iCIMS, Inc.

INFORMATION SECURITY
IT SECURITY POLICY

Policy Document

Contents

1. Policy Statement

This policy addresses iCIMS, Inc. ("iCIMS") protection of Subscriber Data and protected information as identified in the Data Security & Privacy Statement (DSPS) and Incident Response Process.

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 DSPS. It is designed to provide a consistent application of security policy and controls for iCIMS and all iCIMS customers. Customization of these policies on a per-customer basis is generally not allowed, except for product security control configurations that can be customized, often by the customer, to customer needs.

Protection of iCIMS 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.

As with all iCIMS policies, failure of iCIMS personnel to follow the policy requirements shall result in disciplinary action, up to and including termination.

Printed documents are uncontrolled. Refer to Promapp for controlled versions.

2. Terms & Definitions

Term/Acronym	Definition
Access Control	The process of limiting access to the resources of a system only to authorized users, programs, processes, or other systems.
Anonymized Data	Data that has been produced as the output of a PII anonymization process.
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 completion.
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, which is enforced by Access Control.
Data Breach	*Refer to iCIMS Incident Response Policy & Process*
Deidentified Data	Information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular individual, provided that an organization that uses Deidentified Data: (1) has implemented technical safeguards that prohibit reidentification of the individual to whom the information may pertain; (2) has implemented processes that specifically prohibit reidentification of the information; (3) has implemented processes to prevent inadvertent release of Deidentified Data; and (4) makes no attempt to reidentify the information.
De-Militarized Zone (DMZ)	A physical or logical subnetwork that contains and exposes an organization's externally 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 usernames.
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 iCIMS information security management systems (ISMS).
IT Administrator	Individual responsible for the upkeep, configuration, security, and reliable operation of computer systems.
IT Department	Departments within iCIMS responsible for the management of IT systems, including servers, workstations, mobile devices, and network infrastructure.
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.
Personal Data	*Refer to iCIMS Incident Response Process*
Personal Identifiable Information (PII)	*Refer to iCIMS 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.
Private Branch Exchange (PBX)	Small telephone exchange used internally within a company.
Pseudonymized Data	Process applied to PII which replaces identifying information with an alias.
Security Event	*Refer to iCIMS Incident Response Process*
Security Incident	*Refer to iCIMS Incident Response Process*
Security Incident Response Team (SIRT)	*Refer to iCIMS Incident Response Process*
Security Vulnerability	*Refer to iCIMS Incident Response Process*
Security Weakness	*Refer to iCIMS 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 (SCI)	Means any record, whether in paper, electronic, or other form, that includes any one or more of the following elements in relation to iCIMS 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 iCIMS'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 must be anonymous as to the current or past employee/intern, must not reasonably be linked back to a current or past employee/intern, and must not contain any Personal Data.
Subscriber Data	*Refer to iCIMS Subscription Agreement.*
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 later.
Wide Area Network (WAN)	A telecommunications network or computer network that extends over a large geographical distance.

3. Ownership & Administration

This IT Security Policy is owned and administered by iCIMS Information Security Department.

4. Applicability

This policy applies to all systems, including network equipment and communication systems, supporting iCIMS internal and remote operations and products and services. These policy requirements supersede all other policies, processes, practices, and guidelines relating to the matters set forth herein, except for the Data Security and Privacy Statement and Incident Response Policy & Process. However, additional policies shall be put in place that document enhanced requirements when such policy requirements are considered confidential. For example, policies that address the specifics of key management. These policies will be reviewed at least once per calendar year and updated to meet current best practice.

iCIMS uses reasonable efforts to protect the security and privacy of all information received by, though or on behalf of iCIMS. 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.

5. SECURITY POLICIES

1. Data Protection & Encryption Policy

1.1. 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.

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

1.2. 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.

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

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

1.5. 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.

1.6. Encryption of wireless networks shall be enabled using the following encryption levels, while separating the networks based on the type of device being used:

1.6.1 Corporate owned:
- Network Access: All corporate plus Internet
- Authentication 802.1x + AES (MFA)

1.6.2 Corporate owned (generic, such as video kiosks):
- Network Access: Only Internet
- Authentication: MAC (WPA2 PSK)

1.6.3 Employee Bring Your Own Device (BYOD):
- Network Access: Only Internet
- Authentication: 802.1x + AES

1.6.4 Guest BYOD:
- Network Access: Only Internet
- Authentication: MAC with captive portal

1.6.5 Any wireless network encryption requirements that cannot be addressed by the identified device types above must be reviewed and approved by Information Security.

1.7. Personal Data, PII, SCI or Subscriber Data shall not be stored on equipment that is not owned or managed by iCIMS, Inc.

1.8. Data shall be transferred only for the purposes determined/identified in iCIMS's Data Security & Privacy Statement.

1.9. Documented policies and process shall be implemented to ensure appropriate encryption and key management is in place, including periodic key rotation.

1.10. If you are unsure regarding the level of required encryption or specific encryption policies, you shall contact Information Security for guidance and approval.

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

2. Password Policy

2.1. Unless otherwise specified within this IT Security Policy, NIST 800-63b standards will be followed when managing passwords. As such, the following security requirements shall be adhered to when creating passwords:

2.1.1 Minimum of eight (8) characters in length. If unable to follow NIST 800-63b standards, which do not require complexity standards, passwords should include the following three categories:

2.1.1.1. English uppercase characters (A through Z)

2.1.1.2. English lowercase characters (a through z)

2.1.1.3. Base 10 digits (0 through 9)

2.1.2. NIST 800-63b does not required complexity standards, but where possible the use of non-alphabetic characters (e.g., !, $, #, %) is recommended.

2.1.3. Passwords history shall be kept for the previous six (6) passwords and passwords shall be unique across the password history.

2.1.4. NIST 800-63b does not required periodic password resets. However, where NIST 800-63b cannot be applied maximum password age should be ninety (90) days.

2.1.5. Shall not be the same as or include the user id.

2.1.6. Passwords shall not be visible by default when entered, but in alignment with NIST 800-63b can be visible when typing where possible and password “Paste-In” should be allowed.

2.1.7. Passwords shall not be easily guessable.

2.1.8. Set first-time passwords to a unique value for each user and change immediately after the first use.

2.1.9. User accounts shall be locked after seven (7) incorrect attempts.

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

2.1.10. 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.

2.1.11. Password hints should not be used, in compliance with NIST 800-63b.

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

2.2.1. Verify user identity before performing password resets.

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

2.2.3. 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.

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

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

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

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

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

2.2.9. 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 Data Protection & Encryption Policy (*refer to policy #1*) and access restricted accordingly.

2.2.10. Default passwords on systems must be changed after installation.

2.2.11. Render all passwords inaccessible during transmission using encryption as defined in Data Protection & Encryption Policy (*refer to policy #1*).

2.2.12. Passwords shall be protected in storage by hashing following Data Protection & Encryption Policy (*refer to policy #1*).

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

2.2.14. In alignment with NIST 800-63B, breached passwords should be monitored, and mandatory password changes should occur if a password breach is identified, or the user suspects their password may have been compromised.

3. Authorized Software Policy

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

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

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

3.4. Workstation configurations or build standards defined by the IT Department in alignment with Information Security policies 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.

3.5. 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.

3.6. Software that is end-of-life and no longer supported is considered unauthorized software.

4. Physical Security Policy

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

4.2. Personnel and authorized third parties shall ensure that SCI, PII, PI, and customer data are only recreated in hardcopy format where absolutely needed for an identified purpose and are appropriately secured.

4.3. All Personnel and authorized third parties shall follow clean desk/clean screen best practices, especially when stepping away from workspaces.

4.4. 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:

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

4.4.1.1. Store video for at least ninety (90) days, unless otherwise required by law.

4.4.2. Restriction of unauthorized access to network access points.

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

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

4.4.5. 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.

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

4.4.7. Ensure that any physical access required by NKPs are supervised.

4.4.8. All visitors shall log in and receive the appropriate access card, as necessary, and identifying badge.

4.4.9. Any paper and electronic media that contain Subscriber Data, PII, SCI or Personal Data shall be physically secured.

4.4.10. Doors to physically secured facilities shall always be kept locked.

4.5. <u>Power Availability</u>

4.5.1. All servers are required to use universal power supplies (UPS).

4.5.2. All hubs, bridges, repeaters, routers and switches and other critical network equipment shall be UPS protected.

4.5.3. Sufficient power availability shall be in place to keep the network and servers running until the Disaster Recovery Plan can be implemented.

4.5.4. UPS software shall be installed on all servers to implement an orderly shutdown in the event of a total power failure.

4.5.5. All UPSs shall be periodically tested.

4.5.6. Emergency generators shall be in place and tested periodically to ensure that the operate properly for production data centers.

4.5.7. Fuel delivery services shall be in place to ensure the continued operation of emergency generators.

4.6. Environmental Protection

4.6.1. Consideration shall be taken to ensure environmental concerns are addressed such as fire, flood, and natural disaster (e.g., earthquake, flood, etc.)

4.6.2. Redundant air conditioning units shall be in place to ensure maintenance of appropriate temperature and humidity in the data center.

4.7. Data centers shall be required to perform SOC 2 or equivalent audits on an annual basis and vendors shall be required to remediate any findings in a reasonable timeframe.

5. Business Continuity and Disaster Recovery Policy

5.1. Disaster recovery plans support Subscriber business continuity plans and shall be in place and tested on a regular basis as set forth in the Support & Maintenance Policy ("SMP").

5.2. A business continuity plan that considers information security requirements shall be implemented and tested at least once per calendar year.

6. Backup Policy

6.1. 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 Support and Maintenance Policy (“SMP”) and iCIMS Data Retention Policy.

6.2. All backups shall be encrypted following Data Protection & Encryption Policy (*refer to policy #1*) for data at rest and in transit.

6.3. Backups shall be encrypted and stored in a physically and logically secure geographically separate location

6.4. 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.

7. Virus and Malware Protection Policy

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

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

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

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

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

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

7.7. 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.

7.8. 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.

7.9. Users or Subscriber's impacted by virus related security incidents shall be notified as soon as reasonably possible in alignment with Incident Response Procedures.

7.10. Potential virus and malware infections shall be immediately reported to Information Security and escalated to the Security Incident Response Team (SIRT).

8. Access Control Policy

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

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

8.3. The IT Department shall be notified of all personnel leaving iCIMS's employ by Talent (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.

8.4. Administrators shall only log into systems with user ids attributable to them or follow processes that would not break attribution. For example, administrators shall use the su command to obtain root privileges, rather than login as root onto UNIX or Linux systems.

8.5. 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.

8.6. 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).

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

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

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

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

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

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

8.9.2.2. 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.

8.9.3. 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).

8.9.4. Inactive user accounts reviewed and disabled and/or remove at least every ninety (90) days. Exceptions shall be documented, reviewed, and approved by Information Security.

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

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

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

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

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

8.9.10. 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.

8.10. Remove external access to subscriber databases immediately upon notification that subscriber has terminated their relationship with iCIMS.

8.10.1. Remove subscriber databases from system within thirty (30) days of subscriber termination.

8.10.2. Overwrite or destroy all subscriber backup data within twelve (12) months of the subscriber's termination date.

8.11. Access to the Internet and other external services shall be restricted to authorized parties only based on the assigned role.

8.12. Revalidation timeouts for SaaS products and services used by iCIMS personnel must be set to 12 hours or less, in compliance with NIST 800-63b.

9. Auditing, Logging, and Monitoring Policy

9.1. 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.

9.2. Secure audit trails shall be protected so they cannot be altered.

9.3. Central repositories of security related logs shall be administered and managed by the Information Security Department.

9.4. 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.

9.5. Intrusion detection and logging systems shall be implemented to detect unauthorized access to the networks.

9.6. 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.

9.7. Auditing features on wireless access points and controllers shall be enabled, if supported, and resulting logs shall be reviewed periodically Information Security.

9.8. All external ingress/egress connections shall be logged.

9.9. Logs shall be retained for one year.

9.10. The following automated audit trails shall be implemented for all system components to reconstruct the following events:

9.10.1. All individual accesses to PII.

9.10.2. Actions taken by any individual with root or administrative privileges.

9.10.3. Access to controlled audit trails.

9.10.4. Invalid logical access attempts.

9.10.5. Use of identification and authentication mechanisms.

9.10.6. Initialization of/changes to system logging.

9.10.7. Creation and deletion of system-level objects.

9.11. Record at least the following audit trail entries for all system components for each event:

9.11.1. User identification.

9.11.2. Type of event.

9.11.3. Date and time.

9.11.4. Success or failure indication.

9.11.5. Identity or name of affected data, system component, or resource.

9.12. Viewing of audit trails shall be limited to those with a job-related need.

9.13. 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.

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

10. Vulnerability Management Policy

10.1. An independent third party 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:

10.1.1. Network-layer/infrastructure penetration tests.

10.1.2. Application-layer penetration tests.

10.1.3. Mobile application penetration testing

10.1.4. Attestation of successful completion, including the remediation status of any findings.

10.2. Perform internally conducted internal and external vulnerability tests at least quarterly. Ensure findings are addressed in a timely manner.

10.3. Address newly identified threats and vulnerabilities on an ongoing basis based on severity and skill level required to take advantage of the identified vulnerability.

10.4. Ensure the following are implemented:

10.4.1. Static code testing

10.4.2. Dynamic code testing of the test and production environment

10.4.3. Manual testing after any significant changes

10.4.4. 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.

10.4.5. Processes to ensure identified vulnerabilities are addressed in a timely manner, based on risk.

10.4.5.1. 30 days for high-risk critical and/or security vulnerabilities

10.4.5.2. 14 days for zero-day vulnerabilities.

11. Security Awareness, Vulnerabilities, Weaknesses, Events, and Incidents Policy

11.1. 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:

11.1.1. Security awareness training shall be given at the first onboarding session attended by new employees (usually within two weeks of employment)

11.1.2. Specialized training shall be given to key stakeholders (i.e., incident reporting and management, ISO 27001, security policy and process, assessment response best practice, phishing, etc.)

11.2. Identified Security Weaknesses or Security Vulnerabilities shall be immediately reported to the Information Security.

11.3. Unless authorized by the Information Security Department, at no time shall an attempt be made to take advantage of any Security Weakness or Security Vulnerability.

11.4. Security Weaknesses or Vulnerabilities that have been compromised could trigger a Security Event. Security Events shall be analyzed by the Information Security to

determine whether they are considered Security Incidents, which are required to be addressed in accordance with the Incident Response Procedures.

12. Audit and Assessments Policy

12.1. An Independent Party shall verify iCIMS's compliance with the IT Security Policy through periodic audits, at least once per calendar year.

12.2. iCIMS will maintain ISO 27001 certification, or equivalent, ensuring that iCIMS information security management system (ISMS) continues to perform in alignment with the standard.

12.3. Data center providers shall have SOC 2 audits performed at least once per calendar year.

12.4. Customers can perform reasonable security assessments once per calendar year, following industry best practice.

12.5. Customer audits are generally not allowed, due to confidentiality, complexity, and resource requirements. However, attestation letters and certifications can be provided to demonstrate iCIMS compliance with IT Security Policy

13. Server Security Policy

13.1. Servers shall be physically secured.

13.2. All administrative access shall be encrypted in adherence with iCIMS's Data Protection & Encryption Policy (*refer to policy #1*).

13.3 Access via unencrypted protocols (i.e Telnet / FTP) is not allowed without prior Information Security approval.

13.4. Limit the number of concurrent administrative connections to two (2), where possible.

13.5. Only one (1) primary function per server shall be implemented, where possible.

13.6. Server administrators shall be limited to one primary administrator and two backup administrators, where feasible. Exceptions shall be approved by Information Security.

13.7. Information Security shall be informed and approve access in cases where no other method of attributable accessibility is available.

13.8. End-of-life and/or end-of-support servers shall not be used and, if discovered, removed from the network as soon as possible.

13.9. Define and implement server build standards that include, at a minimum, the following:

13.9.1. Hardening based on industry best practice (i.e. CIS standards)

13.9.2. Host based intrusion detection (HIDS)/ File integrity Management (FIM)

13.9.3. Anti-virus/anti-malware

13.9.4. Centralized logging configuration

13.9.5. Security Incident Event Management (SIEM)

14. Patch Management Policy

14.1. Server operating systems shall be patched within 30 days of a critical and/or security patch release.

14.2. Workstations and Laptops shall be patched within 30 days of a critical and/or security patch release.

14.3. Network devices shall be patched within 30 days of the release of a critical and/or security patch.

14.4. 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.

14.5. Patches shall be tested prior to rollout in the production environment. Less critical systems shall be patched first.

14.6. Failure to patch within defined timelines could result in disciplinary action, up to and including termination.

15. Endpoint Security Policy

15.1. Users shall shutdown, logout or lock workstations when leaving them for any length of time.

15.2. Workstations and laptops shall be restarted periodically.

15.3. Workstations and laptops shall adhere to Virus and Malware Protection Policy (*refer to policy #7*).

15.4. Define and implement endpoint build standards that include, at a minimum, the following:

15.4.1. Defined configurations based on industry best practice.

15.4.2. Authorized software

15.4.3. Anti-virus/anti-malware

15.4.4. Web Filtering/Cloud Access Security Broker (CASB)

15.4.5. Security Incident Event Management (SIEM) agents (e.g. Rapid7 IDR)

15.5. Workstation access to the Internet shall be controlled based on assigned or departmental role.

16. Mobile Computing Policy

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

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

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

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

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

16.5. Devices owned by personnel or authorized parties are not allowed to connect to corporate or production networks.

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

17. Network Security Policy

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

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

17.1.2. Firewall policies, or equivalent.

17.1.3. Security groups, or equivalent.

17.1.4. IP whitelists, or equivalent.

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

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

17.1.7. Two-factor authentication for remote access shall be implemented as defined in the Access Control Policy (*refer to policy #8*).

17.2. 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:

17.2.1. Configuration standards shall be established and implemented.

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

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

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

17.2.5. Only IT and Information Security approved connections shall be allowed into iCIMS networks.

17.2.6. The use of all services, protocols, and ports allowed to access iCIMS networks shall be reviewed on a periodic basis, at a minimum every six (6) months, for appropriate usage and control implementation.

17.2.7. All internet facing rule set modifications shall be reviewed and approved by the Information Security Department prior to implementation.

17.2.8. Direct access between the Internet and any system containing PII shall be prohibited.

17.3. Network equipment shall be configured to close inactive sessions.

17.4. Remote access servers shall be placed in the firewall DMZs.

17.5. Network intrusion detection systems (IDS) shall be implemented and monitored by Information Security.

17.6. <u>Routers, Hubs and Switches</u>

17.6.1. LAN equipment, hubs, bridges, repeaters, routers, and switches shall be kept in physically secured facilities.

17.6.2. Network equipment access shall be restricted to appropriate personnel only. Other staff and contractors requiring access are required to be supervised.

17.6.3. Network equipment access shall occur over encrypted channels as defined in the Data Protection & Encryption Policy (*refer to policy #1*).

17.6.4 Access via unencrypted protocols (http, telnet, ftp, tftp) shall not occur. Unused channels shall be disabled.

17.6.5. Wireless access points and controllers shall not be allowed to connect to the production subscriber network.

17.6.6 Unnecessary protocols shall be removed from routers and switches.

17.8. Cabling

17.8.1. Network cabling shall be documented in physical and/or logical network diagrams.

17.8.2. All unused network access points shall be disabled when not in use.

17.8.3. Storing or placing any item on top of network cabling shall be avoided.

17.8.4. Redundant cabling schemes shall be used whenever possible.

17.9. Secure, encrypted VPN connections to other networks controlled by iCIMS or outside entities, when required, shall be approved by Information Security.

17.10. Configuration of routers and switches shall be documented and align with industry best practice. This shall include changing any vendor-supplied defaults (passwords, configurations, etc.) before installing in production.

17.11. End-of-life and/or unsupported network devices shall not be used and, if discovered, removed from the network as soon as possible.

18. Wireless Network Security Policy

18.1. Wireless networks shall be encrypted as defined by iCIMS's Data Protection & Encryption Policy (*refer to policy #1*).

18.2. Access to wireless networks shall be restricted to only authorized devices. Any SSID can be used as long at the appropriate device and access and authentication types are utilized. Wireless network configuration should be as follows:

1.6.6 Corporate owned:

- Network Access: All corporate plus Internet
- Authentication 802.1x + AES (MFA)

1.6.7 Corporate owned (generic, such as video kiosks):

- Network Access: Only Internet
- Authentication: MAC (WPA2 PSK)

1.6.8 Employee Bring Your Own Device (BYOD):

- Network Access: Only Internet
- Authentication: 802.1x + AES

1.6.9 Guest BYOD:

- Network Access: Only Internet
- Authentication: MAC with captive portal

1.6.10 Any wireless network encryption requirements that cannot be addressed by the identified device types above must be reviewed and approved by Information Security.

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

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

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

19. Clock Synchronization Policy

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

20. Test, Development and Production Environments Policy

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

20.1.1. Validate proper error handling.

20.1.2. Validate secure communications.

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

20.1.4. Performance impact

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

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

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

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

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

21. Software Development Policy

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

21.2. 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.

21.3. Deliver security fixes and improvements aligning to a pre-determined schedule based on identified severity levels.

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

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

21.6. 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:

21.6.1.1. A1:2017- Injection

21.6.1.2. A2:2017- Broken Authentication

21.6.1.3. A3:2017- Sensitive Data Exposure

21.6.1.4. A4:2017- XML External Entities (XXE)

21.6.1.5. A5:2017- Broken Access Control

21.6.1.6. A6:2017- Security Misconfiguration

21.6.1.7. A7:2017- Cross-Site Scripting (XSS)

21.6.1.8. A8:2017- Insecure Deserialization

21.6.1.9. A9:2017- Using Components with Known Vulnerabilities

21.6.1.10. A10:2017- Insufficient Logging & Monitoring

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

22. Transfer of Information Policy

22.1. To protect the confidentiality of PII in transit:

22.1.1. Ensure that all data in transit is either encrypted and/or the transmission channel itself is encrypted following Data Protection & Encryption Policy (refer to policy #).

22.1.2. Monitor all data exchange channels to detect unauthorized information releases.

22.1.3. Use Information Security approved security controls and data exchange channels.

23. Data Classification, Labeling, and Handling Policy

23.1. Data classification, labelling and handling polices 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.)

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

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

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

23.4.1. 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 the NIST 800-88 standard, where possible.

23.4.2. 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.

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

24. Messaging Security Policy

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

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

24.3. 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.

25. Removable Media Policy

25.1. All removable media brought in from outside iCIMS 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.

25.2. Personal Data is prohibited on any kind of removable device unless the device is approved and documented by Information Security and the iCIMS Privacy team (privacy@icims.com) and is encrypted following Data Protection & Encryption Policy (*refer to policy #1*). 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.

25.3. 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 Paragraph 25.2.

25.4. 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

26. Voice System Security Policy

26.1. When applicable, the default and maintenance passwords on the voice system shall be changed to user defined passwords that meet iCIMS's Password Policy (*refer to policy #2*).

26.2. Call accounting shall be used to monitor access and abnormal call patterns and misuse.

26.3. Separate internal and external call forwarding privileges shall be in place to prevent inbound calls being forwarded to an outside line.

26.4. Use of MFA or an access pin with a minimum length of six (6) digits shall be used for critical voice mail accounts.

26.5. Do not match voice mail access pins to the last six (6) digits of the phone number.

26.6. Lock out the caller to a voice mail account after three (3) attempts at pin validation.

27. Inventory Management Policy

27.1. An inventory of all computer equipment and software in use throughout iCIMS shall be maintained.

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

27.2.1. Unauthorized copies of software

27.2.2. Unauthorized changes to hardware and software configurations

27.2.3. Accuracy of current inventory

28. Background Check Policy

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

28.1.1. Social Security number trace.

28.1.2. Education.

28.1.3. Work Experience.

28.1.4. Criminal Background Check.

28.1.5. Credit Check, if relevant to the position.

28.1.6. Reference Check.

28.2. Where required and/or permitted by applicable local law, iCIMS 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.

29. Vendor/Partner Risk Management Policy

29.1. Vendor and partner risk management policies and process shall be defined to verify that vendors and partners comply with iCIMS' security and policies.

29.2. Vendor and partner contracts shall include language requiring adherence to iCIMS' security and privacy policy requirements, or their equivalent.

29.3. Mission critical vendors / sub-processors shall be reviewed at least once per calendar year, to ensure continued alignment with iCIMS security and privacy policies.

30. Print Management Policy

30.1. 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.