corporate network.
14.12. Remove external access to subscriber databases immediately upon notification that subscriber has terminated their relationship with eConnect.
14.13. Remove subscriber databases from the system within thirty (30) days of subscriber termination.
14.14. Overwrite all subscriber backup data within twelve (12) months of the subscriber's termination date.
14.15. Access to the internet and other external services shall be restricted to authorized parties only based on the assigned role.
14.16. Revalidation timeouts for SaaS products and services used by eConnect Personnel must be set to 12 hours or less.

15. Logging, and Monitoring

15.1. System auditing/logging facilities shall be enabled and forward to a centralized logging system, which in the event of any applicable log restoration efforts shall capture the name of the person responsible for restoration and a description of the Personal Data and PII being restored.
15.2. Secure audit trails shall be protected so they cannot be altered.
15.3. Central repositories of security related logs shall be administered and managed by the Information Security Department.
15.4. Monitoring systems used to record login attempts/failures, successful logins and changes made to systems shall be implemented. Any exceptions shall be approved by Information Security.
15.5. Intrusion detection and logging systems shall be implemented to detect unauthorized access to the networks.
15.6. Security related monitoring tools and software shall 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.
15.7. Auditing features on wireless access points and controllers shall be enabled, if supported, and resulting logs shall be reviewed periodically Information Security.
15.8. All external ingress/egress connections shall be logged.
15.9. Logs shall be retained for one year.
15.10. The following automated audit trails shall be implemented for all system components to reconstruct the following events:
15.10.1. All individual accesses to PII.
15.10.2. Actions taken by any individual with root or administrative privileges.
15.10.3. Access to controlled audit trails.

15.10.4. Invalid logical access attempts.
15.10.5. Use of identification and authentication mechanisms.
15.10.6. Initialization of/changes to system logging.
15.10.7. Creation and deletion of system-level objects.

15.11. Record at least the following audit trail entries for all system components for each event:
15.11.1. User identification.
15.11.2. Type of event.
15.11.3. Date and time.
15.11.4. Success or failure indication.
15.11.5. Identity or name of affected data, system component, or resource.
15.11.6. Viewing of audit trails shall be limited to those with a job-related need.

15.12. Appropriate security monitoring tools shall 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.

15.13. Access logs shall be periodically reviewed, and immediate actions taken as necessary to mitigate issues found.

16. Vulnerability Management

16.1. The eConnect IT team shall perform external and application penetration testing at least once per calendar year or after any significant infrastructure or application upgrade or modification. These penetration tests shall include the following:
16.1.1. Network-layer/infrastructure penetration tests.
16.1.2. Application-layer penetration tests.
16.1.3. Mobile application penetration testing
16.1.4. Attestation of successful completion, including the remediation status of any findings.
16.1.5. Perform internally conducted internal and external vulnerability tests at least quarterly. Ensure findings are addressed in a timely manner.
16.1.6. Address newly identified threats and vulnerabilities on an ongoing basis based on severity and skill level required to take advantage of the identified vulnerability.
16.1.7. Ensure the following are implemented:
16.1.8. Static code testing
16.1.9. Dynamic code testing of the test and production environment
16.1.10. Manual testing after any significant changes
16.1.11. Processes to ensure that security vulnerabilities identified as Severity 2 or higher using the OWASP DREAD model or equivalent are not released into the production environment.

16.1.12. Processes to ensure identified vulnerabilities are addressed in a timely manner, based on risk.
16.1.13. 30 days for high-risk critical and/or security vulnerabilities.
16.1.14. 14 days for zero-day vulnerabilities.

17. Security Awareness

17.1. Security awareness training shall be conducted at least once per calendar year. Training shall cover information security policies, as well as best practice. In addition, the following shall occur:
17.2. Security awareness training shall be given at the first onboarding session attended by new employees (usually within two weeks of employment)
17.3. Specialized training shall be given to key stakeholders around security policy and process, assessment response best practices.
17.4. Identified Security Weaknesses or Security Vulnerabilities shall be immediately reported to the IT.
17.5. Unless authorized by the IT Department, at no time shall an attempt be made to take advantage of any Security Weakness or Security Vulnerability.
17.6. Security Weaknesses or Vulnerabilities that have been compromised could trigger a Security Event. Security Events shall be analyzed to determine whether or not they are considered Security Incidents.

18. Auditing and Assessments

18.1. The eConnect CTO shall verify eConnect's compliance with the IT Security Policy through periodic audits, at least once per calendar year.
18.2. eConnect will maintain a high level of industry standards, ensuring that eConnect information security management system (ISMS) continues to perform in alignment with the standard.
18.3. Data center providers shall have SOC 2 audits performed regularly.
18.4. Customers can perform reasonable security assessments as needed following industry best practice.
18.5. Customer audits are generally not allowed, due to confidentiality, complexity, and resource requirements. However, attestation letters and certifications can be provided to demonstrate eConnect compliance with IT Security Policy

19. Server Security

19.1. Servers shall be physically secured.
19.2. All administrative access shall be encrypted in adherence with eConnect's policy. Access via unencrypted protocols (i.e Telnet / FTP) is not allowed without prior IT approval.
19.3. Limit the number of concurrent connections to two (2), where possible.
19.4. Only one (1) primary function per server shall be implemented, where possible.

19.5. Server administrators shall be limited to one primary administrator and two backup administrators, where feasible. Exceptions shall be approved by IT.
19.6. End-of-life and/or end-of-support servers shall not be used and, if discovered, removed from the network as soon as possible.
19.7. Define and implement server build standards that include, at a minimum, the following:
19.7.1. Hardening based on industry best practice (i.e. CIS standards);
19.7.2. Host based intrusion detection (HIDS)/ File integrity Management (FIM)
19.7.3. Anti-virus/anti-malware;
19.7.4. Centralized logging configuration
19.7.5. SIEM Security information and event management

20. Patch Management

20.1. Server operating systems shall be patched within 30 days of a critical and/or security patch release.
20.2. Workstations and Laptops shall be patched within 30 days of a critical and/or security patch release.
20.3. Network devices shall be patched within 30 days of the release of a critical and or security patch.
20.4. Zero-day patches shall be applied on all systems containing Subscriber Data and critical systems within 14 days, and all other systems within 30 days.
20.5. Patches shall be tested prior to rollout in the production environment. Less critical systems shall be patched first.
20.6. Failure to patch within defined timelines could result in disciplinary action, up to and including termination.

21. Endpoint Security

21.1. Users shall shutdown, logout or lock workstations when leaving for any length of time.
21.2. Workstations and laptops shall be restarted periodically.
21.3. Workstations and laptops shall adhere to virus and malware protection policy.
21.4. Define and implement endpoint build standards that include, at a minimum, the following:
21.4.1. Defined configurations based on industry best practice;
21.4.2. Authorized software
21.4.3. Anti-virus/anti-malware
21.4.4. Web Filtering/Cloud Access Security Broker (CASB)
21.4.5. SIEM agents (e.g. Rapid7 IDR)
21.5. Workstation access to the Internet shall be controlled based on assigned or departmental role.

22. Mobile & Remote Computing

22.1. Ensure appropriate controls are in place to mitigate risks to protected information from mobile computing and remote working environments.

22.2. Data loss prevention processes and tools shall be implemented to identify and/or prevent data loss.

22.3. eConnect data shall be removed from employee owned mobile devices within the timelines defined in termination policies.

22.4. Use of personally owned devices shall comply with acceptable use and information security policies if used to access Personal Data, PII or SCI data.

22.5. Devices owned by personnel shall never be used to access customer data, unless appropriate monitored controls, approved by IT have been implemented.

22.6. Devices owned by personal or authorized parties are not allowed to connect to corporate or production networks.

22.7. Employee owned mobile devices shall have the ability to connect to a network separate from the guest network, where feasible.

23. Network Security

23.1. Access to internal and external network services that contain Subscriber's Data shall be controlled through:

23.1.1. Network access control lists (NACLs), or equivalent.

23.1.2. Firewall policies, or equivalent.

23.1.3. Security groups, or equivalent.

23.1.4. IP whitelists, or equivalent

23.1.5. A multi-tier architecture that prevents direct access to data stores from the internet.

23.1.6. Usage of role-based access controls (RBAC) shall be implemented to ensure appropriate access to networks

23.1.7. Two-factor authentication for remote access shall be implemented using appropriate access control best practices.

23.2. Firewalls, routers, and access control lists, or equivalent access controls, shall be used to regulate network traffic for connections to/from the Internet or other external networks, as follows:

23.3. Configuration standards shall be established and implemented.

23.4. Access control policy shall limit inbound and outbound traffic to only necessary protocols, ports, and/or destinations.

23.5. Internal IP address ranges shall be restricted from passing from the Internet into the DMZ or internal networks.

23.6. All inbound internet traffic shall terminate in a DMZ.

23.7. Only IT approved connections shall be allowed into eConnect networks.

23.8. The use of all services, protocols, and ports allowed to access eConnect networks shall be reviewed on a periodic basis, at a minimum every twelve (12) months, for appropriate usage and control implementation.
23.9. All internet facing rule set modifications shall be reviewed and approved by the Information Security Department prior to implementation.
23.10. Direct access between the Internet and any system containing PII shall be prohibited.
23.11. Network equipment shall be configured to close inactive sessions.
23.12. Remote access servers shall be placed in the firewall DMZs.
23.13. Network intrusion detection systems (IDS) shall be implemented as needed and monitored by IT.

24. Routers, Hubs and Switches

24.1. LAN equipment, hubs, bridges, repeaters, routers and switches shall be kept in physically secured facilities.
24.2. Network equipment access shall be restricted to appropriate Personnel only. Other staff and contractors requiring access are required to be supervised.
24.3. Network equipment access shall occur over encrypted channels as defined in the Data Protection & Encryption Policy and Encryption and Key Management Policy. Access via unencrypted protocols (http, telnet, ftp, tftp) shall not occur. Unused channels shall be disabled.
24.4. Wireless access points and controllers shall not be allowed to connect to the production subscriber network.
24.5. Unnecessary protocols shall be removed from routers and switches.

25. Cabling & Physical Infrastructure

25.1. Network cabling shall be documented in physical and/or logical network diagrams.
25.2. All unused network access points shall be disabled when not in use.
25.3. Storing or placing any item on top of network cabling shall be avoided.
25.4. Redundant cabling schemes shall be used whenever possible.
25.5. Secure, encrypted VPN connections to other networks controlled by eConnect or outside entities, when required, shall be approved by Information Security.
25.6. Configuration of routers and switches shall be documented and aligned with industry best practice. This shall include changing any vendor-supplied defaults (passwords, configurations, etc.) before installing in production.
25.7. End-of-life and/or unsupported network devices shall not be used and, if discovered, removed from the network as soon as possible.

26. Wireless Network Security

26.1. Wireless networks shall be encrypted as typical in best practices and by eConnect's Policy.

26.2. Access to wireless networks shall be restricted to only those authorized, as follows:

26.2.1. Guest Network: Accessible by guests with appropriate employee approval or employees with minimal web-filtering in place (no direct access to corporate/production network).

26.2.2. Extranet Network: Only accessible by approved employee owned devices with minimal web-filtering in place (no direct access to corporate/production network)

26.2.3. Corporate Network: Only accessible by eConnect owned devices with controlled ingress/egress and web filtering (no direct access to the production network).

26.2.4. Personnel and authorized third parties are not allowed to install unauthorized wireless equipment.

26.2.5. All Wi-Fi bridges, routers and gateways shall be physically secured.

26.2.6. SSIDs and default usernames and passwords shall be modified or removed prior to implementation in a production environment.

27. Clock Synchronization

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

28. Test, Development and Production Environments

28.1. Test software upgrades, security patches and system and software configuration changes before deployment, including but not limited to the following:

28.1.1. Validate proper error handling.

28.1.2. Validate secure communications.

28.1.3. Validate proper role-based access control (RBAC).

28.1.4. Performance impact

28.2. Development, test, and production environments shall be segregated.

28.3. Separation of duties shall exist between development, test, and production environments.

28.4. Do not use Personal Data and PII for testing and/or development, and only use false/synthetic data (preferred) or Deidentified and strongly Pseudonymised Data for testing and/or development..

28.5. Remove test data and accounts before production systems become active.

28.6. Follow change control procedures for all changes to system components. The procedures shall include testing of operational functionality.

29. Development & Source Code

29.1. Manage all code through a version control system to allow viewing of change history and content.

29.2. Ensure that a test engineering (i.e. quality assurance (QA)) methodology is followed using a multi-phase quality assurance release cycle that includes security testing.

29.3. Deliver security fixes and improvements aligning to a predetermined schedule based on identified severity levels.

29.4. Perform vulnerability testing as a component of QA testing and address any severity 2 or higher findings prior to software release.

29.5. Ensure that software is released only via production managed change control processes, with no access or involvement by the development and test teams.

29.6. 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:

- 29.6.1. Injection
- 29.6.2. Broken Authentication
- 29.6.3. Sensitive Data Exposure
- 29.6.4. XML External Entities (XXE)
- 29.6.5. Broken Access Control
- 29.6.6. Security Misconfiguration
- 29.6.7. Cross-Site Scripting (XSS)
- 29.6.8. Insecure Deserialization
- 29.6.9. Using Components with Known Vulnerabilities
- 29.6.10. Insufficient Logging & Monitoring

29.7. Awareness training regarding secure coding shall be conducted at least once per calendar year. The curriculum shall be approved by Information Security.

30. Transfer of Information

30.1. To protect the confidentiality of PII in transit:

- 30.1.1. Ensure that all data in transit is either encrypted and/or the transmission channel itself is encrypted following Data Encryption Policy.
- 30.1.2. Monitor all data exchange channels to detect unauthorized information releases.
- 30.1.3. Use Information Security approved security controls and data exchange channels.

31. Data Classification, Labeling, and Handling

31.1. Data classification, labelling and handling policies shall be put in place in order to ensure that data is appropriately handled (e.g. Data Security and Privacy Statement, Data Classification Policy, etc.)

31.2. Strict control over the storage and accessibility of media that contains Personal Data shall be maintained.

31.3. Properly maintain inventory logs of all media and conduct media inventories at least annually.

31.4. Destroy media containing Personal Data when it is no longer needed for business or legal reasons by following procedures including, but not limited to:

31.5. Disposal of media containing Personal Data so that it is rendered unreadable or undecipherable, such as by burning, shredding, pulverizing, or overwriting. Media sanitization processes shall be implemented following best practices.

31.6. Disposal logs that provide an audit trail of disposal activities shall be securely maintained. Disposal logs will be kept for a minimum of ninety (90) days.

31.7. Certificates of destruction shall be maintained for at least one year.

32. Messaging Security

32.1. All incoming email shall be scanned for viruses, phishing attempts, and spam.

32.2. Outgoing email shall have data loss prevention (DLP) monitoring in place.

32.3. Any messaging service shall be approved by Information Security prior to usage and shall include appropriate audit trails and encryption of data at rest and in transit. Data loss prevention (DLP) tools and processes shall be implemented, where possible.

33. Removable Media

33.1. All removable media brought in from outside eConnect shall be scanned for viruses/malware prior to use. Any identified malware/viruses shall be removed with the assistance of End User Support prior to use.

33.2. Personal Data is prohibited on any kind of removable device, unless the device is approved and documented by the eConnect IT team (support@eConnect.com) and is encrypted following Data Protection & 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 Employee Handbook and Data Security and Privacy Statement, to mitigate the risk of a Data Breach.

33.3. Individuals in sensitive positions, with access to Personal Data, SCI or Subscriber Data, shall not store such data on removable media, unless required by their role

and approved by Information Security and Privacy in accordance with best practices.

33.4. In the rare event that physical media containing Personal Data and PII is approved for use in accordance with this Section 25, the Privacy team will document the applicable details, including the type of physical media, the authorized sender/recipients, the date and time, the number of physical media, and the type of encryption used

34. Inventory Management

34.1. An inventory of all computer equipment and software in use throughout eConnect shall be maintained.

34.2. Computer hardware and software audits shall be periodically carried out. Audits shall also be used to track:

34.2.1. Unauthorized copies of software

34.2.2. Unauthorized changes to hardware and software configurations

34.2.3. Accuracy of current inventory

35. Background Checks

35.1. Where required and/or permitted by applicable local law, eConnect will conduct a pre-employment background and/or criminal records check on all new hires. Employment at eConnect is contingent upon a satisfactory background and/or criminal records check, including where applicable:

35.1.1. Social Security number trace.

35.1.2. Education.

35.1.3. Work Experience.

35.1.4. Criminal Background Check.

35.1.5. Credit Check, if relevant to the position.

35.1.6. Reference Check.

35.2. Where required and/or permitted by applicable local law, eConnect may also conduct background and/or criminal records checks on its employees throughout the course of their employment. Generally, this will occur in circumstances involving transfer to a position of high-level security or responsibility.

36. Vendor/Partner Risk Management

36.1. Vendor and partner risk management policies and processes shall be defined to verify that vendors comply with eConnect' security and policies.

36.2. Vendor and partner contracts shall include language requiring adherence to eConnect' security and privacy policy requirements or their equivalent.

36.3. Critical vendors shall be reviewed at least once per calendar year, to ensure continued alignment with eConnect security and privacy policies.

37. Print Management

37.1. When Confidential Data, including Personal Data, SCI, PII or Subscriber Data is printed to centralized printers secure print or equivalent shall be used, where a PIN is required at the printer before the document is printed.