Daily Operating Policies

Normal day to day operating policies.

- Acceptable Encryption Policy
- Acceptable Use Policy
- Acquisition Assessment Policy
- Audit Logging Standard
- Basic - Precision Computer Recycling Authorization Form
- Bluetooth Baseline Requirements Policy
- Change Management Policy
- Clean Desk Policy
- Client Data Management Policy
- Client Onboarding and Offboarding Policy
- Client System Access Control Policy
- Data Breach Response Policy
- Data Protection, Storage, and Recovery Policy
- Digital Signature Acceptance Policy
- Email Policy
- End User Encryption Key Protection Policy
- Ethics Policy
- Hardware, Media Management, and Data Destruction Policy
- HIPAA Media Destruction SOP (Step-by-Step)
    - HIPAA Media Destruction SOP
    - HIPAA_Media_Destruction_Form
- HIPAA_Data_Recovery_SOP

    - HIPAA_Data_Recovery_Form
    - HIPAA_Data_Recovery_SOP

- HIPPA - Precision Computer Recycling Authorization Form
- Incident Management Policy
- Lab Security Policy
- Multi-Tenancy Security Policy
- Password Construction Guidelines
- Password Protection Policy
- Remote Access Policy
- Remote Access Tools Policy
- Router and Switch Security Policy
- Secure Database Credential Handling Policy
- Server Security Policy
- Service Level Agreement (SLA) Management Policy / Framework
- Software Installation Policy
- Technology Equipment Disposal Policy
- Third-Party / Vendor Risk Management Policy
- Verify Technicians on Arrival
- Web Application Security Policy
- Wireless Communication Policy
- Wireless Communication Standard
- Workstation Security (For HIPAA) Policy

Acceptable Encryption Policy

1.0 Purpose

The purpose of this policy is to establish standards for the use of cryptographic algorithms and technologies within the organization. This policy aims to ensure that only strong, publicly vetted encryption algorithms are employed to protect the confidentiality and integrity of organizational data. It also serves to provide guidance regarding compliance with applicable regulations, particularly concerning the implementation and potential export of encryption technologies.

2.0 Scope

This policy applies to all employees, contractors, vendors, and affiliates of the organization involved in the selection, implementation, or management of systems or processes that utilize encryption for protecting organizational data.

3.0 Policy Statements

The following standards define the acceptable use of encryption algorithms within the organization:

3.1 Approved Encryption Algorithms

* Encryption algorithms used for protecting organizational data must be selected from internationally recognized, publicly reviewed, and currently accepted standards.
* Proprietary or non-standard encryption algorithms are prohibited unless explicitly reviewed, approved, and formally excepted by the designated IT authority (e.g., Precision Computer team) based on a thorough security assessment.

3.2 Symmetric Encryption

* For symmetric encryption (where the same key is used for encryption and decryption), ciphers must meet or exceed the security level defined as "AES-compatible" or "partially AES-compatible" by relevant industry bodies (e.g., IETF/IRTF guidance) or be approved under current U.S. National Institute of Standards and Technology (NIST) standards, such as FIPS 140-2 (or its successors).
* The use of the **Advanced Encryption Standard (AES)** with appropriate key lengths (e.g., 128 bits or higher, preferably 256 bits for new implementations) is the required standard for symmetric encryption unless a specific, approved exception exists.

3.3 Asymmetric Encryption

* For asymmetric encryption (using public/private key pairs), algorithms must meet the standards defined in NIST FIPS 140-2 (or its successors).
* The use of **RSA** (with key lengths of 2048 bits or higher, 3072 bits recommended for new

implementations) or **Elliptic Curve Cryptography (ECC)** (using NIST-approved curves like P-256 or higher) is required for asymmetric encryption. Secure padding schemes (e.g., OAEP for RSA) must be employed.

3.4 Hash Functions

* Cryptographic hash functions used for integrity checks, digital signatures, or other security functions must adhere to current NIST guidance (e.g., the NIST Policy on Hash Functions).
* Algorithms such as SHA-256, SHA-384, SHA-512, or newer SHA-3 family algorithms are required. The use of deprecated algorithms like MD5 or SHA-1 for security purposes is prohibited.

3.5 Digital Signature Algorithms

* Algorithms used for digital signatures must provide an appropriate level of security, corresponding to the requirements for asymmetric encryption and hash functions. Approved algorithms include:
    * **ECDSA** (Elliptic Curve Digital Signature Algorithm) using approved curves (e.g., P-256 or higher). Implementation should consider relevant standards (e.g., RFC6090) to address potential issues.
    * **RSA** (using key lengths specified in section 3.3) with secure padding schemes (e.g., PSS) and appropriate message hashing (as per section 3.4).
    * Other NIST-approved hash-based signature schemes may be considered where appropriate.

3.6 Key Management

* Cryptographic keys must be generated, stored, distributed, rotated, and destroyed securely in accordance with established cryptographic best practices and organizational key management procedures (which may be detailed in a separate Key Management Policy or Standard).

4.0 Compliance

4.1 Compliance Measurement

The designated IT authority (e.g., Precision Computer team) will verify compliance with this policy through various methods, including but not limited to, configuration audits of systems, review of security architecture designs, internal and external security assessments, and analysis of reports from security tools. Feedback will be provided to the policy owner and relevant management.

4.2 Exceptions

Any exception to this policy requires formal, documented justification detailing the business need and compensating controls, and must receive advance approval from the designated IT authority (e.g., Precision Computer team). Approved exceptions will be reviewed periodically.

4.3 Enforcement

Failure to comply with this policy may result in the disabling of non-compliant systems or applications, and may lead to disciplinary action for responsible personnel, up to and including termination of employment or contract, consistent with organizational procedures.

5.0 Referenced Standards and Definitions

*   **NIST FIPS 140-2 (and successors):** U.S. government standard for cryptographic modules.
*   **NIST Policy on Hash Functions:** Guidance on acceptable cryptographic hash algorithms.
*   **AES (Advanced Encryption Standard):** The standard symmetric encryption algorithm.
*   **RSA (Rivest–Shamir–Adleman):** A widely used public-key (asymmetric) algorithm.
*   **ECC (Elliptic Curve Cryptography):** An approach to public-key cryptography based on elliptic curves.
*   **ECDSA (Elliptic Curve Digital Signature Algorithm):** A digital signature algorithm using ECC.
*   **SHA (Secure Hash Algorithm):** A family of cryptographic hash functions (e.g., SHA-256, SHA-512).
*   **Proprietary Encryption:** Encryption algorithms developed privately without public review, generally discouraged due to lack of vetting.

Acceptable Use Policy

1.0 Purpose

This policy outlines the acceptable use of the organization's information technology resources. Its purpose is to ensure these resources are used for legitimate business purposes, to protect employees, partners, and the organization from illegal, damaging, or unethical actions conducted knowingly or unknowingly via these resources, and to safeguard the confidentiality, integrity, and availability of information systems. The organization is committed to a culture of openness, trust, and integrity, and this policy supports these values by defining clear expectations for responsible use. Effective security is a shared responsibility, requiring the participation and support of every user.

2.0 Scope

This policy applies to all employees, contractors, consultants, temporary staff, vendors, agents, and other workers of the organization and its subsidiaries ("Users"). It governs the use of all information, electronic and computing devices, network resources, and systems (including internet, intranet, extranet, email, and cloud services) owned, leased, or managed by the organization, as well as personal or third-party devices when used to conduct organization business or interact with internal networks and business systems.

3.0 Policy Statements

3.1 Ownership and General Use

* All organization-provided IT resources, including computer equipment, software, operating systems, storage media, network accounts, and associated data, are the property of the organization.
* These systems are intended primarily for business purposes in service of the organization's interests and its clients/customers. Limited personal use may be permissible provided it is brief, occasional, does not interfere with work duties, does not consume significant resources, and complies with all organizational policies (including this AUP). Users should have no expectation of privacy when using organizational resources. Refer to Human Resources policies for further details on personal use expectations.
* Users are responsible for exercising good judgment and conducting their activities in accordance with organizational policies, standards, and applicable laws and regulations.

3.2 Security Requirements

* Users must comply with the organization's Password Policy for all system and user-level passwords. Sharing passwords or allowing others (including family members) to use your account is strictly prohibited.

* All computing devices used to access organizational resources must comply with the Minimum Access Policy and relevant workstation security standards.
* Workstations must be secured (screen locked or logged off) when unattended. Password-protected screensavers with an automatic activation of 10 minutes or less are required.
* Users must exercise extreme caution when handling emails or files from unknown senders or unverified sources, particularly regarding opening attachments or clicking links that could contain malware.
* Providing unauthorized access to organizational resources, either deliberately or through failure to secure credentials or devices, is prohibited.

3.3 Proprietary and Confidential Information

* Users must handle proprietary and confidential organizational information appropriately, adhering to the Data Classification Policy and Data Protection Standard.
* When posting to external forums (newsgroups, etc.) from an organizational email address or identifying oneself as affiliated with the organization, users must include a disclaimer stating that the opinions expressed are their own and not necessarily those of the organization, unless the posting is an official duty.
* Providing information about or lists of organizational employees to external parties without authorization is prohibited.

3.4 Unacceptable System and Network Activities

The following activities are strictly prohibited:

* Engaging in any activity that is illegal under local, state, federal, or international law.
* Violating intellectual property rights (copyright, patent, trade secret), including installing or distributing unlicensed ("pirated") software, or unauthorized copying/distribution of copyrighted materials (music, images, text, etc.).
* Introducing malicious software (viruses, worms, Trojan horses, ransomware, spyware) into the network.
* Attempting or effecting security breaches or disruptions:
    * Unauthorized access to data, servers, or accounts.
    * Network sniffing, port scanning, security scanning, packet spoofing, denial-of-service attacks, ping floods, or forging routing information without explicit authorization from the designated IT authority (e.g., Precision Computer).
    * Circumventing user authentication or security measures of any host, network, or account.
    * Monitoring network data not intended for the user's device unless explicitly authorized as part of job duties.
    * Interfering with or denying service to any user or system.
    * Using programs/scripts/commands intended to interfere with or disable another user's session.
* Introducing honeypots, honeynets, or similar unauthorized security-testing technologies onto the network.
* Exporting software or technical information in violation of export control laws. Consult management if unsure.

3.5 Unacceptable Email and Communication Activities

The following activities are strictly prohibited:

* Sending unsolicited bulk email ("spam"), junk mail, chain letters, "Ponzi" or pyramid schemes.
* Engaging in harassment via email, messaging, or other communication channels (based on language, frequency, or message size).
* Unauthorized use or forgery of email header information.
* Soliciting email for addresses other than one's own with intent to harass or collect replies fraudulently.
* Posting the same or similar non-business-related messages to large numbers of newsgroups (newsgroup spam).
* Using organizational resources to procure or transmit material that violates sexual harassment or hostile workplace laws.
* Making fraudulent offers or unauthorized statements about warranties.

3.6 Blogging and Social Media

* All activities on blogs, wikis, social networking sites, and related platforms are subject to this AUP, whether using organizational or personal systems, if the activity relates to the organization or identifies the user as affiliated with it. Refer to the organization's Social Media Policy for detailed guidance.
* Users must not disclose organizational confidential or proprietary information or trade secrets.
* Users must not engage in blogging or social media activities that could harm the organization's reputation or goodwill, or that involve discriminatory, disparaging, defamatory, or harassing content prohibited by other organizational policies (e.g., Non-Discrimination and Anti-Harassment).
* Users must not attribute personal statements, opinions, or beliefs to the organization. If expressing personal opinions while identifying affiliation, clearly state that the views are personal.
* Organizational trademarks, logos, or other intellectual property may not be used in personal blogging or social media activities without authorization.

4.0 Compliance

4.1 Compliance Measurement

The designated IT authority (e.g., Precision Computer team) will verify compliance with this policy through various methods, including but not limited to, monitoring network traffic, reviewing system logs, audits (internal and external), inspection of devices, and analysis of reports from security tools. User activity on organizational resources may be monitored without notice.

4.2 Exceptions

Certain restrictions (e.g., security scanning, network monitoring) may be exempted for specific job responsibilities (e.g., IT system administration) with appropriate authorization. Any other exception to this policy requires formal, documented justification and advance approval from the designated IT authority (e.g., Precision Computer team).

4.3 Enforcement

Violation of this policy may result in disciplinary action, up to and including termination of employment or contract, as well as potential legal action. Access privileges may be restricted or revoked pending investigation.

5.0 Related Policies and Definitions

*   **Related Policies:**
    *   Data Classification Policy
    *   Data Protection Standard
    *   Human Resources Policies (regarding personal use, conduct)
    *   Minimum Access Policy
    *   Non-Discrimination and Anti-Harassment Policy
    *   Password Policy
    *   Social Media Policy
    *   Workstation Security Policy/Standards
*   **Definitions:**
    *   **Blogging:** Writing and publishing posts on a blog (web log).
    *   **Honeypot/Honeynet:** Decoy computer systems set up to attract and detect unauthorized use attempts or malware.
    *   **Proprietary Information:** Information owned by the organization, often confidential, providing a competitive advantage (e.g., trade secrets, internal processes, customer lists).
    *   **Spam:** Unsolicited bulk electronic messages, typically commercial emails.

Acquisition Assessment Policy

1.0 Purpose

The purpose of this policy is to establish the framework and minimum security requirements for assessing and integrating newly acquired companies into the organization's environment. Integrating acquisitions can significantly impact the security posture of both entities due to differences in infrastructure, policies, and culture. This policy aims to manage these risks by defining a process to:

* Assess the acquired company's security landscape, posture, and practices.
* Protect both the parent organization and the acquired company from increased security risks during and after integration.
* Educate the acquired company's personnel on the organization's security policies and standards.
* Facilitate the adoption and implementation of the organization's security policies and standards within the acquired entity.
* Ensure secure integration of networks and systems.
* Establish requirements for ongoing monitoring and auditing post-acquisition.

This policy outlines the responsibilities of the designated IT authority (e.g., Precision Computer Team) and defines the minimum security baseline required before connecting acquired systems or networks to the organization's infrastructure.

2.0 Scope

This policy applies to all corporate acquisitions made by the organization. It pertains to all personnel, systems, networks, data, laboratories, test equipment, hardware, software, and firmware owned and/or operated by the acquired company that will be integrated or connected to the organization's environment.

3.0 Policy Statements

3.1 Acquisition Assessment and Integration Process

* **IT Authority Involvement:** The designated IT authority (e.g., Precision Computer Team) must be an active member of the corporate acquisition team from the outset and throughout the entire process.
* **Risk Assessment:** The IT authority is responsible for conducting thorough security

assessments of the acquired company to identify and evaluate information security risks related to their infrastructure, systems, applications, data handling practices, and overall security posture.
*   **Remediation Planning:** Based on the risk assessment, the IT authority will develop a remediation plan in collaboration with relevant parties from both the organization and the acquired company.
*   **Implementation:** The IT authority will work with the acquisition integration team to implement necessary security controls and remediate identified risks *before* establishing connectivity between the acquired entity's network and the organization's network.

3.2 Minimum Security Requirements for Integration

The following minimum requirements must be met by the acquired company before network integration, unless a formal, risk-accepted exception is granted:

*   **Hosts (Servers, Desktops, Laptops):**
    *   All end-user devices (desktops, laptops) must either be replaced with organization-standard equipment, re-imaged with the organization's standard operating environment build, or demonstrably meet all requirements outlined in the organization's endpoint security standards (e.g., Baseline Workstation Configuration Standard).
    *   All hosts must have organization-approved and updated endpoint protection (anti-virus/anti-malware) software installed and operational before network connection.
    *   Business-critical production servers that cannot be immediately replaced or re-imaged require a specific security audit and a formal waiver granted by the IT authority (e.g., Precision Computer Team). These servers must meet applicable organizational security standards for servers.
*   **Networks:**
    *   Network infrastructure devices (routers, switches, firewalls) within the scope of integration must typically be replaced with organization-standard equipment or reconfigured/re-imaged to meet organization standards.
    *   Wireless network access points must be reconfigured or replaced to comply strictly with the organization's Wireless Network Connection Standard. Unauthorized or insecure wireless networks must be disabled.
*   **Internet Connections:**
    *   Existing direct internet connections of the acquired company must generally be terminated post-integration, with internet access routed through the organization's controlled perimeter.
    *   Air-gapped or segmented internet connections required for specific, justified business needs must be reviewed and formally approved by the IT authority (e.g., Precision Computer Team).
*   **Remote Access:**
    *   All existing remote access solutions (VPNs, dial-up, etc.) of the acquired company must be terminated.
    *   Remote access for acquired personnel will be provisioned through the organization's standard, approved remote access solutions and policies.
*   **Laboratory Environments (If Applicable):**
    *   Laboratory networks must be logically and, where appropriate, physically segregated from corporate/production networks, typically using firewalls managed according to organizational standards.
    *   Physical access to lab environments must be secured and restricted based on organizational

physical security policies.
    * Any direct external network connections (e.g., to partners, customers) originating from labs must be reviewed, justified, and approved by the relevant security authority (e.g., Precision Computer Team or a specialized Lab Security Group ["LabSec"], if applicable).
    * All acquired labs must adhere to the organization's specific lab security policies/standards or obtain a formal waiver from the relevant authority ("LabSec" or IT Security).

3.3 High-Risk Acceptance

* In exceptional circumstances where critical business needs necessitate connecting acquired networks or systems that fail to meet these minimum requirements, the associated risks must be formally documented by the IT authority. Connection under such circumstances requires explicit acknowledgment and acceptance of the identified risks by the organization's Chief Information Officer (CIO) or another designated executive sponsor.

4.0 Compliance

4.1 Compliance Measurement

The designated IT authority (e.g., Precision Computer team) will verify the acquired company's compliance with these requirements through audits, configuration reviews, vulnerability scans, interviews, documentation review, and other assessment methods before and during integration. Ongoing compliance will be monitored post-integration.

4.2 Exceptions

As noted in sections 3.2 and 3.3, exceptions to specific requirements require formal documentation, risk assessment, justification, compensating controls (if applicable), and advance approval from the designated IT authority (e.g., Precision Computer team) or, for high-risk acceptance, the CIO.

4.3 Enforcement

Failure to meet these requirements may delay or prevent the integration of the acquired company's networks and systems. Continued non-compliance post-integration may result in disconnection or further remediation actions. Policy violations by personnel may be subject to disciplinary action according to the parent organization's policies.

5.0 Definitions

* **Business Critical Production Server:** A server hosting applications or services whose failure would significantly impact core business operations, revenue generation, or service delivery.
* **Air-gapped:** A security measure where a computer network or device is physically isolated from other networks, particularly unsecured ones like the public internet.

Audit Logging Standard

1.0 Purpose

Comprehensive logging from critical systems, applications, and services is essential for security monitoring, incident response, forensic analysis, and compliance verification. Audit logs provide crucial information about activities performed, potential indicators of compromise, and system behavior. The purpose of this policy is to define the minimum requirements for generating, formatting, storing, and protecting audit logs across the organization's information systems. This ensures that sufficient information is captured to reconstruct events, detect anomalies, investigate security incidents, and meet regulatory obligations. These requirements should guide the configuration of existing systems and serve as baseline criteria for developing or procuring new systems.

2.0 Scope

This policy applies to all production systems, applications, network devices, and services operating on the organization's network, particularly those that handle sensitive or confidential information, accept network connections, perform authentication or authorization functions, or are otherwise deemed critical to business operations or security.

3.0 Policy Statements

All systems and applications within the scope of this policy must be configured to generate and manage audit logs according to the following requirements:

3.1 General Logging Requirement

Systems must record and retain audit log information sufficient to establish accountability and answer key questions about activities performed, including:

* **What** activity occurred?
* **Who/What** performed the activity (subject identity, source system/IP)?
* **On What** was the activity performed (object/target)?
* **When** did the activity occur (timestamp)?
* **With What Tool** was the activity performed (application, utility)?
* **What** was the outcome (status, success/failure)?

3.2 Logged Activities

At a minimum, audit logs must be generated for the following types of activities:

*   **Data Access/Modification:** Creation, reading, updating, or deletion of sensitive or confidential information (including authentication credentials like passwords). Creation, update, or deletion of other significant data.
*   **Network Activity:** Initiation or acceptance of network connections (e.g., firewall logs, server connection logs).
*   **Authentication/Authorization:** User login attempts (success and failure), user logouts, elevation of privileges.
*   **Access Control Changes:** Granting, modifying, or revoking access rights or permissions (e.g., adding/deleting users/groups, changing privilege levels, modifying file/database permissions, altering firewall rules, user password changes).
*   **System/Configuration Changes:** Significant changes to system, network, or service configurations, including installation/removal of software, application of patches/updates, modification of critical configuration files.
*   **Application Lifecycle:** Application process startup, shutdown, restart, abort, failure, or abnormal termination, particularly events related to resource exhaustion (CPU, memory, disk, network) or service failures (DNS, DHCP).
*   **Security Events:** Detection of suspicious or malicious activity by security tools (e.g., Intrusion Detection/Prevention Systems, Anti-Virus/Anti-Malware, File Integrity Monitoring).

3.3 Required Log Content (Log Elements)

Each log entry must contain sufficient detail to meet the requirements in section 3.1. Where possible, log entries should include, directly or indirectly (unambiguously inferred), at least the following elements:

*   **Timestamp:** Accurate date and time of the event, including time zone information or use of Coordinated Universal Time (UTC).
*   **Event/Activity Type:** Clear description of the action performed (e.g., login, read, delete, connect, modify_permission).
*   **Subject Information:** Identity of the user, service, or process performing the action (e.g., User ID, service account name, process ID).
*   **Source Information:** Origin of the activity (e.g., source IP address, source hostname, client application name).
*   **Object Information:** Target of the action (e.g., file path accessed, database record ID, target IP address, target hostname, service modified).
*   **Status/Outcome:** Indication of success or failure of the action.
*   **Reason Codes (if applicable):** For denied actions, codes or descriptions explaining the reason for denial (e.g., invalid password, insufficient permissions).
*   **Before/After Values (if feasible):** For update actions on critical data elements, logging the value before and after the change.
*   **System/Service Identifier:** Clear identification of the system, application, or service generating the log entry.

(Standardization of identifiers like usernames and IP addresses across logs is crucial for effective correlation.)

3.4 Log Formatting, Storage, and Protection

*   **Integrity:** Logs must be generated and stored in a manner that prevents unauthorized modification or deletion. Write-once media, secure append-only modes, digital signing, or forwarding to a secure, centralized logging system are required.
*   **Centralization:** Logs from systems within scope should be forwarded in near real-time to the organization's centralized log management system (e.g., SIEM - Security Information and Event Management).
*   **Standard Formatting:** Systems should support logging in a standardized, well-documented format suitable for parsing and analysis by the centralized log management system. Acceptable mechanisms include:
    *   Microsoft Windows Event Logs (forwarded securely).
    *   Syslog (using secure protocols like TLS-encrypted syslog or reliable syslog variants).
    *   Database logging (to tables within an ANSI-SQL compliant database that is itself securely logged).
    *   Other industry-standard formats compatible with the organization's SIEM (e.g., CEF, LEEF, JSON formats).
*   **Retention:** Audit logs must be retained according to the organization's Record Retention Schedule and relevant regulatory/compliance requirements, both online (in the SIEM) for analysis and offline (archived securely) for long-term storage.
*   **Access Control:** Access to audit logs must be restricted to authorized personnel on a need-to-know basis.

4.0 Compliance

4.1 Compliance Measurement

The designated IT authority (e.g., Precision Computer team, Information Security, Internal Audit) will verify compliance with this policy through various methods, including configuration audits, review of log content and coverage, testing log forwarding mechanisms, reviewing SIEM integration, internal/external audits, and assessing incident response capabilities reliant on logs.

4.2 Exceptions

Any exception to this policy (e.g., for legacy systems unable to meet specific requirements) requires formal, documented justification, risk assessment outlining compensating controls, and advance approval from the designated IT authority (e.g., Precision Computer team or Information Security).

4.3 Enforcement

Systems found to be non-compliant with this policy may be required to undergo remediation within a defined timeframe or risk being isolated or removed from the network. Failure by personnel responsible for system administration or development to adhere to this policy may result in disciplinary action, up to and including termination of employment or contract.

5.0 Definitions

*   **Audit Log:** A chronological record of system activities, including events related to security, operations, and data access.
*   **SIEM (Security Information and Event Management):** Technology providing real-time analysis of security alerts generated by applications and network hardware. Combines Security Information Management (SIM) and Security Event Management (SEM).
*   **Syslog:** A standard protocol for sending system log or event messages to a specific server (syslog server).

6.0 Related Policies

*   Information Security Policy (Overall)
*   Data Classification Policy
*   Record Retention Schedule / Policy
*   Incident Response Plan
*   Change Management Policy
*   Secure Development Policy / Standards

Basic – Precision Computer Recycling Authorization Form

Precision Computer Recycling Authorization Form

Owner Information

Owner Full Name: _____

Address: _____

City/State/ZIP: _____

Phone: _____ Email: _____

(Optional) Business/Organization Name: _____

(Optional) Authorized Signer Title: _____

Description of Items to be Recycled (attach list if needed)

[ ] Computer/Desktop [ ] Laptop [ ] Monitor [ ] Printer/Copier/Scanner/Fax

[ ] Phone/Tablet [ ] Cables/Accessories [ ] Keyboards/Mice [ ] Projector

[ ] Server [ ] Networking Gear [ ] Batteries/UPS [ ] External/Internal Hard Drives

Other (list any additional items): _____

Ownership and Authority

I, the undersigned Owner (or authorized agent of the Owner), represent and warrant that:

- I am the lawful owner of the listed items or have full legal authority to dispose of them.

- The items are free of liens or third-party claims unless disclosed in writing.

Authorization and Transfer

I authorize Precision Computer to collect, transport, and recycle (and, where applicable, refurbish, resell, dismantle for parts, or otherwise process) the listed items in accordance with applicable laws and industry standards. I hereby transfer all right, title, and interest in the items to Precision Computer upon pickup/drop-off. Items and components will not be returned; disposition decisions are final.

Data-Bearing Devices

I understand items may contain data (e.g., computers, phones, drives). I consent to data destruction procedures used by Precision Computer and release Precision Computer from liability for any data remaining after reasonable, commercially accepted data destruction practices.

Hazardous/Prohibited Materials

I confirm the items do not contain prohibited or hazardous materials except as disclosed in writing. Precision Computer may refuse any item at its discretion.

Release and Indemnity

To the fullest extent allowed by law, I release and hold harmless Precision Computer, its employees, and agents from claims arising out of the removal, transport, processing, or recycling of the items, and I waive and disclaim any and all damages of any kind (including direct, indirect, incidental, consequential, special, exemplary, or punitive damages) arising from or related to the items after transfer, the services provided, or any disposition decisions, except to the extent caused by Precision Computer’s willful misconduct or gross negligence.

Compliance and Records

Precision Computer will handle items in compliance with applicable laws and may use certified downstream recyclers. Certificates of recycling or data destruction (if requested and offered) will be provided after processing.

Signatures

Owner/Authorized Agent (print): _____

Signature: ..... Date: ___/___/____

If signing for a business, Title: _____

Accepted by Precision Computer Representative (print): _____

Signature: ..... Date: ___/___/____

Bluetooth Baseline Requirements Policy

1.0 Purpose

The proliferation of Bluetooth-enabled devices presents potential security risks if connections are not properly secured. Insecure Bluetooth usage can expose organizational devices and networks to unauthorized access, data leakage, or malware introduction. The purpose of this standard is to establish minimum security requirements for the use of Bluetooth technology with organization-owned devices or when connecting to the organization's network, ensuring sufficient protection for organizational data, including Personally Identifiable Information (PII) and other confidential information.

2.0 Scope

This standard applies to all employees, contractors, vendors, and other personnel utilizing any Bluetooth-enabled device (whether organization-owned or personal) that connects to organization-owned equipment (e.g., laptops, mobile phones) or directly interacts with the organization's network infrastructure.

3.0 Policy Statements

The following minimum standards must be adhered to when using Bluetooth technology in conjunction with organizational resources:

3.1 Approved Bluetooth Versions

* Unless a formal exception is granted in advance by the designated IT authority (e.g., Precision Computer Team), only Bluetooth devices meeting the Bluetooth Core Specification version 2.1 + EDR (Enhanced Data Rate) or higher are permitted for use with organization equipment or networks.
* Devices purchased prior to the implementation date of this standard may be exempt from the minimum version requirement but must comply with all other aspects of this standard. However, upgrading legacy devices is strongly encouraged.

3.2 Secure Pairing Procedures

* **Pairing Location:** Initial pairing of Bluetooth devices (establishing a trusted connection) should only be performed in a private, secure location to prevent unauthorized observation or interception of pairing codes (PINs) or processes. Avoid pairing devices in public areas.
* **PIN Security:** Use strong, non-default PINs for pairing whenever possible. Do not use easily

guessable PINs like "0000" or "1234".
* **Unsolicited Pairing Requests:** If a device prompts for pairing or requests a PIN unexpectedly after the initial secure pairing has been completed, *do not* accept the request. This could indicate an attempted security compromise. Report such incidents immediately to the IT Help Desk for investigation by the designated IT authority (e.g., Precision Computer Team).

3.3 Discoverability (Visibility)

* Bluetooth devices should be set to "non-discoverable" or "hidden" mode whenever Bluetooth functionality is not actively needed for pairing or connection establishment. This limits the ability of unauthorized devices to detect their presence.

3.4 Unused Connections

* Disable Bluetooth functionality on organizational devices when it is not actively required for business purposes to reduce the potential attack surface.
* Regularly review the list of paired devices on organizational equipment and remove any devices that are no longer needed or recognized.

4.0 Compliance

4.1 Compliance Measurement

The designated IT authority (e.g., Precision Computer Team) may verify compliance with this standard through various methods, including device configuration audits, security scans (where feasible), and investigation of reported incidents.

4.2 Exceptions

Any exception to this standard (e.g., use of older Bluetooth versions for specific legacy equipment) requires formal, documented justification and advance approval from the designated IT authority (e.g., Precision Computer Team).

4.3 Enforcement

Failure to comply with this standard may result in the disabling of Bluetooth functionality on organizational devices or other corrective actions. Violations may also lead to disciplinary action, up to and including termination of employment or contract, consistent with organizational procedures.

5.0 Definitions

* **Bluetooth:** A short-range wireless technology standard used for exchanging data between fixed and mobile devices over short distances.
* **Pairing:** The process of establishing a trusted, authenticated connection between two Bluetooth devices, often involving the exchange or confirmation of a PIN.
* **PIN (Personal Identification Number):** A numeric or alphanumeric code used in some

Bluetooth pairing processes for authentication.
*   **Discoverable Mode:** A Bluetooth setting that allows a device to be detected by other nearby Bluetooth devices scanning for connections.

Change Management Policy

1.0 Purpose

This policy establishes the standard process for managing all changes to client IT environments and services managed by Precision Computer. Unauthorized or poorly managed changes can lead to service disruptions, security vulnerabilities, and client dissatisfaction. The purpose of this policy is to ensure that all changes are requested, assessed, approved, implemented, and reviewed in a controlled manner to minimize risk, avoid negative impacts on service quality and security, and maintain clear communication with clients.

2.0 Scope

This policy applies to all changes made by Precision Computer personnel or systems to client-owned or client-managed IT infrastructure, applications, configurations, or services under a management agreement. This includes, but is not limited to, hardware modifications, software installations/upgrades, operating system patching, configuration changes (network, server, application), security control adjustments, and implementation of new services or features. It covers all personnel involved in requesting, planning, approving, implementing, and reviewing changes to client environments.

3.0 Policy Statements

3.1 Change Management Principles

* All changes to client environments must follow this documented Change Management process.
* Changes must be assessed for potential impact on service availability, security, performance, and compliance.
* Changes must be appropriately authorized before implementation.
* Changes must be scheduled and communicated effectively to minimize disruption to client operations.
* All changes must be logged, tracked, and reviewed.

3.2 Change Types

Changes are categorized based on risk, impact, and urgency:

* **Standard Changes:** Low-risk, pre-authorized changes that are common, follow a documented procedure, and have minimal impact (e.g., password reset for a client user, approved software installation via RMM). Standard changes follow an expedited approval workflow defined by the Change Manager/Authority.
* **Normal Changes:** Changes that are not Standard or Emergency. They require formal risk assessment, planning, and approval through the full Change Advisory Board (CAB) process or

delegated authority based on impact.
*   **Emergency Changes:** Changes required to restore service during a critical incident or address an immediate, significant security vulnerability. These changes require expedited approval but must be fully documented, reviewed, and potentially validated retrospectively.

3.3 Change Management Process

All Normal and Emergency changes must follow these steps (Standard changes follow a defined, expedited subset):

1. **Request for Change (RFC) Submission:** Changes must be formally requested via the [MSP Name] ITSM system, detailing the change description, justification/business need, affected client(s) and Configuration Items (CIs), proposed implementation plan, risk/impact assessment, backout plan, and requested schedule.
2. **Review and Assessment:** The RFC is reviewed by the Change Manager or designated authority. A technical and business impact assessment is performed, evaluating risks, resource requirements, potential conflicts, and alignment with client configurations and agreements.
3. **Approval:**
    *   Approval is required based on the change type, risk, and impact. This may involve the requester's manager, technical subject matter experts, the Change Manager, the Change Advisory Board (CAB), and **crucially, client approval** as stipulated in the service agreement or based on the change's potential impact.
    *   The CAB (composed of representatives from technical teams, service delivery, security, and potentially account management) reviews and approves/rejects Normal changes with significant potential impact.
    *   Emergency changes require approval from authorized emergency approvers (e.g., senior management, designated on-call manager) but must still be logged.
4. **Scheduling:** Approved changes are scheduled in coordination with the client (considering business hours, maintenance windows defined in SLAs) and added to the change calendar to avoid conflicts.
5. **Implementation:** The change is implemented according to the approved plan by authorized technical personnel.
6. **Testing and Validation:** Post-implementation testing is performed to verify the change was successful and did not negatively impact related services. Client validation may be required.
7. **Closure and Review:** The RFC is updated with implementation details, test results, and closure status. Failed or problematic changes trigger backout procedures or incident management. The CAB may review implemented changes, especially Emergency changes or those with issues.

3.4 Roles and Responsibilities

*   **Change Requester:** Any authorized individual initiating a change request.
*   **Change Implementer:** Authorized technical personnel responsible for carrying out the change.
*   **Change Approver(s):** Manager(s), CAB members, Client contacts (as required), or designated authorities responsible for authorizing changes.
*   **Change Manager:** Oversees the change management process, facilitates CAB meetings,

manages the change schedule, and ensures policy adherence.
* **Change Advisory Board (CAB):** A group responsible for assessing, prioritizing, and authorizing significant Normal changes.
* **Client Contact:** Designated client representative(s) involved in approving or being notified of changes as per the service agreement.

3.5 Client Communication and Approval

* Communication with the client regarding planned changes (especially Normal and Emergency changes) is mandatory.
* Notification methods, timelines, and required approval levels will be governed by the client's Service Level Agreement (SLA) and the nature/impact of the change.
* Precision Computer must obtain explicit client approval for changes where contractually required or where the change significantly impacts client operations, cost, or risk posture.
* A forward schedule of change, including approved client maintenance windows, must be maintained and communicated appropriately.

4.0 Compliance

4.1 Compliance Measurement: Compliance will be measured through audits of RFC records in the ITSM system, review of CAB meeting minutes and approvals, analysis of change success rates, tracking of unauthorized changes identified during incident investigation, and client feedback.
4.2 Exceptions: Deviations from the standard process (e.g., for Emergency Changes) must be documented within the RFC and reviewed retrospectively by the Change Manager or CAB. Other exceptions require explicit approval from the Change Manager or designated senior management.
4.3 Enforcement: Implementing unauthorized changes or repeatedly failing to follow the change management process may result in disciplinary action, up to and including termination. Unauthorized changes causing client outages or security incidents will be treated as serious violations.

5.0 Related Policies

* Incident Management Policy (Client Focus)
* Service Level Agreement (SLA) Framework / Specific Client SLAs
* Client Communication Protocols
* Configuration Management Policy / CMDB Procedures
* Risk Management Policy
* Security Patch Management Policy
* Audit Logging Standard
* Problem Management Policy

6.0 Definitions

* **Change:** The addition, modification, or removal of anything that could have an effect on IT services delivered to a client.
* **Request for Change (RFC):** A formal proposal for a change to be made, including details of the proposed change.

*   **Configuration Item (CI):** Any component or asset that needs to be managed in order to deliver an IT service (e.g., server, router, application, documentation).
*   **Change Advisory Board (CAB):** A group of people that supports the assessment, prioritization, authorization, and scheduling of changes.
*   **IT Service Management (ITSM):** The entirety of activities performed by an organization to design, plan, deliver, operate and control IT services offered to customers.
*   **Backout Plan:** A documented plan detailing the steps required to restore a system or service to its original state if a change fails or causes unacceptable issues.

Clean Desk Policy

1.0 Purpose

This policy establishes the minimum requirements for maintaining a secure workspace environment, commonly referred to as a "clean desk." A clean desk practice is a critical control for protecting sensitive and confidential information (in both physical and electronic formats) from unauthorized access, disclosure, or loss. It helps reduce the risk of security breaches, increases awareness about information protection responsibilities, and supports compliance with information security standards (such as ISO 27001) and privacy regulations. The goal is to ensure that sensitive or critical information pertaining to the organization, its employees, customers, vendors, and intellectual property is appropriately secured when unattended or at the end of the workday.

2.0 Scope

This policy applies to all employees, contractors, consultants, temporary staff, and affiliates of the organization working within organizational facilities or handling organizational information assets.

3.0 Policy Statements

All individuals subject to this policy are required to adhere to the following clean desk practices:

3.1 Securing Workstations and Electronic Media

*   **Lock Workstations:** Computer workstations must be locked (e.g., using Ctrl+Alt+Del or Win+L) whenever the workspace is unoccupied, even for short periods.
*   **End-of-Day Shutdown:** Computer workstations should typically be logged off or shut down at the end of the workday, unless specific instructions are provided by IT for maintenance purposes.
*   **Secure Laptops and Portable Devices:** Laptops and other portable computing devices (e.g., tablets) must be physically secured using a locking cable or stored in a locked drawer or cabinet when unattended and at the end of the workday.
*   **Secure Removable Media:** Mass storage devices (e.g., USB drives, external hard drives, CDs, DVDs) containing sensitive or confidential information must be treated as sensitive and secured appropriately, typically by storing them in a locked drawer or cabinet when not in use.

3.2 Securing Physical Documents and Materials

*   **Clear Desks:** Sensitive or confidential documents (Restricted or Sensitive information as per the Data Classification Policy) must be removed from the desk surface and secured in a locked drawer, cabinet, or other approved secure container when the workspace is unoccupied and always at the end of the workday.
*   **Lock Cabinets:** File cabinets and drawers containing sensitive or confidential information must be kept closed and locked when not in direct use or when unattended.

*   **Secure Keys:** Keys used to access cabinets or drawers containing sensitive or confidential information must not be left unattended at a desk or in an unsecured location.
*   **Printer/Fax Output:** Printouts and faxes, especially those containing sensitive or confidential information, should be retrieved immediately from printers, copiers, and fax machines to prevent unauthorized viewing or removal.
*   **Secure Disposal:** Documents containing sensitive or confidential information must be disposed of properly using designated secure methods, such as official shredder bins or locked confidential disposal bins. They should not be placed in regular trash receptacles.
*   **Whiteboards:** Whiteboards containing sensitive or confidential information should be erased when the information is no longer needed or when the workspace will be left unattended.

3.3 Password Security

*   Passwords must never be written down and left in an accessible location, such as on sticky notes attached to monitors, under keyboards, or in unlocked drawers. Refer to the Password Policy for secure password management practices.

4.0 Compliance

4.1 Compliance Measurement

The designated authority (e.g., Precision Computer team, Facilities Security, Internal Audit) will verify compliance with this policy through various methods, including but not limited to, periodic physical walk-throughs of workspaces, awareness checks, audits, and review of security incident reports.

4.2 Exceptions

Any exception to this policy requires formal, documented justification based on business needs and must be approved in advance by the designated authority (e.g., Precision Computer team or relevant department manager). Compensating controls may be required.

4.3 Enforcement

Failure to adhere to this policy may result in disciplinary action, up to and including termination of employment or contract, consistent with organizational procedures and the severity of the violation. Repeated non-compliance may lead to removal of access privileges.

5.0 Related Policies

Users should also be familiar with policies related to:

*   Data Classification Policy
*   Password Policy
*   Information Handling Policy
*   Workstation Security Policy

Client Data Management Policy

1.0 Purpose

This policy defines the principles, responsibilities, and mandatory procedures for the secure handling, processing, storage, protection, retention, and disposal of all data belonging to or entrusted by clients to Precision Computer. As a Managed Service Provider (MSP), safeguarding the confidentiality, integrity, and availability of client data is paramount. This policy ensures that client data is managed responsibly throughout the service lifecycle, complying with contractual obligations, regulatory requirements, and industry best practices.

2.0 Scope

This policy applies to all Precision Computer employees, contractors, consultants, temporary staff, and authorized third parties who access, process, store, transmit, or otherwise handle client data in any format (electronic or physical). It covers all client data residing on Precision Computer systems, client systems managed by Precision Computer, third-party cloud services used by Precision Computer for service delivery, and any physical media containing client data.

3.0 Policy Statements

3.1 Data Classification and Ownership

* Client data is owned by the respective client. Precision Computer acts as a data processor or custodian based on contractual agreements.
* Client data must be treated as, at minimum, Confidential information according to Precision Computer's internal Data Classification Policy, unless explicitly classified otherwise by the client in writing or by contractual agreement. Specific regulatory requirements (e.g., for PHI, PII, CUI) may impose higher classification and handling standards, which must be strictly adhered to.

3.2 Data Access Control

* Access to client data must be strictly controlled based on the principle of least privilege and role-based access control (RBAC). Personnel shall only be granted access to the specific client data necessary to perform their assigned job duties related to service delivery for that client.
* Access requests must be formally documented and approved by designated authorities.
* Access privileges must be reviewed regularly (e.g., quarterly) and revoked immediately upon termination of employment, change in job role, or conclusion of the need for access.
* Authentication for access to systems handling client data must comply with the Precision

Computer Password Policy and Client System Access Control Policy, including mandatory Multi-Factor Authentication (MFA) where applicable.

3.3 Data Segregation

* Client data must be logically (and where feasible or required, physically) segregated from the data of other clients and from Precision Computer's internal corporate data.
* Multi-tenant systems used for service delivery must employ robust technical controls to ensure strict data isolation between tenants (clients).

3.4 Data Protection (In Transit and At Rest)

* Client data must be protected using strong encryption mechanisms both at rest (when stored on servers, backups, laptops, mobile devices) and in transit (when transmitted over internal or public networks).
* Encryption methods must comply with the Precision Computer Acceptable Encryption Policy.
* Physical media containing client data must be physically secured according to the Physical Security Policy.

3.5 Data Handling and Processing

* Client data must only be processed for the specific purposes outlined in the client service agreement.
* Copying or moving client data requires authorization and must be done using secure methods. Storing client data on personal devices or unauthorized cloud services is strictly prohibited.
* Use of client data for testing or development requires explicit client consent and adherence to data masking or anonymization procedures where feasible.

3.6 Data Backup and Recovery

* Client data must be backed up according to schedules and retention periods defined in the client service agreement or associated service descriptions.
* Backup procedures must ensure data confidentiality (e.g., encryption of backups) and integrity.
* Backup media must be stored securely, potentially including offsite storage, as defined by client agreements or internal standards.
* Data recovery procedures must be documented and tested regularly to ensure reliability and meet client Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) where applicable.

3.7 Data Retention and Disposal

* Client data must be retained only as long as necessary to fulfill service obligations, contractual requirements, or legal/regulatory mandates, as defined in client agreements or the Precision Computer Record Retention Schedule.
* Upon contract termination or explicit client request, client data must be securely returned to the client or disposed of according to procedures defined in the Client Onboarding and Offboarding Policy and the Technology Equipment Disposal and Data Sanitization Policy.

*   Secure disposal methods (e.g., cryptographic erasure, physical destruction) must be used to ensure data is irrecoverable. Certificates of destruction may be required.

3.8 Data Sovereignty and Cross-Border Transfer

*   Where applicable based on client location or data type, data sovereignty requirements must be adhered to. Client data may need to reside within specific geographic locations.
*   Transferring client data across borders requires adherence to applicable data privacy regulations (e.g., GDPR, CCPA) and client contractual stipulations.

4.0 Responsibilities

*   **All Personnel:** Responsible for adhering to this policy when handling client data.
*   **Account Managers/Service Delivery Managers:** Responsible for ensuring client contracts accurately reflect data handling requirements and communicating these to relevant teams.
*   **Technical Teams:** Responsible for implementing and maintaining the technical controls required by this policy (access control, encryption, segregation, backup, etc.).
*   **[Designated Authority, e.g., Compliance Officer/Security Team]:** Responsible for overseeing policy compliance, providing guidance, and managing exceptions.

5.0 Compliance

5.1 Compliance Measurement: Compliance will be verified through internal and external audits, review of access logs, assessment of technical controls, review of contractual agreements, and investigation of reported incidents.
5.2 Exceptions: Exceptions require documented justification, risk assessment, client consent where applicable, and approval from the [Designated Authority].
5.3 Enforcement: Violations may result in disciplinary action, up to and including termination, and potential legal liability for Precision Computer and individuals involved.

6.0 Related Policies

*   Data Classification Policy
*   Acceptable Encryption Policy
*   Access Control Policy / Client System Access Control Policy
*   Password Policy
*   Physical Security Policy
*   Backup and Recovery Policy (or sections within this policy)
*   Technology Equipment Disposal and Data Sanitization Policy
*   Client Onboarding and Offboarding Policy
*   Incident Response Policy / Data Breach Response Policy
*   Record Retention Schedule / Policy
*   Multi-Tenancy Security Policy (if applicable)

7.0 Definitions

*   **Client Data:** Any information provided by, created for, or belonging to a client that is accessed, processed, stored, or managed by Precision Computer.
*   **Data Segregation:** The practice of keeping distinct data sets separate, typically preventing data from one client being exposed to another.
*   **Data Sovereignty:** The concept that information is subject to the laws and legal jurisdiction of the country in which it is located.
*   **Least Privilege:** Granting only the minimum permissions necessary for a user or process to perform its function.
*   **Multi-Factor Authentication (MFA):** Authentication requiring more than one verification factor.
*   **Role-Based Access Control (RBAC):** Managing access based on roles and responsibilities rather than individual user identities.

Client Onboarding and Offboarding Policy

1.0 Purpose

This policy defines the standardized processes and security requirements for onboarding new clients into Precision Computer's management and offboarding clients upon termination of the service agreement. A consistent and secure process for both onboarding and offboarding is critical to ensure smooth service transitions, establish necessary security controls, manage access effectively, protect client and Precision Computer data, and meet contractual and legal obligations during these crucial phases of the client lifecycle.

2.0 Scope

This policy applies to all Precision Computer personnel involved in the sales, service delivery, technical support, billing, and administrative functions related to initiating services for new clients and terminating services for existing clients. It covers all technical, administrative, security, and data handling procedures associated with client onboarding and offboarding.

3.0 Policy Statements

3.1 Client Onboarding Process

The onboarding process transitions a new client from sales closure to active service management. Key steps include:

1. **Contract Finalization & Handover:** Ensure service agreements, SLAs, and statements of work (SOW) are finalized and signed. Handoff from Sales to Service Delivery/Onboarding Team.
2. **Information Gathering:** Collect necessary technical details about the client's environment, existing infrastructure, user base, critical applications, third-party vendors, and specific requirements or compliance needs through structured discovery processes (questionnaires, interviews, initial scans).
3. **Account Setup:** Create client records in relevant Precision Computer systems (PSA, RMM, Billing, Documentation Platform).
4. **Credential Establishment:** Securely establish necessary administrative credentials for Precision Computer access to the client environment, adhering to the Client System Access Control Policy (unique credentials, MFA where applicable). Obtain necessary client approvals.
5. **Tool Deployment:** Deploy required Precision Computer management tools (e.g., RMM agents, monitoring tools, security agents) onto client systems according to standard procedures and client agreement.

6. **Baseline Configuration & Assessment:** Perform initial system assessments, apply agreed-upon baseline security configurations (where applicable), and establish initial monitoring and backup configurations based on the SOW.
7. **Documentation:** Document the client's environment, configurations, credentials (securely stored), procedures, and points of contact within the designated Precision Computer documentation platform.
8. **Welcome & Introduction:** Formally introduce the client to support procedures, points of contact, and reporting mechanisms.
9. **Service Activation:** Formally commence service delivery according to the agreed-upon start date.

3.2 Client Offboarding Process

The offboarding process formally concludes the service relationship with a client. Key steps include:

1. **Notification & Planning:** Receive formal termination notice and confirm the final service date. Plan the offboarding timeline and tasks.
2. **Data Return/Destruction:** Execute data handling procedures as defined in the client agreement and the Client Data Management Policy. This includes:
    * Securely returning client-owned data managed by Precision Computer (e.g., backups, cloud data) to the client in an agreed format.
    * Securely sanitizing/destroying any client data residing solely on Precision Computer systems according to the Technology Equipment Disposal and Data Sanitization Policy upon contract termination and confirmation from the client.
3. **Credential Revocation:** Revoke all Precision Computer administrative and user access credentials within the client's environment (e.g., disable service accounts, remove VPN access). This must be coordinated with the client.
4. **Tool Removal:** Uninstall all Precision Computer management tools (RMM agents, monitoring agents, security agents) from client systems, unless contractually agreed otherwise (e.g., client purchases licenses).
5. **Configuration Removal:** Remove client-specific configurations from shared Precision Computer infrastructure (e.g., firewall rules, monitoring checks, backup jobs) after service termination.
6. **Final Reporting:** Provide final service and asset reports to the client as required by the contract.
7. **Final Billing:** Ensure all outstanding service fees are invoiced and processed.
8. **Documentation Archival:** Archive relevant client documentation according to the Record Retention Schedule.
9. **System Deactivation:** Deactivate client records in active Precision Computer management systems (PSA, RMM) after the final offboarding steps are complete.

3.3 Security and Data Handling During Transitions

* All data handling during onboarding (collection) and offboarding (return/destruction) must comply with the Client Data Management Policy.
* All access established during onboarding and removed during offboarding must comply with the

Client System Access Control Policy.
* Secure methods must be used for transferring credentials or sensitive configuration data.

4.0 Responsibilities

* **Sales Team:** Responsible for finalizing contracts and initiating the handover to onboarding teams.
* **Onboarding Team/Project Manager:** Responsible for coordinating and executing the onboarding process according to this policy.
* **Technical Teams:** Responsible for tool deployment, configuration, credential setup, technical assessments during onboarding, and technical removal tasks during offboarding.
* **Account Management/Service Delivery:** Responsible for coordinating offboarding planning, client communication, and ensuring contractual obligations are met during offboarding.
* **Billing/Finance:** Responsible for final billing during offboarding.
* **[Designated Authority, e.g., Security/Compliance Team]:** Responsible for ensuring security requirements are met during both processes.

5.0 Compliance

5.1 Compliance Measurement: Compliance will be verified through audits of onboarding and offboarding checklists/project plans, review of documentation, verification of credential/tool removal, confirmation of data return/destruction, and client feedback.
5.2 Exceptions: Deviations from the standard onboarding/offboarding process require documented justification and approval from designated management (e.g., Service Delivery Manager, Head of Operations).
5.3 Enforcement: Failure to follow the defined onboarding and offboarding procedures may result in service delivery issues, security incidents, contractual breaches, and potential disciplinary action.

6.0 Related Policies

* Client Data Management Policy
* Client System Access Control Policy
* Password Policy
* Remote Access Tools Policy
* Technology Equipment Disposal and Data Sanitization Policy
* Service Level Agreement (SLA) Framework
* Record Retention Schedule / Policy
* Change Management Policy (for changes during onboarding)

7.0 Definitions

* **Onboarding:** The process of integrating a new client into the MSP's service management systems and processes.
* **Offboarding:** The process of formally terminating the service relationship with a client and removing MSP access and tools.
* **PSA (Professional Services Automation):** Software used by MSPs to manage business

operations, including client information, ticketing, billing, and projects.
*   **RMM (Remote Monitoring and Management):** Software used by MSPs to remotely monitor and manage client endpoints and infrastructure.
*   **ITSM (IT Service Management):** The entirety of activities performed by an organization to design, plan, deliver, operate and control IT services offered to customers.

Client System Access Control Policy

1.0 Purpose

This policy defines the mandatory requirements and procedures governing access to client information systems, networks, and data by Precision Computer personnel and systems. Unauthorized or excessive access to client environments represents a significant security risk to both the client and Precision Computer. The purpose of this policy is to ensure that all access to client systems is appropriately authorized, authenticated, logged, monitored, and restricted based on the principle of least privilege, thereby protecting the confidentiality, integrity, and availability of client assets.

2.0 Scope

This policy applies to all Precision Computer employees, contractors, consultants, temporary staff, and authorized third-party service providers who require or are granted access to any client-owned or client-managed IT infrastructure, applications, or data repositories via Precision Computer tools (e.g., RMM, remote access software) or direct login methods. It covers all forms of access, including administrative, user-level, read-only, and automated system access.

3.0 Policy Statements

3.1 Authorization

* Access to client systems must be explicitly authorized based on documented job roles and responsibilities related to specific client service delivery.
* Requests for access must be formally documented, justified by business need (specific client task or support function), and approved by both the relevant Precision Computer manager and, where contractually required, the client contact.
* Access levels must adhere strictly to the principle of least privilege – personnel shall only be granted the minimum level of access necessary to perform their authorized tasks for a specific client.
* Standing privileged access (e.g., Domain Admin) to client environments should be minimized. Privileged access should ideally be granted on a temporary, time-bound, and explicitly authorized basis using Privileged Access Management (PAM) solutions where feasible.

3.2 Authentication

*   **Unique Credentials:** All Precision Computer personnel accessing client systems must use unique, individual credentials. Use of shared accounts for client access is strictly prohibited.
*   **Password Requirements:** Passwords for accounts used to access client systems must comply with the Precision Computer Password Policy and should ideally meet or exceed client-specific password requirements if more stringent.
*   **Multi-Factor Authentication (MFA):** MFA is **mandatory** for all remote access by Precision Computer personnel into client networks or systems. MFA must also be used for accessing any Precision Computer management tool (e.g., RMM, PSA, Cloud Portals) that provides indirect access or control over client systems.
*   **Credential Management:** Credentials used for client access must be stored securely, never embedded in scripts or configuration files in clear text, and managed according to secure practices (e.g., using approved password managers or PAM solutions).

3.3 Access Methods and Tools

*   Access to client systems must only occur via Precision Computer-approved remote access tools and methods, as defined in the Remote Access Tools Policy.
*   Direct connections or use of unapproved tools are prohibited.
*   All remote access sessions must utilize secure, encrypted protocols (e.g., SSH, TLS-encrypted RDP, secure VPN).

3.4 Logging and Monitoring

*   All access attempts (successful and failed) to client systems by Precision Computer personnel or systems must be logged.
*   Logs must capture, at a minimum: timestamp, source IP address, Precision Computer user identity, client system accessed, type of access/protocol used, and session duration (where applicable).
*   Logs related to client system access must be forwarded to Precision Computer's central logging system (SIEM) and retained according to the Audit Logging Standard and potentially client-specific contractual requirements.
*   Logs should be regularly reviewed for anomalous or unauthorized access attempts.

3.5 Access Review

*   Access rights granted to Precision Computer personnel for client systems must be reviewed periodically (e.g., quarterly or aligned with client contract reviews) by designated Precision Computer managers.
*   Reviews must verify the continued need for access and ensure privileges align with the principle of least privilege based on current job roles and client assignments.
*   Client contacts may be involved in the review process as defined by contractual agreements.

3.6 Access Revocation

*   Access to client systems must be revoked immediately upon:
    *   Termination of employment or contract with Precision Computer.
    *   Change in job role eliminating the need for access.

    * Completion of the specific project or task requiring access.
    * Termination of the client service agreement (as part of the offboarding process).
* Revocation procedures must be documented and verifiable.

4.0 Responsibilities

* **All Personnel:** Responsible for adhering to this policy, using unique credentials, enabling MFA, and accessing client systems only via approved methods for authorized purposes.
* **Managers:** Responsible for approving access requests based on business need and least privilege, and for conducting periodic access reviews for their team members.
* **Technical Teams/Access Management:** Responsible for provisioning, modifying, and revoking access based on approved requests, implementing technical controls (MFA, logging), and maintaining access records.
* **[Designated Authority, e.g., Security Team]:** Responsible for overseeing policy compliance, auditing access logs, managing exceptions, and defining approved tools/methods.

5.0 Compliance

5.1 Compliance Measurement: Compliance will be verified through audits of access logs, review of access control lists and group memberships, assessment of MFA implementation, review of access request/approval documentation, periodic access reviews, and investigation of security incidents.
5.2 Exceptions: Exceptions require documented justification, risk assessment, potentially client approval, and explicit approval from the [Designated Authority].
5.3 Enforcement: Unauthorized access attempts, sharing of credentials, bypassing MFA, or other violations may result in disciplinary action, up to and including termination, and potential legal consequences.

6.0 Related Policies

* Remote Access Tools Policy
* Remote Access Policy
* Password Policy
* Audit Logging Standard
* Client Data Management Policy
* Acceptable Use Policy
* Incident Response Policy
* Client Onboarding and Offboarding Policy
* Privileged Access Management Policy (if separate)

7.0 Definitions

* **Client System:** Any IT infrastructure, application, network device, or data repository owned or managed by a client, which Precision Computer personnel access as part of service delivery.
* **Least Privilege:** The security principle of granting only the minimum permissions necessary.
* **Multi-Factor Authentication (MFA):** Authentication requiring more than one verification factor.

*   **Privileged Access Management (PAM):** Solutions and processes for securing, controlling, and monitoring access to critical administrative accounts and credentials.
*   **Remote Monitoring and Management (RMM):** Software platforms used by MSPs to remotely monitor and manage client endpoints and infrastructure.
*   **Role-Based Access Control (RBAC):** Managing access based on roles and responsibilities.

Data Breach Response Policy

1.0 Purpose

This policy establishes the framework and objectives for the organization's data breach response process. It defines the scope of applicability, outlines procedures for suspected or confirmed breaches, clarifies roles and responsibilities, sets standards for incident prioritization, and mandates reporting, remediation, and feedback mechanisms. The purpose is to ensure a coordinated, effective, and timely response to protect the organization's data, personnel, and stakeholders. This policy must be effectively communicated and readily accessible to all personnel involved in data privacy and security protection.

The organization is committed to maintaining a culture of openness, trust, and integrity. This includes a proactive approach to data security and a structured response to potential breaches. This policy aims to protect the organization, its employees, partners, and associated individuals from harm resulting from unauthorized data access or disclosure, whether intentional or unintentional.

2.0 Background

Any individual who suspects that a theft, breach, or unauthorized exposure of the organization's Protected Data or Sensitive Data may have occurred has an immediate obligation to report the incident. Reports should describe the circumstances and be submitted promptly through the designated internal channels (e.g., IT Help Desk email, dedicated phone line, or internal reporting portal). These reporting channels are actively monitored by the designated Information Security personnel or team responsible for initiating investigations. All reports will be investigated to determine if a data breach or exposure has occurred. Confirmed incidents will trigger the established Incident Response Procedure.

3.0 Scope

This policy applies to all employees, contractors, vendors, and partners who collect, access, maintain, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle sensitive or protected information, including Personally Identifiable Information (PII) and Protected Health Information (PHI), on behalf of the organization. Agreements with third-party vendors must include provisions requiring adherence to comparable data protection and breach notification standards.

4.0 Policy: Incident Response Protocol

4.1 Incident Confirmation and Initial Response

Upon confirmation of a theft, data breach, or exposure involving Protected or Sensitive Data, immediate steps will be taken to contain the incident, including isolating affected systems and

revoking access where necessary to prevent further unauthorized activity.

4.2 Incident Response Team Activation

The designated Executive Leader (e.g., Executive Director, Chief Information Security Officer) will activate and chair an Incident Response Team (IRT) to manage the breach or exposure event. The core IRT will be composed of representatives from relevant departments, including:

* IT Infrastructure
* IT Applications / Information Security
* Legal Counsel
* Communications / Public Relations
* Finance (if financial data is impacted)
* Member/Customer Services (if member/customer data is impacted)
* Human Resources
* The business unit(s) directly affected or responsible for the compromised system/data.
* Additional members as deemed necessary by the IRT Chair based on the nature and scope of the incident.

4.3 Investigation and Analysis

The IRT, potentially supported by internal IT and designated external forensic specialists (often coordinated through cyber insurance providers), will conduct a thorough investigation. The objectives are to:

* Determine the root cause of the breach or exposure.
* Identify the specific types of data involved.
* Ascertain the extent of the impact, including the number of individuals and/or organizations potentially affected.
* Assess the scope and severity of the incident.

4.4 Communication Strategy

The IRT, in collaboration with Legal, Communications, and Human Resources departments, will develop and execute a strategic communication plan. This plan will address necessary notifications to:

* Internal personnel
* Regulatory bodies (as required by law)
* Affected individuals
* The public, if deemed necessary.

5.0 Ownership and Responsibilities

* **Data Sponsors:** Individuals or departments with primary responsibility for overseeing specific information resources. Sponsors are typically designated based on administrative roles or their function in collecting, developing, or managing data.

*   **Information Security Administrator/Team:** Designated personnel responsible for the administrative implementation, oversight, and coordination of security procedures and systems, acting in consultation with Data Sponsors.
*   **Users:** All members of the organization community (including staff, contractors, consultants, etc.) with authorized access to information resources. Users are responsible for adhering to security policies and reporting suspected incidents.
*   **Incident Response Team (IRT):** Chaired by Executive Management, this cross-functional team is responsible for managing the response to confirmed data breaches as outlined in section 4.2.

6.0 Enforcement

Violations of this policy by organizational personnel may result in disciplinary action, up to and including termination of employment, subject to applicable laws and internal procedures. Violations by third-party partners may lead to remediation actions, including termination of contracts or network access.

7.0 Definitions

*   **Breach:** The unauthorized acquisition, access, use, or disclosure of Protected Data or Sensitive Data that compromises its security or privacy.
*   **Encryption:** The process of converting data (plain text) into a coded format (ciphertext) requiring a specific key or password for decryption, enhancing data security.
*   **Information Resource:** The data and information assets managed by the organization or its units.
*   **Personally Identifiable Information (PII):** Any information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information.
*   **Protected Health Information (PHI):** As defined under applicable laws (e.g., HIPAA in the US), information relating to health status, healthcare provision, or payment for healthcare that can be linked to a specific individual.
*   **Protected Data:** A collective term referring to PII and/or PHI requiring specific security measures.
*   **Plain Text:** Data that is not encrypted.
*   **Safeguards:** Technical, administrative, and physical controls implemented to protect information resources from threats and minimize security risks.
*   **Sensitive Data:** Data classified by the organization as requiring protection due to its confidential nature, including but not limited to Protected Data.

Data Protection, Storage, and Recovery Policy

1.0 Purpose

The purpose of this policy is to establish guidelines and requirements for the protection, storage, retention, and recovery of the organization's data assets. This policy aims to safeguard sensitive and critical information from unauthorized access, disclosure, modification, loss, or destruction, ensuring data integrity, confidentiality, and availability. It also outlines procedures for preventing data loss and recovering data effectively in the event of an incident.

2.0 Scope

This policy applies to all employees, contractors, consultants, temporary staff, and other agents of the organization who create, access, manage, store, transmit, or dispose of organizational data, regardless of the format (electronic or physical) or location (on-premises or cloud-based). It covers all types of organizational data, including but not limited to customer information, financial records, employee data, intellectual property, and operational data.

3.0 Policy Statements

The following statements outline the specific requirements and guidelines governing data protection, storage, prevention, and recovery within the organization:

3.1 Data Classification

Organizational data must be classified according to its sensitivity and criticality (e.g., Public, Internal, Confidential, Restricted). Data classification levels determine the required security controls for protection, storage, access, and disposal. Detailed data classification guidelines will be maintained separately and made available to relevant personnel.

3.2 Data Protection Measures

* **Access Control:** Access to data shall be granted based on the principle of least privilege, ensuring users have access only to the information necessary to perform their job functions. Robust authentication mechanisms must be employed.
* **Encryption:** Sensitive and confidential data must be encrypted both at rest (when stored) and in transit (when transmitted over networks), using organization-approved encryption standards and tools.
* **Endpoint Security:** All endpoints (desktops, laptops, mobile devices) accessing organizational data must have approved security software installed and maintained, including anti-

malware protection and firewalls, where applicable.
*   **Secure Data Transfer:** Transferring sensitive or confidential data must be done using secure, approved methods (e.g., encrypted email, secure file transfer protocols).
*   **Physical Security:** Physical access to areas where data is stored or processed (e.g., server rooms, file storage areas) must be restricted to authorized personnel.

3.3 Data Storage

*   **Approved Locations:** Organizational data must be stored only on approved systems and platforms (e.g., designated network servers, sanctioned cloud storage services). Storing sensitive or confidential data on personal devices, removable media (unless encrypted and approved), or unauthorized third-party cloud services is prohibited.
*   **Data Minimization:** Only necessary data should be collected and retained. Data should not be stored longer than required for legitimate business or legal purposes.
*   **Secure Disposal:** Data must be disposed of securely when no longer needed, following established procedures that ensure irreversible destruction or deletion, especially for sensitive information and physical media.

3.4 Data Loss Prevention (DLP)

The organization will implement technical and administrative controls to prevent accidental or malicious data loss or exfiltration. This may include DLP software solutions, email content filtering, regular security awareness training for users, and adherence to acceptable use policies. Users are responsible for handling data carefully and reporting any suspected policy violations or security risks.

3.5 Data Backup

*   **Regular Backups:** Critical organizational data must be backed up regularly according to a defined schedule based on data criticality and recovery objectives.
*   **Backup Storage:** Backup copies must be stored securely, with at least one copy maintained in an offsite location to protect against local disasters. Backup media must be protected with appropriate security controls (e.g., encryption, physical security).
*   **Backup Verification:** Backup procedures must include regular testing to verify the integrity of the backups and the ability to restore data successfully.

3.6 Data Recovery

*   **Recovery Procedures:** Documented procedures must be in place for restoring data from backups in the event of data loss, system failure, or disaster. These procedures should align with the organization's Disaster Recovery and Business Continuity Plans.
*   **Recovery Objectives:** Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) should be defined for critical systems and data, guiding backup frequency and recovery priorities.
*   **Incident Response:** Data recovery efforts will be initiated as part of the overall incident response process following a data loss event.

4.0 Roles and Responsibilities

*   **IT Department / Designated Authority:** Responsible for implementing and managing technical controls (security systems, backups, storage infrastructure), developing detailed procedures, and overseeing policy compliance.
*   **Data Owners/Sponsors:** Responsible for classifying data within their purview, defining access requirements, and ensuring appropriate handling according to this policy.
*   **Users:** Responsible for adhering to this policy in their daily work, handling data securely, using approved systems, and reporting incidents or concerns promptly.

5.0 Compliance

5.1 Compliance Measurement

Adherence to this policy will be monitored through various methods, including system audits, security assessments, reviews of access logs, and internal/external audits. The IT Department or designated compliance team (potentially including external partners like Precision Computer where applicable for managed services) will assist in verification activities.

5.2 Exceptions

Any exception to this policy must be formally documented, justified, approved by designated management or the IT Department/Security Team in advance, and regularly reviewed.

5.3 Enforcement

Non-compliance with this policy may result in disciplinary action, up to and including termination of employment or contract termination for third parties, consistent with organizational procedures and applicable regulations.

6.0 Policy Review

This policy shall be reviewed at least annually, or more frequently as needed due to changes in technology, regulations, or business requirements, and updated accordingly.

Digital Signature Acceptance Policy

1.0 Purpose

As electronic communication and documentation become standard practice, digital signatures provide a mechanism for verifying the identity of a sender or signatory and ensuring message/document integrity. The purpose of this policy is to define when digital signatures are considered an acceptable and trusted substitute for traditional handwritten ("wet") signatures for internal organizational documents and correspondence, thereby reducing confusion and standardizing practice.

2.0 Scope

This policy applies to all employees, contractors, consultants, and other agents conducting business on behalf of the organization using organization-issued digital identities (key pairs). This policy specifically governs the use and acceptance of digital signatures on *intra-organizational* documents and correspondence (i.e., communications and documents shared solely within the organization). It does not cover electronic materials sent to or received from external parties unless explicitly stated otherwise in separate agreements or policies.

3.0 Policy Statements

3.1 Acceptance of Digital Signatures

* A digital signature applied using the organization's approved infrastructure and tools is considered an acceptable substitute for a wet signature on any intra-organizational document or correspondence, **except** for specific document types explicitly excluded by the organization.
* An official list of document types requiring traditional wet signatures (not covered by this policy) will be maintained by the designated financial or administrative authority (e.g., the Chief Financial Officer's office) and made available through designated internal resources (e.g., the organization's intranet).

3.2 Signature Validity

* Digital signatures must be associated with an individual user's identity. Digital signatures purporting to represent a role, position, or title (e.g., "Finance Department," "Project Manager") without being tied to a specific individual's key pair are not considered valid under this policy for authentication purposes.

3.3 Responsibilities

The effective use and acceptance of digital signatures rely on specific actions by both the signatory (signer) and the relying party (recipient).

*   **Signer Responsibilities:**
    *   Signers must obtain an official digital signing key pair issued through the organization's designated Identity Management group or process.
    *   This key pair must be generated and managed within the organization's approved Public Key Infrastructure (PKI), with the public key certified by the organization's designated Certificate Authority (CA).
    *   Signers must use only organization-approved software and tools for applying digital signatures.
    *   Signers have a critical responsibility to protect their private key from unauthorized access, loss, or disclosure. The private key must remain secret.
    *   If a signer suspects their private key has been compromised (e.g., stolen, lost, accessed by an unauthorized person), they must *immediately* report the compromise to the designated Identity Management group to initiate key revocation.
*   **Recipient Responsibilities:**
    *   Recipients must use organization-approved software and tools to view digitally signed documents or correspondence and verify the signatures.
    *   Recipients must verify the validity of a digital signature. This includes checking that the signature is cryptographically valid and that the signer's public key certificate was issued by the organization's designated CA and has not expired or been revoked. Verification is typically performed automatically by approved software, but recipients should understand how to check certificate details if needed.
    *   If a digital signature appears invalid, expired, revoked, or associated with an untrusted CA, the recipient must *not* trust the signature or the authenticity/integrity of the document based solely on that signature. Investigate further or request resubmission.
    *   If a recipient suspects misuse or forgery of a digital signature, they must report the concern to the designated Identity Management group or Information Security team.

4.0 Compliance

4.1 Compliance Measurement

The designated IT authority (e.g., Precision Computer team, Information Security, Internal Audit) will verify compliance with this policy through various methods, including audits of the PKI infrastructure, review of approved software lists, investigation of reported incidents, and user awareness checks.

4.2 Exceptions

Any exception to this policy (e.g., temporary use of alternative methods under specific circumstances) requires formal, documented justification and advance approval from the designated IT authority (e.g., Precision Computer team or Information Security).

4.3 Enforcement

Failure to comply with this policy, particularly regarding the protection of private keys or reporting compromises, may result in disciplinary action, up to and including termination of employment or contract. Misuse of digital signatures may lead to revocation of signing privileges and other sanctions.

5.0 Definitions

*   **Digital Signature:** A cryptographic mechanism used to verify the authenticity (originator identity) and integrity (unaltered content) of electronic data.
*   **Public Key Infrastructure (PKI):** A set of roles, policies, hardware, software, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption.
*   **Certificate Authority (CA):** An entity trusted to issue, manage, and revoke digital certificates, which bind public keys to specific identities.
*   **Key Pair:** In asymmetric cryptography, a pair of linked cryptographic keys: a public key (shared openly) and a private key (kept secret by the owner).
*   **Private Key:** The secret component of a key pair used to create digital signatures and decrypt messages encrypted with the corresponding public key.
*   **Public Key:** The publicly shared component of a key pair used to verify digital signatures created with the corresponding private key and encrypt messages for the private key holder.
*   **Wet Signature:** A traditional, handwritten signature on a physical document.

Related Policies:

*   Password Policy / Credential Management Policy
*   Information Handling Policy
*   Acceptable Use Policy
*   (Potentially) Key Management Policy

Email Policy

1.0 Purpose

Electronic mail (email) is a primary communication tool essential for business operations within the organization. However, its misuse can create significant legal, privacy, security, and reputational risks. The purpose of this policy is to ensure the appropriate, secure, and lawful use of the organization's email system. It defines acceptable and unacceptable uses and clarifies user responsibilities regarding email security, content, and retention.

2.0 Scope

This policy applies to all employees, contractors, consultants, temporary staff, vendors, agents, and any other individual ("Users") granted access to the organization's email system. It covers all email sent from or received by an organization-provided email address (@\[organization_domain].com) and the use of organizational email services on any device.

3.0 Policy Statements

3.1 General Use and Expectations

*   **Business Purpose:** The organization's email system is provided primarily for conducting official organizational business.
*   **Limited Personal Use:** Limited, occasional personal use may be permissible provided it does not interfere with job performance, consume significant resources, violate any organizational policies (including the Acceptable Use Policy), or incur costs for the organization. Users should have no expectation of privacy in their use of the organization's email system.
*   **Monitoring:** Use of the organization's email system is subject to monitoring, logging, and review by authorized personnel for security, compliance, and operational purposes, in accordance with applicable laws and organizational policies.

3.2 Security Practices

*   **Account Security:** Users are responsible for safeguarding their email account credentials (passwords) according to the organization's Password Policy. Sharing email account access is prohibited.
*   **Malicious Content:** Users must exercise extreme caution when handling emails from unknown or unverified senders. Do not open unexpected attachments, click suspicious links, or provide sensitive information in response to unsolicited emails. Report suspicious emails (phishing attempts, spam, malware) immediately to the IT Help Desk or designated security contact.
*   **Sending Sensitive Information:** Sending sensitive or confidential organizational data (as defined by the Data Classification Policy) via email requires adherence to the Data Protection Standard, which may include requirements for encryption or use of approved secure file transfer

methods. Avoid sending sensitive data via email unless absolutely necessary and appropriately protected.

3.3 Unacceptable Use

The organization's email system must not be used for activities that violate the law, organizational policies, or ethical standards. Such activities are detailed in the Acceptable Use Policy and include, but are not limited to:

* Sending spam, chain letters, or unauthorized bulk emails.
* Transmitting offensive, harassing, discriminatory, defamatory, or threatening content.
* Distributing malicious software (viruses, worms, etc.).
* Violating copyright or intellectual property laws.
* Engaging in illegal activities or fraudulent schemes.
* Forging email headers or attempting to impersonate others.
* Using email for unauthorized commercial solicitation or outside business activities.

3.4 Representation and Disclaimers

* When sending emails externally, users represent the organization. Ensure communications are professional and appropriate.
* When expressing personal opinions that might be construed as representing the organization, include a disclaimer stating that the views expressed are personal and not necessarily those of the organization (as detailed in the Acceptable Use Policy).

3.5 Email Retention and Business Records

* Email messages should only be retained if they qualify as an official organizational business record needed for legitimate and ongoing business, legal, or regulatory purposes.
* Emails identified as business records must be retained and disposed of according to the official organizational Record Retention Schedule and related policies/procedures. Users may be required to file such emails in designated record-keeping systems.
* Non-record emails (e.g., transitory messages, personal communications) should be deleted regularly to manage mailbox size and reduce data clutter.

4.0 Compliance

4.1 Compliance Measurement

The designated IT authority (e.g., Precision Computer team, Information Security, Internal Audit) will verify compliance with this policy through various methods. These may include monitoring email system usage logs, content filtering, audits (internal and external), investigation of reported incidents, and review of security tool reports.

4.2 Exceptions

Any exception to this policy requires formal, documented justification and advance approval from the designated IT authority (e.g., Precision Computer team or Information Security).

4.3 Enforcement

Violation of this policy may lead to disciplinary action, up to and including termination of employment or contract, suspension or revocation of email access, and potential legal action, depending on the severity of the violation.

5.0 Related Policies

Users should familiarize themselves with the following related organizational documents:

* Acceptable Use Policy (AUP)
* Password Policy
* Data Classification Policy
* Data Protection Standard
* Record Retention Schedule / Policy
* Information Security Policy (Overall)
* Social Media Policy (regarding communication standards)

End User Encryption Key Protection Policy

1.0 Purpose

Effective encryption relies on the secure management of cryptographic keys. Improper handling, storage, or distribution of encryption keys, particularly private keys or symmetric keys, can lead to their compromise, negating the security provided by encryption and potentially exposing sensitive organizational data. While users may understand the need to encrypt data, specific practices for protecting the keys themselves are crucial. This policy outlines the minimum requirements for securely managing and protecting encryption keys under the control of end users to prevent unauthorized disclosure or fraudulent use.

2.0 Scope

This policy applies to all employees, contractors, consultants, and other personnel ("Users") who generate, possess, manage, or use cryptographic keys for organizational business purposes. It specifically covers the management and protection of:

* Encryption keys issued by or on behalf of the organization.
* Encryption keys used for conducting organizational business.
* Encryption keys used to protect data owned by the organization.

This policy applies to both symmetric (secret) keys and the private keys of asymmetric (public-key) key pairs. Public keys contained within digital certificates are generally considered public information and are exempt from the protection requirements outlined herein (though the integrity of certificates is managed via PKI processes).

3.0 Policy Statements

All encryption keys covered by this policy must be protected diligently against unauthorized disclosure, modification, loss, or misuse.

3.1 General Protection Principles

* The level of protection applied to an encryption key must be at least as strong as the protection required for the data it encrypts.
* Keys must be generated, stored, used, and destroyed using organization-approved methods and tools that adhere to cryptographic best practices.

3.2 Symmetric (Secret) Key Management

*   **Distribution:** When symmetric keys must be distributed, the distribution method must be secure. Keys must be encrypted during transit using a strong, approved asymmetric algorithm (referencing the Acceptable Encryption Policy) or an equally strong symmetric algorithm with a key that meets or exceeds the strength of the key being distributed. If distributing keys for the strongest approved algorithm, techniques like key splitting (encrypting portions with different keys and sending via separate channels) should be employed.
*   **Storage:** Symmetric keys, when stored at rest, must be protected using encryption or access control mechanisms at least as stringent as those used for their secure distribution.

3.3 Asymmetric (Public Key) Private Key Management

Asymmetric cryptography uses public/private key pairs. While the public key is shared, the private key must remain confidential and securely managed by the user.

*   **Organization PKI Keys (e.g., on Smart Cards):**
    *   Private keys associated with the organization's Public Key Infrastructure (PKI), often used for digital signatures and encryption, may be generated and stored on secure hardware tokens like smart cards issued to users.
    *   Private keys used *only* for digital signatures (identity certificates) should ideally be non-exportable and remain solely on the hardware token. Escrow of such signing-only private keys is generally not performed and may be technically infeasible or prohibited.
    *   Private keys used for *data encryption* **must** be securely backed up and escrowed according to organizational procedures managed by the designated IT authority (e.g., Precision Computer Team or Identity Management group). This ensures data recovery if the user's key is lost or unavailable. Refer to the organization's Certificate Practice Statement or related documentation for escrow details.
    *   Access to private keys stored on organization-issued hardware tokens (e.g., smart cards) must be protected by a strong PIN or password known only to the user, compliant with the Password Policy. The device/software must require PIN/password entry for each session or operation involving the private key.
*   **Other Software-Generated Keys:**
    *   If key pairs are generated in software (e.g., by an application or browser) and stored as files, the user is responsible for their protection.
    *   The private key file must be protected with a strong password or passphrase compliant with the Password Policy.
    *   Users **must** create at least one secure backup of software-based private keys used for encryption.
    *   Users **must** provide a copy of any software-based private key used for *data encryption* to the designated organizational authority (e.g., local Information Security representative, IT Help Desk) for secure escrow, following established procedures.
    *   Backup and escrow copies must be protected with strong passwords/passphrases compliant with the Password Policy. Storage of escrowed keys by the organization will adhere to requirements in the Certificate Practice Statement or equivalent documentation.
*   **Commercial / External PKI Keys:**
    *   When interacting with external partners requires using keys from commercial CAs (e.g., VeriSign/DigiCert, Thawte) or partner PKIs, these keys are often generated and stored within

software (e.g., a web browser's certificate store).
    * Users must protect access to these software-based key stores with a strong password. Browser or application settings should be configured to require this password upon accessing the private key. Users remain responsible for securely backing up these keys if used for critical data encryption or access. Escrow requirements may apply if used for encrypting organizational data.
* **PGP Keys:**
    * PGP key pairs may be stored in key ring files on a hard drive or preferably on a hardware token (e.g., secure USB drive, smart card).
    * Access to the PGP private key(s) must be protected by a strong passphrase compliant with the Password Policy.
    * PGP software should be configured to require passphrase entry for each use of the private key.

3.4 Hardware Token Security

* Hardware tokens (smart cards, USB tokens, etc.) storing encryption keys are considered sensitive organizational assets.
* They must be physically secured according to the organization's Physical Security policy, especially when outside organizational premises.
* Tokens must not be left unattended or connected to computers when not actively in use.
* When traveling, tokens should ideally be carried separately from the computer they are used with.

3.5 Authentication (PINs, Passwords, Passphrases)

* All PINs, passwords, or passphrases used to protect encryption keys or access to hardware tokens must meet the complexity, length, and management requirements defined in the organization's Password Policy.

3.6 Loss, Theft, or Compromise Reporting

* The loss, theft, or suspected compromise (unauthorized disclosure or access) of any encryption key covered by this policy, or any hardware token containing such keys, **must be reported immediately** to the designated IT authority (e.g., Precision Computer Team or IT Help Desk).
* IT personnel will guide the user through necessary actions, including key/certificate revocation and replacement procedures.

4.0 Compliance

4.1 Compliance Measurement

The designated IT authority (e.g., Precision Computer team, Information Security, Internal Audit) will verify compliance with this policy through various methods, including audits of key management practices, review of PKI configurations, checks on escrow procedures, user awareness assessments, and investigation of reported incidents.

4.2 Exceptions

Any exception to this policy requires formal, documented justification, risk assessment, and advance approval from the designated IT authority (e.g., Precision Computer Team or Information Security).

4.3 Enforcement

Failure to comply with this policy, particularly regarding key protection, escrow, or incident reporting, may result in disciplinary action, up to and including termination of employment or contract. It may also lead to revocation of access privileges or certificates.

5.0 Definitions

* **Certificate Authority (CA):** An entity trusted to issue, manage, and revoke digital certificates.
* **Digital Certificate:** An electronic document binding a public key to an identity (user, device, service), signed by a CA.
* **Digital Signature:** A cryptographic mechanism using a private key to sign data, allowing verification of origin and integrity using the corresponding public key.
* **Hardware Token:** A physical device (e.g., smart card, USB key) used to store cryptographic keys securely and potentially perform cryptographic operations.
* **Key Escrow:** The practice of securely storing a copy of a cryptographic key (typically a private encryption key) with a trusted third party or organizational authority to allow for data recovery.
* **PGP (Pretty Good Privacy):** A popular encryption program providing cryptographic privacy and authentication, often used for email and file encryption.
* **PIN (Personal Identification Number):** A short numeric or alphanumeric code used for authentication, often to access a hardware token.
* **Private Key:** The secret component of an asymmetric key pair.
* **Public Key:** The publicly shared component of an asymmetric key pair.
* **Public Key Cryptography (Asymmetric Cryptography):** A cryptographic system using pairs of keys (public and private).
* **Symmetric Cryptography (Secret Key Cryptography):** A cryptographic system using the same key for encryption and decryption.

6.0 Related Policies

* Acceptable Encryption Policy
* Certificate Practice Statement (or equivalent PKI documentation)
* Password Policy
* Physical Security Policy
* Data Classification Policy
* Information Handling Policy

Ethics Policy

1.0 Purpose

This policy establishes the organization's commitment to upholding the highest standards of ethical conduct in all business practices. It serves as a guide for employees and affiliates, emphasizing the expectation of fairness, honesty, integrity, and trust in all interactions. The purpose is to foster a culture of openness, ensure fair business practices, protect the organization and its stakeholders from impropriety, and guide behavior to align with our core values and legal obligations. Effective ethics is a collective responsibility requiring the active participation and support of everyone associated with the organization.

2.0 Scope

This policy applies to all employees at all levels, directors, officers, contractors, consultants, temporary staff, agents, and other workers conducting business for or on behalf of the organization, including personnel affiliated with third parties when interacting with or representing the organization.

3.0 Policy Statements

3.1 Foundational Principles

* All business conduct must adhere to the highest standards of honesty, integrity, and fairness.
* All interactions, whether internal or external, must be based on mutual respect.
* Compliance with all applicable laws and regulations is mandatory.
* The intent and appearance of unethical or compromising practices must be avoided.

3.2 Leadership Commitment

* Senior leaders and executives must set a clear example of ethical conduct and champion the organization's ethical values.
* Leadership must foster an environment where ethical concerns can be raised without fear of retaliation, maintaining an "open door" approach to suggestions and concerns.
* Executives must promptly disclose any actual or potential conflicts of interest related to their position or responsibilities within the organization.

3.3 Employee Commitment

* Employees are expected to treat colleagues, customers, vendors, and partners fairly and with respect, promoting a positive and collaborative team environment.
* Employees must apply diligence and sound judgment to uphold ethical standards in their daily work.

* Employees must promptly disclose any actual or potential conflicts of interest related to their position or responsibilities.
* Employees contribute to customer and vendor satisfaction by providing quality products/services and responding professionally and promptly to inquiries.
* Employees are encouraged to evaluate the ethics of any situation by considering questions such as:
    * Is it legal and compliant with all organizational policies?
    * Does it reflect the organization's values?
    * Could it negatively impact stakeholders (customers, employees, partners, the organization)?
    * Would I be comfortable if this action appeared in a news headline?
    * Could it harm the organization if everyone acted this way?

3.4 Maintaining an Ethical Culture

* The organization will actively promote ethical conduct and awareness through training, communication, and reinforcement from leadership.
* Open dialogue, honest feedback, and objective treatment are encouraged to support an ethical atmosphere.
* A designated body (e.g., Ethics Committee, Employee Resource Team, HR Department) is established to oversee the communication of this policy, provide guidance, and address concerns related to ethical conduct.

3.5 Conflicts of Interest

* All employees and leaders must avoid situations where personal interests could conflict, or appear to conflict, with the interests of the organization. Full disclosure of any such potential or actual conflicts is required.

3.6 Use of Company Assets and Information

* Organizational assets, resources, and business relationships must not be used for personal gain or unauthorized purposes.
* Unauthorized use, disclosure, or appropriation of confidential or proprietary information (including trade secrets, financial data, source code, personnel information, etc.) is strictly prohibited and will not be tolerated.

3.7 Harassment and Discrimination

* The organization maintains a zero-tolerance policy for harassment or discrimination of any kind. All employees are entitled to a respectful work environment. (Refer to specific Anti-Harassment/Non-Discrimination policies for details).

4.0 Reporting Ethical Concerns

* Employees are encouraged and expected to report any observed or suspected violations of this policy, illegal activities, or unethical conduct.
* Reports can typically be made to an employee's direct manager, the Human Resources

department, or the designated ethics body/contact. (Organizations may also include specific reporting channels like a hotline here).
* The organization prohibits retaliation against any individual who, in good faith, reports an ethical concern or participates in an investigation.

5.0 Training and Acknowledgment

* All employees are required to familiarize themselves with this Ethics Policy.
* Employees will be required to complete periodic ethics training and acknowledge their understanding and compliance with this policy, typically on an annual basis.

6.0 Compliance and Enforcement

6.1 Compliance Measurement

Compliance with this policy will be monitored and verified through various methods, including but not limited to, internal/external audits, review of business practices, investigation of reported concerns, and feedback mechanisms, overseen by the designated authority (e.g., Employee Resource Team, HR, Internal Audit).

6.2 Consequences of Violations

* Any violation of this Ethics Policy is a serious matter and will be addressed promptly.
* Employees found to have violated this policy will be subject to disciplinary action, which may include warnings, reprimands, suspension, or termination of employment, depending on the severity of the violation.
* Violations may also have legal consequences.

7.0 Related Policies

Users should also be familiar with policies related to:

* Code of Conduct (if separate)
* Anti-Harassment and Non-Discrimination Policy
* Conflict of Interest Policy (if separate)
* Information Security / Data Protection Policies
* Acceptable Use Policy
* Whistleblower Policy (if applicable)

Hardware, Media Management, and Data Destruction Policy

Note: Sections labeled [HIPAA] apply when systems/media create, receive, maintain, or transmit ePHI. Otherwise, follow the baseline requirements.

1.0 Purpose

Define secure lifecycle requirements for hardware and removable media and the standards for data sanitization/destruction at transfer, reuse, or end-of-life. [HIPAA] Ensure alignment with HIPAA Security Rule.

2.0 Scope

All company-owned/managed endpoints, servers, network devices with storage, and removable media (USB, external disks, tapes, optical, mobile) across all sites and cloud environments. [HIPAA] Applies to ePHI-capable systems/media.

3.0 Roles and Responsibilities

- **IT Asset Management**: Inventory, custody tracking, disposition coordination.
- **IT Operations**: Deployment, maintenance, incident handling; execute sanitization/destruction.
- **Security**: Policy oversight, audits, exceptions; [HIPAA] Security/Privacy Officer approvals.
- **Employees**: Proper custody and use of assigned devices and media.

4.0 Policy Statements

4.1 Asset Inventory and Ownership
- Maintain CMDB inventory with unique IDs, owner, location, configuration, and data classification.
- Track chain of custody for device/media transfers.
[HIPAA] Retain records relevant to ePHI for ≥ 6 years.

4.2 Procurement and Standard Builds
- Use approved hardware standards and secure images/baselines.
- Enforce full-disk encryption (FDE) on supported devices; enable secure boot and TPM.
[HIPAA] Encrypt ePHI at rest/in transit; implement access controls and audit logging.

4.3 Storage and Physical Security
- Store spares/returned devices in locked cabinets with access logs; use tamper-evident seals for data-bearing items.
[HIPAA] Limit physical access to authorized personnel; maintain access records.

4.4 Removable Media Controls
- Restrict media use to business need; disable by default where feasible.
- Encrypt removable media; label with owner/asset ID; prohibit personal media for business data.
- Scan media for malware prior to use.
[HIPAA] Apply minimum necessary standard for ePHI; document approved use cases.

4.5 Transport and Shipping
- Use tracked carriers; tamper-evident packaging; document chain of custody for transfers.
- For high sensitivity, use two-person control.
[HIPAA] Protect ePHI during transport; ensure BAAs with handlers where applicable.

4.6 Maintenance and Repair
- Sanitize/remove drives before third-party service when feasible; otherwise ensure vendor data protection.
[HIPAA] Execute BAAs with vendors potentially handling ePHI; log custody.

4.7 Incident Handling
- For loss/theft, quarantine via MDM/EDR; initiate remote wipe if appropriate; notify Security; document.
[HIPAA] Assess for reportable breach; follow Breach Notification procedures.

4.8 Return, Decommission, and Disposition
- Collect devices on offboarding/replacement; reconcile inventory; proceed to sanitization/destruction per Section 4.10.

4.9 Training and Awareness
- Provide onboarding and annual refresher training on hardware/media handling.
[HIPAA] Include HIPAA device/media handling modules.

4.10 Data Sanitization and Destruction
- Follow NIST SP 800-88 Rev.1: select Clear, Purge, or Destroy based on media type and reuse.
- Document method, tool/procedure, operator, witness, serials, timestamps.
- Verify results (hash/visual/certificate) and file Certificates of Destruction when applicable.
[HIPAA] Maintain documentation for ≥ 6 years; ensure alignment with 45 CFR §164.310(d) and §164.312(e).

4.11 Third-Party Vendors
- Use vetted vendors; obtain certificates for destruction; ensure contractual safeguards.
[HIPAA] Execute BAAs with vendors that may handle ePHI; require adherence to NIST 800-88.

4.12 Compliance and Audit
- Perform periodic audits of inventory accuracy, custody logs, storage controls, and destruction

records; remediate gaps.

5.0 Exceptions

Exceptions require documented justification, risk assessment, compensating controls, and Security (and [HIPAA] Security/Privacy Officer) approval.

6.0 Review

Review annually or upon significant operational/regulatory changes.

HIPAA Media Destruction SOP (Step-by-Step)

Records: Retain forms, logs, approvals for 6 years.

(Printable Checklist)

HIPAA Media Destruction SOP

Purpose: Ensure compliant sanitization/destruction of media with ePHI (HIPAA 45 CFR §164.310(d); NIST SP 800-88).

Section A: Authorization
[ ] Complete Media Destruction Form; obtain required approvals.

Section B: Method Selection
[ ] Determine Clear/Purge/Destroy based on media type and reuse.

Section C: Execution
[ ] Perform selected method (e.g., crypto erase, degauss, shred).
[ ] Document tool, serials, operator, witness, timestamps.

Section D: Verification
[ ] Validate results (hash/visual/certification) and record certificate #.

Section E: Disposal & Recycling
[ ] Use vetted vendor; maintain BAA if applicable.
[ ] Ensure environmental compliance and documentation.

Section F: Records & Review
[ ] Update asset records; store forms and certificates 6 years.
[ ] Review failures and implement corrective actions.

Sign-Off
- Performed By (print/sign/date): _____
- Witness (print/sign/date): _____
- Security/Privacy Review (print/sign/date): _____

HIPAA_Media_Destruction_Form

HIPAA Media Destruction Verification & Chain of Custody Form

Instructions: Complete for any media/device containing ePHI. Retain for 6 years.

Section 1: Media Details
- Media Type (HDD/SSD/Tape/USB/Optical/Mobile): _____
- Asset Tag / Serial #: _____
- Capacity: _____
- Location (site/room): _____
- Custodian/Department: _____
- Data Classification (ePHI/PII/etc.): _____

Section 2: Authorization
- Ticket/Change/Incident #: _____
- System Owner Approval (name/sign/date): _____
- Security/Privacy Approval (name/sign/date): _____

Section 3: Sanitization/Destruction Method
- Method (NIST 800-88 Clear/Purge/Destroy): _____
- Tool/Procedure Used (e.g., crypto erase, degauss, shred): _____
- Standard/Ref (e.g., NIST SP 800-88 Rev.1): _____
- Performed By (name/sign/date): _____
- Witness (name/sign/date): _____

Section 4: Validation
- Verification Method (hash match/visual inspection/cert #:): _____
- Result: _____
- Certificate of Destruction/Work Order #: _____

Chain of Custody Log

Date/Time	From	To	Signature	Notes

HIPAA_Data_Recovery_SOP

HIPAA_Data_Recovery_Form

HIPAA Data Recovery Request & Chain of Custody Form

Instructions: Complete all sections. Store completed forms for 6 years per HIPAA retention.

Section 1: Request Details
- Request ID: _____
- Request Date/Time: _____
- Requestor Name/Title/Department: _____
- Contact Info (email/phone): _____
- Business Justification (clinical/operational impact): _____
  _____

Section 2: Data/System Identification
- System/Application Name: _____
- Environment (Prod/Test/Dev): _____
- Data Type(s) (ePHI, PII, other): _____
- Data Owner: _____
- Location (server/VM/endpoint/cloud service): _____
- Asset Tag / Hostname: _____

Section 3: Recovery Parameters
- Incident/Change Reference #: _____
- Desired Restore Point (timestamp/snapshot): _____
- RTO Target (hours): _____
- RPO Target (minutes/hours): _____
- Scope (entire system / database / folder / files): _____
- Dependencies (DB, services, keys, networking): _____

Section 4: Authorization
- Security/Privacy Officer Approval (name/sign/date): _____
- System Owner Approval (name/sign/date): _____

Section 5: Recovery Execution (to be completed by IT)
- Assigned Engineer: _____
- Start Date/Time: _____
- Source Media (backup set ID, snapshot ID): _____
- Hash/Integrity Verification (method/result): _____
- Steps Performed (summary):
  _____

_____

_____

- End Date/Time: _____
- Outcome (success/partial/failed): _____
- Data Validation Results (owner sign-off): _____

Section 6: Post-Recovery Actions
- Incident Record Updated (yes/no): _____
- Gaps/Issues Identified: _____

_____
- Corrective Actions/Follow-ups: _____

_____
- Runbooks Updated (yes/no/date): _____

Chain of Custody (if physical media used)
- Media ID: _____
- Description: _____
- Custodian Transfer Log (name, date/time, from/to, signature):

Date/Time	From	To	Signature	Notes

HIPAA_Data_Recovery_SOP

HIPAA Data Recovery SOP (Printable Checklist)

Purpose: Ensure compliant, timely restoration of ePHI systems (HIPAA 45 CFR §164.308(a)(7)).

Section A: Triage & Authorization
[ ] Validate incident/change request and business impact.
[ ] Confirm data classification and owner; obtain approvals.

Section B: Identify Scope & Restore Point
[ ] Confirm system, dataset, dependencies, and desired timestamp.
[ ] Select backup/snapshot meeting RPO; verify media availability.

Section C: Prepare Environment
[ ] Isolate affected systems if incident-related (malware/ransomware).
[ ] Gather credentials/keys; ensure network and target capacity.

Section D: Execute Recovery
[ ] Follow runbook for system/db/file restore.
[ ] Track actions, timestamps, backup IDs.

Section E: Integrity Validation
[ ] Verify file/system integrity (hashes, DB consistency, app checks).
[ ] Obtain owner validation/sign-off.

Section F: Return to Service
[ ] Reconnect to production networks; monitor performance and logs.
[ ] Validate access controls and audit logging.

Section G: Documentation & Lessons Learned
[ ] Complete Data Recovery Form and attach artifacts (hashes, logs).
[ ] Update runbooks; record corrective actions and test plans.

Sign-Off
- Performed By (print/sign/date): _____
- Owner Validation (print/sign/date): _____
- Security/Privacy Review (print/sign/date): _____

Records: Retain forms, logs, approvals for 6 years.

HIPPA - Precision Computer Recycling Authorization Form

Precision Computer Recycling Authorization Form

Owner Information

Owner Full Name: _____

Address: _____

City/State/ZIP: _____

Phone: _____ Email: _____

(Optional) Business/Organization Name: _____

(Optional) Authorized Signer Title: _____

Description of Items to be Recycled (attach list if needed)

[ ] Computer/Desktop [ ] Laptop [ ] Monitor [ ] Printer/Copier/Scanner/Fax

[ ] Phone/Tablet [ ] Cables/Accessories [ ] Keyboards/Mice [ ] Projector

[ ] Server [ ] Networking Gear [ ] Batteries/UPS [ ] External/Internal Hard Drives

Other (list any additional items): _____

Ownership and Authority

I, the undersigned Owner (or authorized agent of the Owner), represent and warrant that:

- I am the lawful owner of the listed items or have full legal authority to dispose of them.

- The items are free of liens or third-party claims unless disclosed in writing.

Authorization and Transfer

I authorize Precision Computer to collect, transport, and recycle (and, where applicable, refurbish, resell, dismantle for parts, or otherwise process) the listed items in accordance with applicable laws and industry standards. I hereby transfer all right, title, and interest in the items to Precision Computer upon pickup/drop-off. Items and components will not be returned; disposition decisions are final.

Data-Bearing Devices (HIPAA ePHI Handling)

[ ] Items may contain ePHI [ ] Items do NOT contain ePHI [ ] Unknown

Covered Entity/BAA Status:
- Covered Entity/Business Associate Name: _____
- BAA on file: [ ] Yes [ ] No (execute prior to processing)

Requested Data Sanitization per NIST SP 800-88 Rev.1 (select one per device type):
[ ] Clear (logical overwrite) Tool/Procedure: _____
[ ] Purge (e.g., crypto erase, degauss) Details: _____
[ ] Destroy (physical shred/pulverize) Target size/spec: _____

Certificate of Destruction requested: [ ] Yes [ ] No
Certificate to be issued to (name/email): _____

PHI Safeguards Acknowledgment:
- Minimum necessary access will be applied; devices/media safeguarded in transit and storage (locked containers, tamper-evident seals).
- Precision Computer will implement commercially accepted methods aligned to NIST SP 800-88; deviations require written approval.

Hazardous/Prohibited Materials

I confirm the items do not contain prohibited or hazardous materials except as disclosed in writing. Precision Computer may refuse any item at its discretion.

Release and Indemnity

To the fullest extent allowed by law, I release and hold harmless Precision Computer, its employees, and agents from claims arising out of the removal, transport, processing, or recycling of the items, and I waive and disclaim any and all damages of any kind (including direct, indirect, incidental, consequential, special, exemplary, or punitive damages) arising from or related to the items after transfer, the services provided, or any disposition decisions, except to the extent caused by Precision Computer’s willful misconduct or gross negligence.

Compliance and Records

Precision Computer will handle items in compliance with applicable laws and may use certified downstream recyclers. Certificates of recycling or data destruction (if requested and offered) will be provided after processing.

Chain of Custody (Required for data-bearing devices)

Initial Custody
- Released by (print/sign/date/time): _____
- Received by (print/sign/date/time): _____
- Container/Seal #: _____ Condition: _____

Transfers (add rows as needed)

Date/Time	From (Name/Sign)	To (Name/Sign)	Purpose/Notes

Transport/Storage Safeguards

[ ] Tamper-evident packaging used [ ] Locked vehicle/container [ ] Secure on-site cabinet
[ ] Background-checked personnel [ ] Approved downstream vendor [ ] BAA in place (if applicable)

Signatures

Owner/Authorized Agent (print): _____

Signature: ..... Date: ___/___/____

If signing for a business, Title: _____

Accepted by Precision Computer Representative (print): _____

Signature: ..... Date: ___/___/____

Incident Management Policy

1.0 Purpose

This policy defines the standard process for managing operational incidents affecting client services delivered by Precision Computer. The primary goals of this policy are to ensure the timely detection, logging, categorization, resolution, and communication of incidents to restore normal service operation as quickly as possible, minimize adverse impact on client business operations, and maintain client satisfaction in accordance with Service Level Agreements (SLAs).

2.0 Scope

This policy applies to all unplanned interruptions or reductions in the quality of IT services delivered to clients by Precision Computer (referred to as "Incidents"). It covers all personnel involved in the detection, reporting, diagnosis, resolution, and communication of incidents affecting client services, including Service Desk, technical support tiers, network operations, security operations, account management, and relevant management.

This policy is distinct from the Data Breach Response Policy, which covers security incidents involving unauthorized access or data compromise, although an operational incident may escalate into a security incident.

3.0 Policy Statements

3.1 Incident Lifecycle Management

All incidents affecting client services must be managed through a defined lifecycle:

*   **Identification:** Incidents may be identified through automated monitoring systems, client reports (via phone, email, portal), or internal staff detection.
*   **Logging:** All identified incidents must be logged promptly and accurately in the Precision Computer IT Service Management (ITSM) system. The log must include relevant details such as client name, affected service(s), reported symptoms, date/time reported, source of report, and initial impact assessment.
*   **Categorization & Prioritization:** Incidents must be categorized (e.g., hardware failure, software bug, network outage, performance degradation) and prioritized based on their business impact and urgency, aligned with predefined Severity Levels (see section 3.3).
*   **Investigation & Diagnosis:** Appropriate technical personnel will investigate the incident to diagnose the root cause.
*   **Resolution & Recovery:** Actions will be taken to resolve the incident and restore normal service operation. This may involve implementing a workaround initially, followed by a permanent fix. All resolution steps must be documented in the incident log.
*   **Closure:** Once service is restored and confirmed (ideally with client validation), the incident

record will be formally closed in the ITSM system, including documentation of the final resolution.

3.2 Roles and Responsibilities

*   **Service Desk (Tier 1):** Initial point of contact for incident reporting, logging, basic troubleshooting, categorization, prioritization, resolution of simple incidents, and escalation to higher tiers.
*   **Technical Support Tiers (Tier 2/3):** Responsible for in-depth investigation, diagnosis, and resolution of escalated incidents requiring specialized knowledge.
*   **Incident Manager (or designated role):** Oversees the management of major or high-severity incidents, coordinates resources, ensures timely resolution, manages escalations, and oversees communication.
*   **Account Manager:** Acts as a liaison with the client, particularly for major incidents, ensuring client communication needs are met according to SLAs.
*   **All Personnel:** Responsible for identifying and reporting potential incidents promptly.

3.3 Severity Levels and Service Level Agreements (SLAs)

Incidents will be assigned a severity level based on impact and urgency, typically aligned with client SLAs. Examples:

*   **Severity 1 (Critical):** Complete loss of a critical business service affecting multiple users or entire site; significant business impact.
*   **Severity 2 (High):** Significant degradation or loss of a critical service affecting multiple users; major feature/functionality unavailable; significant business impact.
*   **Severity 3 (Medium):** Partial degradation of service affecting some users; minor feature/functionality unavailable; moderate business impact.
*   **Severity 4 (Low):** Minor service issue affecting a single user or minimal impact on business operations; cosmetic issue; information request.

Target response times and resolution goals are defined within individual client SLAs and are linked to these severity levels. All personnel must strive to meet or exceed SLA commitments.

3.4 Communication

*   **Internal Communication:** Clear and timely communication between support tiers, management, and account managers is essential during incident resolution.
*   **Client Communication:**
    *   Clients must be notified of Severity 1 and Severity 2 incidents affecting their services promptly, according to timelines defined in their SLA.
    *   Regular, proactive updates must be provided to affected clients throughout the lifecycle of Severity 1 and Severity 2 incidents.
    *   Communication methods (e.g., portal update, email, phone call) and frequency will be guided by the SLA and the nature of the incident.
    *   Confirmation of service restoration and incident resolution must be communicated to the client.
    *   Account Managers are responsible for ensuring client communication aligns with contractual

obligations and client expectations.

3.5 Escalation

* Incidents that cannot be resolved within the target timeframe or require additional resources must be escalated according to defined technical and managerial escalation paths.
* Escalation triggers and procedures must be documented and understood by all relevant personnel.

3.6 Major Incident Management

* Severity 1 incidents (or other incidents with significant widespread impact) will trigger a formal Major Incident Management process, typically led by an Incident Manager.
* This process involves coordinated communication (bridge calls, status updates), resource allocation, and focused efforts to restore service rapidly.

3.7 Post-Incident Review

* Major incidents (Severity 1) and recurring significant incidents require a Post-Incident Review (PIR).
* The PIR aims to identify the root cause, document lessons learned, evaluate the effectiveness of the response, and determine preventative actions to avoid recurrence.
* Findings and action items from PIRs must be tracked to completion.

4.0 Compliance

4.1 Compliance Measurement: Compliance will be measured through review of incident records in the ITSM system, analysis of SLA performance reports, client satisfaction feedback, and internal audits of the incident management process.
4.2 Exceptions: Deviations from this policy require documented justification and approval from designated management.
4.3 Enforcement: Failure to adhere to this policy may impact performance reviews, client satisfaction, and potentially lead to disciplinary action for repeated or negligent violations.

5.0 Related Policies

* Service Level Agreement (SLA) Framework / Specific Client SLAs
* Change Management Policy
* Problem Management Policy
* Data Breach Response Policy
* Client Communication Protocols
* Monitoring and Alerting Standards
* Audit Logging Standard

6.0 Definitions

*   **Incident:** An unplanned interruption to an IT service or reduction in the quality of an IT service.
*   **Severity:** A measure of the business impact of an incident.
*   **Urgency:** A measure of the speed with which an incident needs to be resolved.
*   **Priority:** Determined by combining impact (Severity) and Urgency; dictates the order of handling.
*   **Workaround:** A temporary solution to reduce or eliminate the impact of an incident for which a full resolution is not yet available.
*   **Resolution:** Action taken to repair the root cause of an incident or implement a permanent fix.
*   **IT Service Management (ITSM):** The entirety of activities performed by an organization to design, plan, deliver, operate and control IT services offered to customers.
*   **Service Level Agreement (SLA):** A commitment between a service provider and a client detailing specific aspects of the service – quality, availability, responsibilities.
*   **Response Time:** The time taken from when an incident is logged until initial assessment and assignment for resolution begins.
*   **Resolution Time:** The time taken from when an incident is logged until it is resolved and normal service is restored.

Lab Security Policy

1.0 Purpose

Laboratory environments (labs) often require configurations and network access distinct from the standard corporate production environment, potentially introducing unique security risks. This policy establishes the information security requirements necessary to manage and safeguard lab resources, minimize the exposure of critical infrastructure and information assets, and protect the organization's networks from threats originating from or traversing lab environments. Its purpose is to ensure labs are operated securely, balancing operational needs with essential security controls.

2.0 Scope

This policy applies to all employees, contractors, consultants, temporary staff, and other workers involved in the management, operation, or use of organizational labs. It covers all organization-owned and managed labs, including those located internally, externally, or within a Demilitarized Zone (DMZ), and applies to all associated systems, networks, equipment, hardware, software, and firmware within these lab environments.

3.0 Policy Statements

3.1 General Lab Management & Responsibility

*   **Ownership and Points of Contact (POC):** Each lab must have a designated owning organization/department, a primary Lab Manager, and at least one designated backup POC. Lab owners must register and maintain up-to-date POC information with the designated IT authority (e.g., Precision Computer) and relevant network/asset management teams. POCs (manager or backup) must be reachable for emergencies; otherwise, necessary security actions may be taken without their direct involvement.
*   **Lab Manager Accountability:** Lab Managers are accountable for the overall security posture of their lab, its compliance with all relevant organizational security policies (including this one), and its potential impact on other networks (corporate or external). They must implement procedures to ensure policy adherence and safeguard against vulnerabilities.
*   **Policy Compliance:** All activities within the lab must comply with applicable organizational policies, including but not limited to Acceptable Use, Data Classification, Password, and Audit Logging policies.
*   **Immediate Access for Security/Support:** Lab Managers must grant immediate access to lab equipment and system logs upon request to authorized personnel from the designated IT authority (e.g., Precision Computer) or Network Support Organization for security investigations or operational support.

3.2 Access Control

*   **Physical Access:** Lab Managers are responsible for controlling and managing physical access to their labs. Access shall only be granted to individuals with a documented, immediate business need. Access lists must be reviewed regularly, and access promptly terminated when no longer required.
*   **Logical Access:**
    *   Individual user accounts on lab devices must comply with the organization's Password Policy.
    *   Individual user accounts must be disabled or deleted within three (3) days of authorization removal.
    *   Passwords for shared or group accounts on lab systems must be changed at least quarterly and meet complexity requirements defined in the Password Policy.

3.3 Host and System Security

*   **Anti-Virus/Malware:** All PC-based lab computers capable of running such software must have organization-standard, supported anti-virus/anti-malware protection installed, configured for regular scans, and kept up-to-date (software and definitions). Infected systems must be immediately isolated from all networks until verified clean. Lab Managers must implement procedures to ensure this.
*   **Malicious Activity:** Intentionally creating or distributing malicious programs (viruses, worms, malware) is strictly prohibited, per the Acceptable Use Policy.
*   **Patching:** Systems within labs should be patched according to organizational vulnerability management standards, especially if connected to other networks. Systems that cannot be patched require compensating controls and potential isolation.

3.4 Data Security and Service Restrictions

*   **Prohibition of Production Services:** Labs must not host ongoing, shared, business-critical services that generate revenue or provide primary customer capabilities ("production services"). Such services must be managed by appropriate production support organizations.
*   **Data Classification Restrictions:** Information classified as Highly Confidential or Restricted (or equivalent high-sensitivity classifications per the Data Classification Policy) is generally prohibited on lab equipment unless the lab has specific approvals and security controls commensurate with that data sensitivity level.
*   **Audit Logging:** Lab systems must comply with the Audit Logging Policy where applicable, especially for systems connected to corporate networks or handling sensitive test data.

3.5 Internal Lab Network Security (Labs connected behind corporate firewall)

*   **Firewall Segregation:** All internal labs must be segregated from the corporate production network via a firewall managed by the designated Network Support Organization or IT authority.
*   **Network Monitoring and Intervention:** The Network Support Organization and/or designated IT authority (e.g., Precision Computer) reserve the right to monitor traffic and interrupt lab connections that negatively impact the corporate production network or pose a security risk.
*   **IP Address Management:** All lab IP addresses routed within organizational networks must be registered in the central IP address management system with current lab POC information.
*   **External Connections:** Adding direct external network connections (e.g., Internet, partner

networks) requires documented business justification, network diagrams, and formal review and approval by the designated IT authority (e.g., Precision Computer) *before* implementation.
*   **Prohibition of Cross-Connections:** Devices (wired or wireless) within the lab must not create unauthorized connections that bypass the designated firewall between the lab and production networks.
*   **Firewall Configuration Control:** Initial firewall configurations and subsequent changes require review and approval by the designated IT authority (e.g., Precision Computer).
*   **Prohibition of Disruptive Activities:** Labs must not engage in activities like unauthorized port scanning, network auto-discovery, or traffic flooding/spamming that could negatively impact corporate or external networks. Such testing must be contained strictly within the isolated lab environment.
*   **Inter-Lab Traffic:** Traffic between lab networks or between labs and production may be permitted based on approved business needs, provided it is properly secured (e.g., via firewall rules) and does not introduce unacceptable risk or negatively impact network performance. Labs must not advertise services that could conflict with production services.
*   **Auditing Rights:** The designated IT authority (e.g., Precision Computer) reserves the right to audit lab network traffic, configurations, and administration processes.
*   **Gateway Device Security:** Lab-owned gateway devices (routers, firewalls) must comply with relevant security advisories/patching requirements and should authenticate administrative access against central authentication servers where feasible. Enable/privileged access passwords must be unique, comply with the Password Policy, and be restricted to authorized administrators.

3.6 Security for Labs with Non-Organizational Personnel Access (e.g., Training Labs)

*   Labs where non-organizational personnel have physical access must *not* have direct connectivity to the corporate production network.
*   Organizational confidential information must not reside on systems within these labs.
*   Connectivity *from* these labs *to* the corporate production network for authorized personnel must use secure, authenticated methods approved by the designated IT authority (e.g., Precision Computer), such as client VPNs, SSH tunnels, or temporary authenticated access lists ('lock and key').

3.7 DMZ Lab Security Requirements

*   **Approval:** Establishing new DMZ labs requires strong business justification and executive (VP-level or higher) approval. Significant changes to existing DMZ lab connectivity or purpose require review and approval by the designated IT authority (e.g., Precision Computer Team).
*   **Physical Security:** DMZ labs must reside within physically secure, dedicated spaces (room, cage, or locked racks) with strictly controlled access lists maintained by the Lab Manager.
*   **Network Management:** DMZ lab personnel are responsible for managing network devices within the lab up to the demarcation point defined by the Network Support Organization.
*   **Prohibition of Internal Connections:** DMZ labs are strictly prohibited from having any direct or logical connection (e.g., IPsec tunnel, wireless bridge, multi-homed host) to corporate internal networks.
*   **Internet Firewall:** An approved firewall, managed by the Network Support Organization or IT authority, must exist between the DMZ lab and the Internet. Configurations must be based on the

principle of least privilege, reviewed and approved by the IT authority (e.g., Precision Computer Team), and all Internet traffic must traverse this firewall. Bypassing the firewall is prohibited.
* **Device Standardization:** Routers and switches within the DMZ lab (not used for testing) should conform to applicable organizational standards.
* **Secure Host Configuration:** Operating systems of hosts providing services within the DMZ must adhere to secure baseline configuration standards published by the designated IT authority (e.g., Precision Computer Team).
* **Secure Administration:** Remote administration must utilize secure, encrypted channels (e.g., SSH, IPsec VPN) or dedicated, out-of-band management networks.
* **No Open Proxies:** DMZ lab devices must not be configured as open proxies to the Internet.
* **Security Intervention:** The Network Support Organization and/or designated IT authority (e.g., Precision Computer) reserve the right to interrupt DMZ lab connections if a security risk is identified.

4.0 Compliance

4.1 Compliance Measurement

The designated IT authority (e.g., Precision Computer team) will verify compliance with this policy through various methods, including network scans, vulnerability assessments, configuration audits, physical inspections (walk-thrus), review of access logs and procedures, internal/external audits, and investigation of security incidents.

4.2 Exceptions/Waivers

Requests for waivers or exceptions to this policy must be formally documented with business justification, risk assessment, and proposed compensating controls. Exceptions require review and advance approval by the designated IT authority (e.g., Precision Computer Team) on a case-by-case basis.

4.3 Enforcement

Non-compliant labs may face network isolation or disconnection. Failure by Lab Managers or personnel to adhere to this policy may result in disciplinary action, up to and including termination of employment or contract.

5.0 Definitions

* **DMZ (Demilitarized Zone):** A perimeter network segment logically placed between an internal network and an external network (like the Internet), designed to host external-facing services while protecting the internal network.
* **Firewall:** A network security device that monitors and controls incoming and outgoing network traffic based on predetermined security rules.
* **Lab Manager:** The individual assigned primary responsibility for the operation, management, and security of a specific laboratory environment.
* **POC (Point of Contact):** An individual designated as a contact person for a specific lab or function.

*   **Production Services:** Ongoing, shared, business-critical IT services essential for core operations, revenue, or customer functions, typically managed under stricter change control and support agreements than lab environments.

6.0 Related Policies

*   Acceptable Use Policy
*   Audit Logging Policy
*   Data Classification Policy
*   Password Policy
*   Physical Security Policy
*   Remote Access Policy
*   Change Management Policy
*   Vulnerability Management Policy
*   Wireless Security Policy

Multi-Tenancy Security Policy

1.0 Purpose

Precision Computer utilizes shared infrastructure and platforms (multi-tenant environments) to efficiently deliver services to multiple clients. While offering scalability and cost-effectiveness, multi-tenancy introduces risks related to data segregation, access control, and resource allocation if not properly managed. The purpose of this policy is to define the mandatory security controls and architectural principles required to ensure the confidentiality, integrity, and availability of each client's data and services within shared environments, preventing unauthorized access or interference between tenants (clients).

2.0 Scope

This policy applies to all shared infrastructure, platforms, and applications managed by Precision Computer used to deliver services to multiple clients simultaneously. This includes, but is not limited to, shared hosting environments, virtualized platforms, cloud infrastructure managed by Precision Computer, shared network segments, multi-tenant applications (e.g., RMM, PSA, backup solutions, security tools), and shared databases. It applies to all personnel involved in the design, deployment, configuration, management, and security of these multi-tenant environments.

3.0 Policy Statements

3.1 Logical Segregation and Data Isolation

* Robust logical segregation controls **must** be implemented and maintained to ensure strict isolation between client tenants at all relevant layers (network, storage, compute, application, database).
* **Network Segregation:** Techniques such as VLANs, VRFs, firewalls with strict rule sets, security groups, or software-defined networking (SDN) must be used to prevent unauthorized network traffic between tenants.
* **Storage Segregation:** Data belonging to different clients must be logically separated using mechanisms like distinct storage volumes, access control lists (ACLs) on file systems/object storage, or database-level separation (e.g., separate schemas, databases, or row-level security). Encryption keys used for data-at-rest encryption should ideally be tenant-specific where feasible.
* **Compute Segregation:** Virtualization technologies must be configured securely to prevent VM escape or unauthorized inter-VM communication. Resource allocation (CPU, RAM, I/O) must be managed to prevent resource exhaustion caused by one tenant impacting others (noisy neighbor problem).

*   **Application/Database Segregation:** Multi-tenant applications must be designed or configured with strong tenant isolation controls. Unique tenant identifiers must be used throughout, and data access logic must rigorously enforce tenant boundaries.

3.2 Access Control

*   Access to the underlying shared infrastructure and management planes must be strictly controlled based on least privilege and role-based access control (RBAC).
*   Administrative access must require Multi-Factor Authentication (MFA) and comply with the Password Policy.
*   Client access to shared platforms (e.g., management portals) must be strictly limited to their own tenant data and configurations.
*   Access controls must prevent personnel assigned to one client from accessing another client's data or environment unless explicitly authorized for a specific, documented purpose (e.g., shared support function with appropriate controls).
*   All administrative access and significant configuration changes to the multi-tenant environment must be logged and monitored according to the Audit Logging Standard.

3.3 Authentication

*   Authentication mechanisms must securely identify and separate users and processes belonging to different tenants.
*   Where federated identity or single sign-on (SSO) is used, configurations must ensure that authentication tokens or assertions cannot be misused to gain cross-tenant access.

3.4 Resource Management

*   Resource allocation and monitoring must be implemented to ensure fair usage and prevent resource contention or denial-of-service conditions caused by one tenant affecting others.
*   Quota management and resource throttling may be employed.

3.5 Change Management

*   Changes to the shared infrastructure or platforms must follow the Precision Computer internal Change Management Policy.
*   Impact assessments must explicitly consider the potential effect on all tenants hosted on the platform.
*   Communication regarding maintenance or changes affecting the shared platform must be provided to all affected clients according to SLA and communication protocols.

3.6 Security Monitoring and Logging

*   The multi-tenant environment must be monitored for security events, performance issues, and availability.
*   Logging must be configured to capture tenant-specific activities where possible while ensuring logs themselves maintain tenant separation if accessed by clients.
*   Logs from the shared infrastructure must be centrally collected and analyzed according to the

Audit Logging Standard.

3.7 Vulnerability Management

* The shared infrastructure and platforms must be included in the scope of Precision Computer's Vulnerability Management program.
* Regular vulnerability scanning and timely patching according to the Patch Management Policy are required.

3.8 Penetration Testing

* Periodic penetration testing specifically targeting the multi-tenant controls and segregation mechanisms should be conducted.

4.0 Responsibilities

* **Architecture/Engineering Teams:** Responsible for designing, building, and configuring multi-tenant environments according to the security principles in this policy.
* **Operations/Infrastructure Teams:** Responsible for the day-to-day management, monitoring, patching, and maintenance of the shared infrastructure.
* **Information Security Team:** Responsible for defining security requirements, performing risk assessments, auditing controls, and overseeing vulnerability management and penetration testing of shared environments.
* **Service Delivery Teams:** Responsible for utilizing shared platforms according to defined procedures and managing client instances within them.

5.0 Compliance

5.1 Compliance Measurement: Compliance will be verified through technical audits of segregation controls, review of configurations (network, virtualization, application), vulnerability scans, penetration test results, access control reviews, log analysis, and review of relevant documentation.
5.2 Exceptions: Exceptions to this policy require rigorous technical justification, detailed risk assessment, documentation of compensating controls, and approval from senior management and the Information Security Team.
5.3 Enforcement: Failure to implement or maintain adequate security controls in multi-tenant environments can lead to significant security incidents and client data breaches. Non-compliance may result in disciplinary action and require immediate remediation efforts.

6.0 Related Policies

* Client Data Management Policy
* Client System Access Control Policy
* Network Security Policy / Firewall Policy
* Server Security Policy
* Virtualization Security Policy (if separate)
* Acceptable Encryption Policy

*   Audit Logging Standard
*   Vulnerability Management Policy
*   Change Management Policy
*   Incident Response Policy

7.0 Definitions

*   **Multi-Tenancy:** An architecture where a single instance of software and its supporting infrastructure serves multiple customers (tenants).
*   **Tenant:** A group of users (typically representing a single client organization) who share common access within a multi-tenant system but are logically isolated from other groups.
*   **Logical Segregation:** The separation of data or network traffic based on software configurations, policies, or protocols, rather than physical separation.
*   **VM Escape:** An exploit where malicious code running within a virtual machine breaks out to access the underlying hypervisor or other virtual machines.

Password Construction Guidelines

1.0 Purpose

Passwords are a fundamental component of information security, acting as the first line of defense for user accounts, systems, and data. Weak or easily guessable passwords significantly increase the risk of unauthorized access and compromise. The purpose of these guidelines is to provide clear best practices for creating and managing strong, secure passwords and passphrases to protect individual users and organizational assets.

2.0 Scope

These guidelines apply to all employees, contractors, consultants, temporary staff, vendors, agents, and other workers, including personnel affiliated with third parties, who are granted access to organizational systems or data. They apply to all passwords used for authentication, including but not limited to user-level accounts, system-level accounts (where applicable), web application accounts, email accounts, screen saver locks, voicemail access, network device logins, and any other system requiring password authentication within the organizational context.

3.0 Guideline Statements: Creating Strong Passwords and Passphrases

To enhance security, all passwords created and used for organizational accounts should adhere to the following principles:

3.1 Length:

*   **Minimum Length:** Passwords should be significantly long to resist brute-force attacks. A minimum length of **14 characters** is strongly recommended for all new passwords. Longer is generally better.
*   **Passphrases Encouraged:** Using **passphrases** (multiple words forming a memorable phrase) is highly encouraged. Examples: `"ItsTime4MyVaca!"`, `"Block-Curious-Sunny-L3aves"`. Passphrases can be easier to remember and type while meeting length and complexity requirements.

3.2 Complexity and Content:

*   Passwords should ideally incorporate a mix of character types (uppercase letters, lowercase letters, numbers, symbols). However, length is the most critical factor. A long passphrase without complex substitutions is often stronger than a short, complex password.
*   **Avoid Weak Content:** Passwords **must not** contain easily guessable information or

predictable patterns. Avoid:

* Personal information (names of family, pets, friends; birthdates; addresses; phone numbers; usernames; real words directly related to you or the organization).
* Common keyboard patterns (e.g., `qwerty`, `asdfgh`, `12345678`).
* Repeating characters or simple sequences (e.g., `aaaaaa`, `111111`, `abcde`).
* Commonly used default or weak passwords (e.g., `Password123`, `Welcome1`, `Changeme`).
* Dictionary words spelled forwards or backward.

3.3 Uniqueness:

* **Unique Passwords:** Each account (work-related or personal accounts accessed via work devices/networks) should have a **unique password**. Reusing passwords across different services dramatically increases risk; if one account is compromised, others using the same password become vulnerable.

4.0 Tools and Best Practices for Password Management

4.1 Password Managers:

* Creating and remembering unique, strong passwords for every account is challenging. The use of organization-approved **password manager software** is highly encouraged. These tools securely store complex passwords and can help generate strong, random ones, requiring you only to remember one strong master password for the manager itself. Only use password managers vetted and approved by the designated IT authority (e.g., Precision Computer).

4.2 Multi-Factor Authentication (MFA):

* Passwords alone are often insufficient. Wherever possible, **Multi-Factor Authentication (MFA)** must be enabled on accounts. MFA adds a crucial layer of security by requiring a second form of verification (e.g., a code from a mobile app, a text message, a hardware token) in addition to the password.

5.0 Compliance

5.1 Compliance Measurement:

While specific password content is not typically audited directly for privacy reasons, compliance with password *policies* (enforced by system settings like minimum length and complexity) and these *guidelines* (through training and awareness) will be assessed. The designated IT authority (e.g., Precision Computer team) may verify compliance through system configuration checks, security audits, monitoring for weak password usage where detectable, and user awareness programs.

5.2 Exceptions:

System-level constraints may occasionally prevent adherence to the ideal length recommendation. Any exceptions to enforced password policies require justification and approval from the

designated IT authority (e.g., Precision Computer team).

5.3 Responsibility:

Users are responsible for creating passwords consistent with these guidelines and for protecting their passwords from disclosure. Violations of enforced password policies may lead to account lockout or disciplinary action.

6.0 Definitions

* **Password:** A secret string of characters used to authenticate a user to a system or service.
* **Passphrase:** A sequence of words or other text used as a password, typically longer and potentially easier to remember than complex character strings.
* **Password Manager:** Software designed to securely store and manage user passwords for various accounts.
* **Multi-Factor Authentication (MFA):** A security process requiring users to provide two or more different authentication factors to verify their identity (e.g., something they know [password], something they have [token/phone], something they are [biometric]).

7.0 Related Policies

* Password Policy (which defines mandatory requirements like minimum length, history, expiration)
* Acceptable Use Policy
* Information Security Policy (Overall)
* Remote Access Policy

Password Protection Policy

1.0 Purpose

Passwords are a critical security control for protecting user accounts, organizational systems, and sensitive information. This policy establishes the mandatory standards for password creation, protection, management, and system-level handling to prevent unauthorized access and mitigate security risks associated with weak or compromised passwords. Adherence to this policy is essential for maintaining the security and integrity of the organization's IT environment.

2.0 Scope

This policy applies to all employees, contractors, consultants, temporary staff, vendors, agents, and any other individuals ("Users") who have or are responsible for any account or form of access requiring a password on any system that:
* Resides within any organizational facility.
* Connects to the organization's network.
* Stores non-public organizational information.

This includes user accounts, service accounts, administrative accounts, application accounts, network device accounts, etc. It also applies to application developers designing systems that handle authentication.

3.0 Policy Statements

3.1 User Responsibilities: Password Creation and Protection

* **Mandatory Requirements:** All passwords used to access organizational resources must meet the minimum requirements enforced by the respective systems. These requirements typically include:
    * **(Placeholder: Minimum Length - e.g., 12 characters)**
    * **(Placeholder: Complexity Requirements - e.g., Must contain characters from 3 of the following 4 categories: Uppercase letters, Lowercase letters, Numbers, Symbols)**
    * **(Placeholder: Password History - e.g., Cannot reuse the last 10 passwords)**
    * **(Placeholder: Maximum Password Age - e.g., Must be changed every 90 days)**
    (Note: The specific values for the placeholders above must be defined and configured by the organization based on risk assessment and best practices).
* **Password Confidentiality:** Users must keep their passwords confidential. Passwords must not be shared with anyone, including colleagues, supervisors, family members, or IT support staff. (IT support will use other methods for assistance). Passwords must not be written down in unsecured locations (e.g., sticky notes, unsecured files).
* **Uniqueness:** Passwords must be unique to each organizational account and should not be reused across different systems or external non-organizational accounts.

*   **Suspicion of Compromise:** If a user suspects their password has been compromised, they must change it immediately and report the suspicion to the IT Help Desk or designated security contact.
*   **Guidance:** Users should follow the best practices outlined in the organization's **Password Creation Guideline** for creating strong, memorable passwords or passphrases that meet these policy requirements.

3.2 System and Application Requirements (Developer/Administrator Responsibilities)

*   **Individual Authentication:** Systems and applications must authenticate individual users. Use of shared or group accounts should be minimized and requires specific approval and controls.
*   **Secure Storage:** Passwords must **never** be stored in clear text or any easily reversible format (e.g., weak hashing, simple encryption with embedded keys). Strong, salted, adaptive hashing algorithms (e.g., bcrypt, scrypt, Argon2, PBKDF2) must be used for storing password hashes. Refer to Secure Database Credential Handling Policy for application credential storage.
*   **Secure Transmission:** Passwords must **never** be transmitted in clear text over any network. Secure, encrypted protocols (e.g., TLS/SSL, SSH) must be used for all authentication processes involving password transmission.
*   **Role Management/Delegation:** Applications should provide mechanisms for role management or delegation (e.g., impersonation, delegated authority) so that administrative tasks or functional coverage can occur without requiring users to share their personal passwords.
*   **Password Policy Enforcement:** Systems must be configured to technically enforce the mandatory password requirements defined in section 3.1 (minimum length, complexity, history, expiration).

4.0 Compliance

4.1 Compliance Measurement

The designated IT authority (e.g., Precision Computer team, Information Security, Internal Audit) will verify compliance with this policy through various methods. These include technical enforcement checks via system configurations, audits of password storage mechanisms in applications, security assessments, review of account management procedures, internal/external audits, and analysis of authentication logs.

4.2 Exceptions

Any exception to this policy (e.g., for specific system accounts or legacy applications where requirements cannot be met) requires formal, documented justification, risk assessment identifying compensating controls, and advance approval from the designated IT authority (e.g., Precision Computer Team or Information Security).

4.3 Enforcement

*   Failure by users to comply with password protection requirements may result in disciplinary action, up to and including termination of employment or contract.
*   Failure by system administrators or developers to ensure systems comply with the technical

requirements of this policy may result in requirements for immediate remediation, system isolation, or disciplinary action.
* Accounts with non-compliant passwords may be disabled until brought into compliance.

5.0 Definitions

* **Password:** A secret string of characters used to authenticate a user to a system or service.
* **Password Hash:** A one-way cryptographic representation of a password, used for secure storage and comparison.
* **Salt:** Random data added to a password before hashing to make precomputed hash attacks (e.g., rainbow tables) ineffective.
* **Clear Text:** Unencrypted, human-readable data.

6.0 Related Policies and Guidelines

* Password Creation Guideline
* Acceptable Use Policy
* Information Security Policy (Overall)
* Secure Database Credential Handling Policy
* Secure Development Policy / Standards
* Remote Access Policy
* Account Management Policy

Remote Access Policy

1.0 Purpose

Remote access to the organization's network is crucial for operational efficiency and productivity. However, connections originating from external networks, which may have lower security standards or potential compromises, introduce inherent risks. The purpose of this policy is to establish the rules and requirements for all remote connections to the organization's network. These measures are designed to minimize potential exposure and mitigate risks, including the loss or compromise of sensitive data, damage to critical systems, reputational harm, and potential legal or financial liabilities.

2.0 Scope

This policy applies to all employees, contractors, vendors, and agents of the organization ("Authorized Users") utilizing any computer or device (whether organization-owned or personally-owned) to connect to the organization's network from a remote location. This includes, but is not limited to, accessing email, intranet resources, or performing any work-related tasks on behalf of the organization. This policy encompasses all methods and technologies used for remote access.

3.0 Policy Statements

The following statements define the specific rules, responsibilities, and technical requirements governing remote access to the organization's network:

3.1 General Principles and Responsibilities

*   **Security Equivalence:** Authorized Users must ensure their remote access connection security is maintained at a level equivalent to that expected within the organization's physical premises.
*   **Authorized Use Only:** Access privileges are granted solely for conducting organizational business. Performance of illegal activities or pursuing outside business interests via the organization's network is strictly prohibited. Recreational use of the internet through the remote connection should be minimal and must comply with the organization's Acceptable Use Policy.
*   **User Accountability:** Authorized Users are responsible for safeguarding their access credentials (logins, passwords, tokens) and preventing unauthorized use of their connection or access to organizational resources by non-Authorized Users (including family members). The Authorized User is accountable for all activities conducted through their access credentials.
*   **Acceptable Use:** All remote access activities must adhere to the organization's Acceptable Use Policy.

3.2 Technical Requirements

*   **Secure Connections:** Remote access must be established using organization-approved secure methods, typically involving encryption technologies like Virtual Private Networks (VPNs). Connections must be authenticated using strong credentials, adhering to the organization's Password Policy.
*   **Endpoint Security:** All devices (organization-owned or personal) used for remote access must have organization-approved, up-to-date endpoint security software installed and active, including anti-virus/anti-malware protection. Authorized Users should utilize organization-provided resources or designated internal portals to obtain required security software.
*   **Network Isolation:** When connected to the organization's network via remote access using an organization-owned computer, Authorized Users must ensure the device is not simultaneously connected to other untrusted or public networks. Connections to personally controlled, secured home networks may be permissible if configured according to organizational guidelines. Split-tunneling configurations require explicit approval based on security assessments.
*   **Configuration Standards:** All devices used for remote access, including personally-owned equipment, must meet the minimum security configuration standards defined by the organization (as detailed in the relevant Hardware and Software Configuration Standards document).
*   **Third-Party Access:** Connections by third parties must comply with the requirements outlined in specific Third-Party Agreements and this policy.

3.3 Use of External Resources

The use of external resources (e.g., non-organizational systems or cloud services) to conduct organizational business via a remote connection requires prior approval from both the relevant business unit manager and the designated IT authority (e.g., Precision Computer team, Internal IT Security).

4.0 Compliance

4.1 Compliance Measurement

The designated IT authority (e.g., Precision Computer team, Internal IT Security) will verify compliance with this policy through various methods. These may include, but are not limited to, network monitoring, log reviews, audits (internal and external), security scans, and inspection of connected devices. Findings will be reported to the policy owner and relevant management.

4.2 Exceptions

Any exception to this policy requires formal, documented justification and advance approval from both the designated IT authority responsible for remote access services and potentially other relevant stakeholders (e.g., IT Security). Approved exceptions will be reviewed periodically.

4.3 Enforcement

Failure to comply with this policy by Authorized Users may result in disciplinary action, up to and including termination of employment or contract. Access privileges may be revoked immediately pending investigation of violations.

5.0 Related Policies and Standards

Authorized Users should familiarize themselves with the following related organizational documents:

* Acceptable Encryption Policy
* Acceptable Use Policy
* Password Policy
* Third Party Agreement / Policy
* Hardware and Software Configuration Standards for Remote Access

Remote Access Tools Policy

1.0 Purpose

Remote access tools and remote desktop software (e.g., RDP, VNC, LogMeIn, GoToMyPC) offer significant benefits for productivity, collaboration, and IT support by enabling screen sharing and remote system control. However, insecure or unmanaged use of these tools creates substantial security risks, potentially providing unauthorized pathways into the organization's network, leading to data theft, unauthorized access, or system compromise. The purpose of this policy is to define the mandatory requirements for the selection, configuration, and use of remote access tools to ensure that all such access to organizational assets is secure, monitored, and controlled.

2.0 Scope

This policy applies to all employees, contractors, consultants, temporary staff, vendors, agents, and other personnel utilizing any remote access tool or technology where at least one endpoint of the communication session terminates on an organizational computer asset (e.g., server, desktop, laptop managed by the organization or connected to its network).

3.0 Policy Statements

3.1 Use of Approved Tools Only

*   Only remote access tools explicitly approved and provided or sanctioned by the organization's designated IT authority (e.g., Precision Computer Team) are permitted for accessing organizational resources remotely or for allowing remote access *to* organizational assets.
*   An official list of approved remote access tools and corresponding mandatory configuration procedures will be maintained by the designated IT authority and made available through internal resources. Using unapproved tools for organizational business is strictly prohibited.

3.2 Security Requirements for Approved Tools

The selection and approval of remote access tools will be based on adherence to the following minimum security requirements:

*   **Multi-Factor Authentication (MFA):** All remote access originating from external networks (Internet, partner systems) into the organization's network *must* require MFA (e.g., using tokens, smart cards, authenticator apps) in addition to standard credentials.
*   **Strong Authentication Source & Protocol:** Authentication must ideally leverage the organization's central identity stores (e.g., Active Directory, LDAP). Authentication protocols must be secure, resistant to replay attacks (e.g., using challenge-response mechanisms), and should mutually authenticate both endpoints of the session where technically feasible.
*   **Proxy Compatibility:** Tools should support routing through organization-approved security

infrastructure, such as application layer proxies or VPN gateways, rather than requiring direct inbound connections through perimeter firewalls, unless explicitly approved as part of a secure architecture.
* **Strong Encryption:** All remote access communication channels must utilize strong, end-to-end encryption that meets or exceeds the standards defined in the organization's Acceptable Encryption Policy and relevant network security protocols.
* **Compatibility with Security Tools:** Remote access tools must not interfere with, disable, or circumvent mandatory organizational security controls deployed on endpoints or networks (e.g., antivirus/anti-malware, Data Loss Prevention (DLP), endpoint detection and response (EDR)).

3.3 Procurement and Configuration

* Any procurement of remote access tools must follow standard organizational procurement processes and requires explicit approval from the designated IT authority (e.g., Information Technology group).
* All approved remote access tools must be configured strictly according to the mandatory procedures provided by the designated IT authority to ensure secure operation.

4.0 Compliance

4.1 Compliance Measurement

The designated IT authority (e.g., Precision Computer team, Information Security) will verify compliance with this policy through various methods, including network monitoring, review of approved software lists, configuration audits of endpoints and servers, security assessments of remote access infrastructure, internal/external audits, and analysis of access logs.

4.2 Exceptions

Any exception to this policy (e.g., use of a non-standard tool for a specific, justified business need with a partner) requires formal, documented justification, thorough risk assessment including compensating controls, and advance approval from the designated IT authority (e.g., Precision Computer Team or Information Security).

4.3 Enforcement

* Unauthorized remote access tools found on organizational assets will be removed.
* Network access for systems using unapproved or insecurely configured remote access tools may be blocked.
* Violations of this policy by personnel may result in disciplinary action, up to and including termination of employment or contract.

5.0 Definitions

* **Remote Access Tool:** Software or hardware that allows a user to connect to and control a computer or network resource from a remote location (e.g., RDP, VNC, VPN clients with remote control features, commercial tools like LogMeIn/GoToMyPC).

*   **Multi-Factor Authentication (MFA):** An authentication method requiring more than one verification factor (e.g., password + token code).
*   **Application Layer Proxy:** A server that acts as an intermediary for requests from clients seeking resources from other servers, specifically filtering traffic at the application layer.
*   **Mutual Authentication:** A process where both parties in a communication session authenticate each other's identity.

6.0 Related Policies

*   Remote Access Policy (Overall VPN/Network Access)
*   Acceptable Use Policy (AUP)
*   Password Policy
*   Acceptable Encryption Policy
*   Information Security Policy (Overall)
*   Procurement Policy
*   Third-Party Connection Policy

Router and Switch Security Policy

1.0 Purpose

Routers and switches form the backbone of the organization's network infrastructure. Their secure configuration is paramount to maintaining network integrity, availability, and protecting data traversing the network. This standard establishes the minimum required security configuration for all routers and switches connected to or operating within the organization's production network environment to mitigate risks associated with misconfiguration and unauthorized access.

2.0 Scope

This standard applies to all employees, contractors, consultants, temporary staff, vendors, and other personnel responsible for the configuration, management, or operation of routers and switches connected to the organization's production networks. It covers all such devices owned or managed by the organization.

3.0 Standard Requirements

All routers and switches within the scope of this standard must adhere to the following minimum security configuration requirements:

3.1 Authentication and Access Control

*   **Centralized Authentication:** Local user accounts must be disabled. All administrative authentication to routers and switches must utilize the organization's approved centralized authentication system (e.g., TACACS+, RADIUS) integrated with central identity stores.
*   **Enable/Privileged Mode Security:** Access to privileged ('enable') mode must be secured. The enable password/secret must be stored in a secure, encrypted format on the device and must comply with the organization's password complexity and management policies. Enable passwords should be managed centrally where possible and rotated regularly.
*   **Management Access Protocols:** Secure protocols must be used for administrative access. SSH version 2 is the required protocol for remote command-line access. Telnet is strictly prohibited unless tunnelled over a secure, encrypted connection (e.g., IPsec VPN).
*   **Access Control Lists (ACLs):** Infrastructure ACLs must be implemented to restrict management access (SSH, SNMP, NTP, TACACS+/RADIUS source IPs, etc.) to the device itself, permitting connections only from authorized management subnets or hosts.
*   **Console/Aux Port Security:** Physical console and auxiliary port access must be controlled through physical security measures and may require additional authentication controls.

3.2 Service Hardening

The following services and features must be **disabled** unless a specific, documented, and approved business justification exists:

* IP Directed Broadcasts
* TCP Small Services (echo, discard, chargen, daytime)
* UDP Small Services (echo, discard, chargen, daytime)
* IP Source Routing
* Proxy ARP (unless specifically required and approved)
* HTTP/HTTPS server (web interface) for device management (unless specifically approved with strong authentication and TLS)
* Telnet server
* FTP server
* Configuration Auto-loading features
* Vendor-specific discovery protocols (e.g., CDP, LLDP) on interfaces facing untrusted networks (e.g., Internet, external partners). May be disabled internally unless required for specific network functions (e.g., VoIP phone discovery).
* Dynamic Trunking Protocol (DTP) on switch ports (configure ports statically as access or trunk).
* Scripting environments (e.g., TCL shell) unless explicitly required for approved automation tasks.

3.3 Secure Configuration Settings

* **Password Encryption:** The service to encrypt passwords stored in the device configuration (e.g., `service password-encryption` or equivalent) must be enabled. (Note: This provides only obfuscation; stronger protection relies on secure authentication protocols and restricted configuration access).
* **Network Time Protocol (NTP):** Devices must be configured to synchronize their time with approved, redundant internal NTP sources traceable to a reliable external standard.
* **Simple Network Management Protocol (SNMP):**
  * If SNMP is used, default community strings (e.g., "public," "private") must be removed or changed to strong, complex values compliant with password policies.
  * SNMP access must be restricted using ACLs to authorized management stations only.
  * SNMPv3, which provides encryption and authentication, is the required version. Use of SNMPv1 or v2c requires a documented exception and strong justification.
* **Logging:** Devices must be configured to log security-relevant events (logins, configuration changes, ACL denials) to the organization's centralized logging system (SIEM) via secure syslog, adhering to the Audit Logging Policy.
* **Login Banner:** The following standard warning banner (or an organization-approved equivalent) must be configured and presented for all login attempts (console, SSH):
  > "UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED. You must have explicit permission to access or configure this device. All activities performed on this device may be logged, and violations of this policy may result in disciplinary action, and may be reported to law enforcement. There is no right to privacy on this device. Use of this system shall constitute consent to monitoring."

3.4 Routing Security

*   **Secure Routing Updates:** Dynamic routing protocols (e.g., EIGRP, OSPF, BGP) must utilize neighbor authentication (e.g., using MD5 or SHA hashes with strong keys) for all routing updates. Password hashing features for the authentication string must be enabled where supported.
*   **Route Filtering:** Appropriate route filtering must be implemented to prevent injection of inappropriate routes.
*   **Anti-Spoofing:** Ingress filtering (e.g., Unicast Reverse Path Forwarding - uRPF, or ACLs) must be implemented on interfaces, particularly edge interfaces, to drop packets sourced with invalid or illegitimate addresses (e.g., RFC1918 addresses from the Internet, bogons, internal addresses arriving on external interfaces).

3.5 Sensitive Device Requirements

Certain critical routers and switches (e.g., core devices, perimeter firewalls/routers, devices handling highly sensitive data) may be designated as "sensitive" and require additional security controls as defined by the designated IT authority (e.g., Precision Computer). These may include:

*   More detailed logging configurations (e.g., IP ACL accounting).
*   Enhanced monitoring.
*   Stricter access controls and change management procedures.

3.6 Network Management Integration

*   All production routers and switches must be registered in the organization's network management and asset inventory systems with accurate configuration details and designated points of contact.

4.0 Compliance

4.1 Compliance Measurement

The designated IT authority (e.g., Precision Computer team, Information Security, Internal Audit) will verify compliance with this standard through various methods, including automated configuration audits, vulnerability scanning, manual reviews, penetration testing, internal/external audits, and review of network monitoring data.

4.2 Exceptions

Any exception to this standard requires formal, documented justification outlining the technical necessity or constraint, risk assessment including compensating controls, and advance approval from the designated IT authority (e.g., Precision Computer Team or Information Security).

4.3 Enforcement

*   Devices found to be non-compliant with this standard must be remediated within a defined timeframe or risk being isolated or removed from the production network.

*   Failure by personnel responsible for device management to adhere to this standard may result in disciplinary action, up to and including termination of employment or contract.

5.0 Definitions

*   **Production Network:** The primary operational network infrastructure supporting the organization's core business functions and services.
*   **TACACS+ (Terminal Access Controller Access-Control System Plus):** A protocol providing centralized authentication, authorization, and accounting (AAA) for network device administration.
*   **RADIUS (Remote Authentication Dial-In User Service):** Another common protocol for centralized AAA.
*   **ACL (Access Control List):** A set of rules applied to network interfaces to permit or deny traffic based on criteria like source/destination IP address, port numbers, and protocols.
*   **SNMP (Simple Network Management Protocol):** A protocol used for monitoring and managing network devices. SNMPv3 adds security features.
*   **SSH (Secure Shell):** A cryptographic network protocol for operating network services securely over an unsecured network.
*   **NTP (Network Time Protocol):** A protocol for synchronizing the clocks of computer systems over packet-switched networks.
*   **RFC1918 Addresses:** Private IPv4 address ranges (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16) not routable on the public Internet.

6.0 Related Policies

*   Password Policy
*   Audit Logging Policy
*   Acceptable Use Policy
*   Change Management Policy
*   Vulnerability Management Policy
*   Information Security Policy (Overall)
*   Network Segmentation Policy / Architecture Documents

Secure Database Credential Handling Policy

1.0 Purpose

This policy establishes the mandatory requirements for securely storing, retrieving, and managing database authentication credentials (usernames and passwords) used by software applications connecting to the organization's databases. Improper handling of these credentials poses a significant security risk, potentially leading to unauthorized database access, compromise of sensitive data, and broader system compromise. The purpose is to prevent credential exposure within source code, configuration files, or insecure storage locations.

2.0 Scope

This policy applies to all system implementers, software engineers, developers, administrators, and any personnel involved in the design, development, deployment, or maintenance of software applications (including programs, modules, libraries, scripts, or APIs) that access production databases operating on the organization's networks. While primarily focused on production environments, applying these principles to non-production and lab environments is strongly recommended due to the potential presence of sensitive data.

3.0 Policy Statements

Applications accessing organization databases must authenticate using credentials handled according to the following requirements:

3.1 Credential Storage Prohibitions

* Database credentials (usernames and passwords) **must not** be stored in clear text within the main executing body of an application's source code.
* Credentials **must not** be stored in files or locations directly accessible by a web server (e.g., within the web server's document root or browseable directories).
* Credentials **must not** be embedded directly within compiled application binaries where they could be easily extracted.

3.2 Approved Credential Storage Methods

Acceptable methods for storing database credentials include, but are not limited to:

* **Secure Configuration Files:** Storing credentials in a separate configuration file outside the application's source code and web-accessible directories. This file must have restricted file system

permissions (not world-readable or world-writeable) limiting access strictly to the application's service account or authorized processes. The credentials within this file should ideally be encrypted or protected using operating system mechanisms.
*   **Secrets Management Systems:** Utilizing dedicated secrets management solutions (e.g., HashiCorp Vault, Azure Key Vault, AWS Secrets Manager) designed for secure storage, retrieval, and rotation of credentials and secrets. This is the preferred method.
*   **Environment Variables:** Passing credentials via secure environment variables accessible only to the application process, configured through secure deployment mechanisms.
*   **Integrated Authentication / Service Accounts:** Leveraging integrated authentication mechanisms (e.g., Windows Authentication for SQL Server, Oracle OS Authentication [carefully configured], Kerberos) where the application authenticates using the operating system identity of its service account, eliminating the need to manage separate database passwords within the application context.
*   **Authentication/Entitlement Servers:** Utilizing centralized authentication services (e.g., LDAP, Active Directory) where database access may be granted based on user or service authentication managed by the central server, potentially reducing the need for direct credential handling by the application itself. (Note: Specific implementation details must be secure).

3.3 Secure Credential Retrieval and Handling in Code

*   When credentials must be read from a configuration file or other source, they should be retrieved immediately prior to establishing the database connection.
*   Once the database connection is established, the memory variables holding the clear-text credentials must be securely cleared, zeroed out, or released as soon as technically feasible within the programming language's capabilities.
*   Source code files dedicated solely to retrieving or managing credentials must be kept separate from the main application logic and protected with appropriate access controls.

3.4 Credential Uniqueness and Management

*   Each distinct application or service implementing a specific business function should utilize unique database credentials. Sharing credentials between different applications or services is prohibited.
*   Database passwords used by applications are considered system-level passwords and must comply with the complexity, rotation, and management requirements defined in the organization's Password Policy.
*   Development teams must implement documented processes for securely managing and rotating application database passwords, restricting knowledge of these passwords on a strict need-to-know basis.

3.5 Pass-Through Authentication

*   Database authentication mechanisms that rely solely on remote host authentication without additional database-level checks (e.g., some configurations of Oracle OPS$) are prohibited if they grant broad, unverified access. Implementations must ensure proper user mapping and authorization within the database.

3.6 Secure Coding Guidelines

*   Development teams must follow organization-approved secure coding guidelines specific to the programming languages and frameworks being used (e.g., Java, C#, Python, Perl). These guidelines should incorporate specific techniques for implementing the requirements of this policy.
(Reference to internal secure coding standard documents should be maintained here).

4.0 Compliance

4.1 Compliance Measurement

The designated IT authority (e.g., Precision Computer team, Information Security, Internal Audit) will verify compliance with this policy through methods such as code reviews, security architecture reviews, configuration audits, vulnerability scanning, penetration testing, and review of documentation and processes.

4.2 Exceptions

Any exception to this policy requires formal, documented justification outlining the technical constraints or business necessity, proposed compensating controls, and risk assessment. Exceptions must be approved in advance by the designated IT authority (e.g., Precision Computer team).

4.3 Enforcement

*   Applications or code found to be in violation of this policy must be remediated within a defined timeframe (e.g., 90 days) or risk being disabled.
*   Violations by employees may result in disciplinary action, up to and including termination of employment.
*   Violations by temporary workers, contractors, or vendors may result in the termination of their contract or assignment.

5.0 Definitions

*   **Credentials:** Authentication information, typically a username and password pair, used to verify identity and grant access.
*   **Executing Body (of code):** The primary source code files containing the main application logic, as distinct from separate configuration files or dedicated credential management modules.
*   **Hash Function:** A cryptographic function that converts an input into a fixed-size string of characters (the hash value). Used for integrity checks and password storage (storing the hash, not the password itself), but not directly applicable for storing credentials needed for active authentication by an application.
*   **LDAP (Lightweight Directory Access Protocol):** A protocol used for accessing and maintaining distributed directory information services, often used for authentication and authorization.
*   **Module:** A self-contained unit of software code that performs a specific task or set of tasks.
*   **Secrets Management System:** A dedicated tool or service designed to securely store, manage, and control access to sensitive information like API keys, passwords, and certificates.

Related Policies:

* Password Policy
* Secure Coding Standards/Guidelines
* Data Classification Policy

Server Security Policy

1.0 Purpose

Servers are critical components of the organization's IT infrastructure, hosting vital applications and sensitive data. Unsecured or improperly configured servers represent a significant vulnerability and a primary target for malicious actors. The purpose of this policy is to establish the minimum standards for the secure configuration, management, operation, and monitoring of all server equipment owned or operated by the organization on its internal networks. Adherence to these standards is crucial to minimize security risks, prevent unauthorized access, and protect the confidentiality, integrity, and availability of organizational information and technology assets.

2.0 Scope

This policy applies to all employees, contractors, consultants, temporary staff, vendors, and other personnel responsible for the deployment, administration, operation, or management of server equipment on the organization's internal network. It covers all physical and virtual servers owned, operated, or leased by the organization or registered under an organization-owned internal network domain. This policy applies specifically to internal servers; servers located in a Demilitarized Zone (DMZ) are subject to additional requirements outlined in the DMZ Equipment Policy.

3.0 Policy Statements

3.1 Ownership, Responsibility, and Registration

* **Ownership:** All internal servers must have a clearly designated owning operational group or department responsible for system administration and policy compliance.
* **Configuration Guides:** Each operational group must establish, maintain, and follow approved server configuration guides (secure baseline builds) tailored to their specific server roles and operating systems. These guides must be based on organizational standards and security best practices and require initial and ongoing review and approval by the designated IT authority (e.g., Precision Computer). A process for managing changes to these guides, including review and approval, must be in place.
* **Registration:** All servers must be registered in the organization's central asset management or enterprise management system. Registration information must be kept accurate and up-to-date, including at a minimum:
    * Server hostname and IP address(es).
    * Primary and backup administrator/owner points of contact (including location).
    * Hardware details and Operating System/Version.
    * Primary functions and applications hosted.
* **Change Management:** All configuration changes applied to production servers must follow formal organizational change management procedures.

3.2 Secure Configuration Requirements

*   **Baseline Conformance:** Servers must be configured in accordance with the approved secure configuration guides/baselines relevant to their operating system and function.
*   **Service Hardening:** Unnecessary services, applications, and network ports must be disabled or removed to minimize the server's attack surface.
*   **Patch Management:** Servers must be kept up-to-date with the latest security patches and updates provided by the OS and application vendors. Patches must be applied promptly according to the organization's vulnerability management timeline requirements, with documented exceptions only permitted for specific, approved business reasons requiring compensating controls.
*   **Principle of Least Privilege:**
    *   Services and applications should run under accounts with the minimum privileges necessary for their function. Use of highly privileged accounts (e.g., root, Administrator) should be restricted to essential administrative tasks.
    *   User access must adhere to the principle of least privilege, granting only the permissions required for assigned job duties.
*   **Trust Relationships:** System-level trust relationships (e.g., domain trusts, Kerberos delegation, SSH key-based trusts) must be implemented judiciously, documented, regularly reviewed, and avoided where alternative secure communication methods suffice.
*   **Secure Administrative Access:** Privileged access (administrative login) must be performed over secure, encrypted channels (e.g., SSH, TLS-protected protocols, console access via secure terminal servers). Unencrypted administrative protocols (e.g., Telnet, FTP) are prohibited.
*   **Access Control Logging:** Access to critical services should be logged and potentially protected by additional access control layers (e.g., web application firewalls for web services) where feasible.

3.3 Physical Security

*   Servers must be physically located within secure, access-controlled environments (e.g., data centers, locked server rooms) compliant with the organization's Physical Security Policy.
*   Operating servers from uncontrolled areas, such as user cubicles or open offices, is strictly prohibited.

3.4 Monitoring and Logging

*   **Audit Logging:** Servers must generate audit logs for security-relevant events as defined in the Audit Logging Policy. This includes logins (success/failure), privilege changes, configuration modifications, critical service start/stop events, significant errors, and security tool alerts.
*   **Log Forwarding:** Security-related logs must be forwarded to the organization's central logging system (SIEM) in near real-time.
*   **Log Retention:** Audit logs must be retained according to the following minimum schedule (or as defined by the organizational Record Retention Schedule, whichever is longer):
    *   Online (e.g., within SIEM): Minimum 1 week
    *   Offline Backups (e.g., daily incrementals): Minimum 1 month
    *   Offline Backups (e.g., weekly fulls): Minimum 1 month
    *   Offline Backups (e.g., monthly fulls): Minimum 2 years

*   **Log Review and Reporting:** Security-related events identified in logs or by monitoring systems (e.g., port scans, unauthorized privilege access attempts, anomalous system behavior) must be reported to and reviewed by the designated security authority (e.g., Precision Computer, Security Operations Center). This authority will coordinate incident response and prescribe corrective measures as needed.

4.0 Compliance

4.1 Compliance Measurement

The designated IT authority (e.g., Precision Computer team, Information Security, Internal Audit) will verify compliance with this policy through various methods, including configuration audits against approved baselines, vulnerability scanning, penetration testing, review of change management records, physical security checks, log reviews, internal/external audits, and assessment of monitoring procedures.

4.2 Exceptions

Any exception to this policy requires formal, documented justification outlining the technical necessity or constraint, risk assessment including compensating controls, and advance approval from the designated IT authority (e.g., Precision Computer Team or Information Security). Operational groups managing servers should maintain a record of approved exceptions relevant to their systems.

4.3 Enforcement

*   Servers found to be non-compliant with this policy must be remediated within a defined timeframe or risk being isolated or removed from the network.
*   Failure by personnel responsible for server administration or management to adhere to this policy may result in disciplinary action, up to and including termination of employment or contract.

5.0 Definitions

*   **Server:** A computer system (physical or virtual) providing shared resources, services, or applications to other computers (clients) over a network.
*   **Baseline (Secure Configuration Guide):** A documented standard configuration defining the required security settings and software state for a specific operating system or server role.
*   **DMZ (Demilitarized Zone):** A perimeter network segment logically placed between an internal network and an external network (like the Internet).
*   **Least Privilege:** The security principle of granting users and processes only the minimum permissions necessary to perform their required functions.
*   **Trust Relationship:** A configured link between systems or domains allowing one system/domain to accept authentication or authorization decisions made by the other.

6.0 Related Policies

* Audit Logging Policy
* Change Management Policy
* Data Classification Policy
* DMZ Equipment Policy
* Information Security Policy (Overall)
* Password Policy
* Physical Security Policy
* Vulnerability Management Policy / Patch Management Policy
* Record Retention Schedule / Policy

Service Level Agreement (SLA) Management Policy / Framework

1.0 Purpose

Service Level Agreements (SLAs) are critical commitments defining the level of service clients can expect from Precision Computer. This policy establishes the framework and mandatory procedures for defining, documenting, implementing, monitoring, reporting on, and reviewing SLAs for all services delivered to clients. The purpose is to ensure clarity and consistency in service level commitments, manage client expectations effectively, align service delivery capabilities with promises, provide a basis for performance measurement, and drive continuous service improvement.

2.0 Scope

This policy applies to all services offered by Precision Computer to clients where specific service levels (e.g., availability, performance, response times, resolution times) are contractually defined. It covers all personnel involved in negotiating, defining, documenting, delivering, monitoring, reporting on, and reviewing SLAs, including Sales, Account Management, Service Delivery, Technical Support Tiers, Network Operations, Security Operations, and relevant management.

3.0 Policy Statements

3.1 SLA Definition and Documentation

* SLAs must be clearly defined, measurable, achievable, relevant, and time-bound (SMART).
* All SLAs must be formally documented within client contracts, Statements of Work (SOWs), or dedicated SLA documents referenced therein.
* SLAs must accurately reflect the capabilities of Precision Computer's service delivery processes and supporting infrastructure.
* Standard SLA templates should be used where possible, with customization requiring formal review and approval.
* SLAs should clearly define:
    * The service(s) covered.
    * Specific metrics and targets (e.g., % uptime, response time by severity, resolution time by severity).
    * Measurement methodology and reporting frequency.

* Service hours and maintenance windows.
* Exclusions (factors outside Precision Computer's control).
* Client responsibilities related to the SLA.
* Consequences of SLA breaches (e.g., service credits, reporting requirements), if applicable.

3.2 Service Catalog Alignment

* SLAs should align with services defined in the Precision Computer Service Catalog to ensure consistency in service descriptions and offerings.

3.3 Monitoring and Measurement

* Systems and processes must be in place to accurately monitor and measure performance against agreed-upon SLA metrics.
* Monitoring tools (e.g., RMM, network monitoring, ITSM systems) must be configured to collect the necessary data.
* Measurement periods and methodologies must align with the documented SLA.

3.4 Reporting

* Regular SLA performance reports must be generated.
* Internal reports are required for service delivery management, identifying trends and areas for improvement.
* Client-facing reports must be provided according to the frequency and format specified in the client contract/SLA.
* Reports must be accurate, clear, and highlight performance against key SLA targets, including any breaches.

3.5 SLA Review

* SLAs should be reviewed periodically (e.g., annually or as defined in the contract) with clients to ensure they remain relevant, achievable, and aligned with evolving business needs and service capabilities.
* Internal reviews of SLA performance should occur more frequently (e.g., quarterly or monthly) to proactively manage service delivery.
* Revisions to SLAs require formal agreement and documentation updates.

3.6 SLA Breach Management

* Potential or actual SLA breaches must be identified promptly (often through incident management or performance monitoring).
* Breaches must be logged and tracked.
* Client communication regarding breaches must follow procedures defined in the SLA and Incident Management policy.
* Root cause analysis should be performed for significant or recurring breaches to identify underlying issues (linking to Problem Management processes).
* Any applicable remedies (e.g., service credits) must be applied according to contractual terms.

3.7 Alignment with Internal and Vendor Agreements

*   Internal Operational Level Agreements (OLAs) between [MSP Name] teams must be established where necessary to support end-to-end client SLA delivery.
*   Underpinning Contracts (UCs) with third-party vendors providing critical service components must include service level commitments that enable [MSP Name] to meet its client-facing SLAs. Vendor performance against UCs must be monitored (ref: Third-Party / Vendor Risk Management Policy).

4.0 Roles and Responsibilities

*   **Sales/Account Management:** Responsible for negotiating achievable SLAs with clients, ensuring clear documentation in contracts, and managing client communication regarding SLA reviews and major breaches.
*   **Service Delivery Management:** Responsible for the overall design and delivery of services to meet SLA targets, overseeing monitoring and reporting, and driving service improvement initiatives based on SLA performance.
*   **Technical Teams:** Responsible for delivering services within agreed parameters, contributing to monitoring configuration, and participating in breach investigation and resolution.
*   **Service Desk:** Often responsible for initial logging related to incident response times contributing to SLAs.
*   **[Designated Authority, e.g., Reporting Analyst/Team]:** Responsible for generating and distributing internal and client-facing SLA performance reports.

5.0 Compliance

5.1 Compliance Measurement: Compliance will be measured through audits of client contracts and SLA documentation, review of monitoring configurations, analysis of SLA performance reports, client satisfaction feedback, and review of breach management records.
5.2 Exceptions: Any deviation from standard SLA templates or processes requires documented justification and approval from designated management (e.g., Head of Service Delivery, Sales Director).
5.3 Enforcement: Failure to manage services according to agreed SLAs can result in contractual penalties (e.g., service credits), client dissatisfaction, loss of business, and may impact performance reviews for responsible personnel.

6.0 Related Policies

*   Incident Management Policy (Client Focus)
*   Change Management Policy (Client Focus)
*   Problem Management Policy
*   Third-Party / Vendor Risk Management Policy
*   Client Communication Protocols
*   Monitoring and Alerting Standards
*   Service Catalog

7.0 Definitions

*   **Service Level Agreement (SLA):** A documented agreement between a service provider and a client identifying services, service targets, and responsibilities.
*   **Operational Level Agreement (OLA):** An internal agreement between different teams or departments within the service provider organization, defining responsibilities and timeframes needed to support client SLAs.
*   **Underpinning Contract (UC):** A contract between the service provider and a third-party vendor, detailing services and targets required from the vendor to support client SLAs.
*   **Key Performance Indicator (KPI):** A measurable value demonstrating how effectively a company is achieving key business objectives. SLAs typically define specific KPIs.
*   **Service Credit:** A remedy sometimes offered to clients in an SLA for failure to meet certain performance targets, often a partial discount on service fees.

Software Installation Policy

1.0 Purpose

The installation of unauthorized or improperly vetted software on organizational computing devices introduces significant risks. These risks include, but are not limited to, software conflicts leading to system instability or loss of functionality, the introduction of malware (viruses, spyware, ransomware), violations of software licensing agreements leading to legal liability, and the installation of tools that could compromise network security or sensitive data. The purpose of this policy is to establish clear requirements and procedures for requesting, approving, and installing software on all organization-owned computing devices to mitigate these risks.

2.0 Scope

This policy applies to all employees, contractors, consultants, temporary staff, vendors, agents, and any other individuals using computing devices owned or managed by the organization. This includes desktops, laptops, servers, smartphones, tablets, and any other device capable of having software installed that connects to the organization's network or accesses organizational data.

3.0 Policy Statements

3.1 Prohibition of Unauthorized Installation

* Users (employees, contractors, etc.) are strictly prohibited from installing any software onto organization-owned computing devices themselves. This includes downloading software from the internet, installing from removable media (USB drives, CDs/DVDs), or using personal software licenses on organizational assets.

3.2 Software Request and Approval Process

* All requests for new software installation must follow a formal process:
    1. The user requiring the software must obtain written approval (email sufficient) from their direct manager, confirming the business need for the requested software.
    2. Once manager approval is obtained, the user must submit a formal request to the designated IT authority (e.g., Information Technology department or IT Help Desk) via approved channels (e.g., ticketing system, designated email).
    3. The request should clearly state the business justification and the specific software needed.

3.3 Approved Software List

* The designated IT authority (e.g., Information Technology department) will maintain a list of standard, approved software titles that have been vetted for security, compatibility, and licensing compliance.

* Users should first attempt to select software from this approved list if it meets their business requirements.
* Requests for software *not* on the approved list will require additional review and justification regarding the specific need that approved alternatives cannot meet.

3.4 IT Department Responsibilities

* Upon receiving an approved request, the designated IT authority (e.g., Information Technology department) is responsible for:
    * Verifying the business need and approvals.
    * Reviewing non-standard software requests for security risks, compatibility issues, and supportability.
    * Procuring the necessary software licenses through approved channels.
    * Tracking all software licenses to ensure compliance.
    * Testing new software for conflicts and compatibility within the organization's standard operating environment where feasible.
    * Performing the installation of the approved software onto the user's device(s).
    * Maintaining records of installed software.

4.0 Compliance

4.1 Compliance Measurement

The designated IT authority (e.g., Precision Computer team, Information Security, Internal Audit) will verify compliance with this policy through various methods, including software inventory scans, audits of devices, review of help desk requests and software licenses, internal/external audits, and investigation of security incidents potentially related to unauthorized software.

4.2 Exceptions

Any exception to this policy (e.g., granting specific users limited installation rights for development purposes under controlled conditions) requires formal, documented justification, risk assessment, and advance approval from the designated IT authority (e.g., Precision Computer team or Information Security).

4.3 Enforcement

* Unauthorized software found on organizational devices will be removed.
* Users found to have violated this policy by installing unauthorized software may be subject to disciplinary action, up to and including termination of employment or contract. Access privileges may also be restricted.

5.0 Related Policies

* Acceptable Use Policy (AUP)
* Information Security Policy (Overall)
* Change Management Policy

* Procurement Policy
* Workstation Security Policy / Standard

Technology Equipment Disposal Policy

1.0 Purpose

Organizational technology equipment often contains sensitive data and components requiring special handling at the end of its lifecycle. Improper disposal poses significant risks, including data breaches if storage media are not securely sanitized, environmental harm, and potential legal non-compliance. Simply deleting files or formatting storage devices is insufficient, as data often remains recoverable. The purpose of this policy is to define the mandatory procedures for the disposal of all organizational technology equipment and components, ensuring secure data sanitization, environmentally responsible disposal, and proper asset management.

2.0 Scope

This policy applies to all employees, contractors, consultants, temporary staff, and affiliates of the organization. It covers any organization-owned or leased technology equipment or peripheral device that is no longer needed or has reached the end of its useful life. This includes, but is not limited to: personal computers (desktops, laptops, tablets), servers, mainframes, hard drives (internal/external), solid-state drives (SSDs), smartphones, handheld devices, peripherals (keyboards, mice, monitors, speakers), printers, scanners, copiers, fax machines, network equipment (routers, switches, firewalls, access points), removable storage media (USB drives, CDs, DVDs, floppy disks), backup tapes, batteries, and related printed materials containing sensitive information.

3.0 Policy Statements

3.1 Centralized Disposal Process

*   **Mandatory Handover:** When organizational technology assets reach the end of their useful life or are no longer needed, they **must** be transferred to the designated organizational team responsible for asset disposal (hereafter referred to as the "Disposal Team"). Users or departments must not dispose of equipment independently.
*   **Prohibited Disposal Methods:** Disposing of organizational technology equipment via unauthorized methods such as general waste skips, dumps, landfill, or unauthorized third parties is strictly prohibited. Unauthorized sale or donation of equipment is also prohibited.
*   **Secure Handling:** The Disposal Team will manage the secure storage, data sanitization, and final disposal or repurposing of all received equipment.

3.2 Mandatory Data Sanitization

*   **Requirement:** Before any equipment containing storage media (hard drives, SSDs, USB drives, memory cards, mobile device storage, tapes, etc.) is disposed of, repurposed, sold, donated, or leaves organizational control, all organizational data, licensed software, and sensitive information **must** be securely and permanently removed (sanitized).
*   **Sanitization Standards:** Data sanitization must be performed by the Disposal Team using methods that meet or exceed established industry standards (such as NIST SP 800-88 Guidelines for Media Sanitization or DoD 5220.22-M). Acceptable methods include:
    *   **Overwriting:** Using approved disk sanitizing software to overwrite every addressable sector on the media multiple times with specified patterns (e.g., zero-filled blocks, random patterns). Simple file deletion or standard OS formatting is **not** sufficient.
    *   **Degaussing:** Using a powerful magnetic field to destroy the magnetic domains on magnetic media like hard drives and tapes (not effective for SSDs or optical media).
    *   **Physical Destruction:** Rendering the storage media physically unreadable and data unrecoverable through methods like shredding, crushing, disintegration, or incineration. This is the required method for SSDs if overwriting is not feasible or verifiable, and for media that are non-functional or cannot be effectively overwritten (e.g., some mobile devices, CDs/DVDs).
*   **Verification and Logging:** The Disposal Team must verify the successful sanitization of storage media. A record must be maintained, potentially including a sticker or tag affixed to the equipment case, indicating the sanitization method used, the date performed, and the initials or ID of the technician responsible.
*   **Non-Functional Media:** Storage devices that are non-functional and cannot be reliably sanitized via overwriting or degaussing must have the physical storage component removed and physically destroyed.

3.3 Employee Purchase Program (Optional)

*   The organization may, at its discretion, make certain functional equipment that has been securely sanitized and reached the end of its organizational lifecycle available for purchase by employees.
*   **Process:** If implemented, this program must use a fair and transparent system (e.g., a lottery) to provide equal opportunity for purchase. Employees cannot directly purchase or reserve their previously assigned equipment.
*   **Pricing:** The designated Finance and IT departments will determine appropriate pricing for items offered.
*   **Condition:** All equipment is sold "as-is," final sale, with no warranty, support, or licensed software provided by the organization.
*   **Inventory Removal:** All purchased equipment must be formally removed from the organization's asset inventory system before leaving the premises.

3.4 Final Disposal/Donation

*   Equipment not sold through the employee purchase program (if applicable), deemed non-functional, or unsuitable for reuse will be disposed of or donated.
*   Disposal must be carried out in an environmentally responsible manner, adhering to all applicable local, state, and federal regulations (e.g., e-waste recycling laws).
*   The Disposal Team will utilize contracted, reputable vendors specializing in secure IT asset

disposition (ITAD) and certified e-waste recycling or donation.

4.0 Compliance

4.1 Compliance Measurement

The designated IT authority (e.g., Precision Computer team, Information Security, Internal Audit, Asset Management) will verify compliance with this policy through various methods, including audits of the disposal process, review of sanitization logs and vendor certifications, physical inventory checks, internal/external audits, and investigation of any potential data incidents related to improper disposal.

4.2 Exceptions

Any exception to the procedures outlined in this policy requires formal, documented justification and advance approval from the designated IT authority (e.g., Precision Computer Team or Information Security) and potentially Legal or Compliance departments, depending on the nature of the exception.

4.3 Enforcement

Failure to comply with this policy, particularly the requirements for centralized disposal and secure data sanitization, may result in disciplinary action, up to and including termination of employment or contract. Improper disposal may also lead to legal liability for the organization and individuals involved.

5.0 Definitions

* **Data Sanitization:** The process of irreversibly removing or destroying data stored on memory devices (hard drives, SSDs, tapes, mobile devices, etc.) to make it unrecoverable.
* **Overwriting:** A data sanitization method using software to write patterns of data (e.g., zeros, ones, random characters) onto storage media sectors.
* **Degaussing:** A data sanitization method using a powerful magnetic field to neutralize the magnetic charge on magnetic media (hard drives, tapes).
* **Physical Destruction:** A data sanitization method that physically damages the storage media beyond the possibility of data recovery (e.g., shredding, crushing, incineration).
* **Disposal Team:** The designated organizational department or group responsible for managing the collection, data sanitization, and final disposition of retired technology assets (e.g., IT Asset Management, Facilities).
* **Technology Equipment:** Includes computers, servers, storage devices, mobile devices, network gear, peripherals, and related items as detailed in the Scope section.

6.0 Related Policies

* Asset Management Policy
* Data Classification Policy
* Information Security Policy (Overall)

* Record Retention Schedule / Policy
* Physical Security Policy
* Change Management Policy (for decommissioning servers/systems)

Third-Party / Vendor Risk Management Policy

1.0 Purpose

Precision Computer relies on various third-party vendors and service providers to support its operations and deliver services effectively to its clients. Engaging with third parties inherently introduces risks, including security vulnerabilities, data breaches, operational disruptions, and compliance failures, which could impact both Precision Computer and its clients. The purpose of this policy is to establish a consistent framework for identifying, assessing, managing, and monitoring the risks associated with engaging third-party vendors, ensuring these relationships do not introduce unacceptable risks to Precision Computer or its clients' data and services.

2.0 Scope

This policy applies to all third-party relationships where the vendor:
* Accesses, processes, stores, or transmits Precision Computer confidential information or client data.
* Provides critical software, hardware, or services essential for Precision Computer's service delivery to clients (e.g., RMM, PSA, cloud hosting, data centers, security tools).
* Has direct or indirect connectivity to Precision Computer's internal network or management platforms.
* Represents Precision Computer or interacts directly with clients on Precision Computer's behalf.

This policy applies to all personnel involved in selecting, contracting, managing, and terminating relationships with third-party vendors.

3.0 Policy Statements

3.1 Vendor Identification and Inventory

* A central inventory of all third-party vendors falling within the scope of this policy must be maintained by the designated department (e.g., Procurement, Vendor Management Office).
* The inventory should include vendor contact details, services provided, data accessed/processed, criticality level, contract status, and risk assessment information.

3.2 Vendor Risk Assessment and Due Diligence

* **Initial Due Diligence:** Before engaging a new vendor or significantly expanding the scope of an existing relationship, a formal risk assessment and due diligence process must be conducted. The depth of the assessment will be proportionate to the criticality of the service provided and the

sensitivity of data involved.
* **Assessment Criteria:** Due diligence must evaluate, at a minimum:
  * The vendor's information security policies, practices, and technical controls.
  * Data privacy policies and compliance with relevant regulations (GDPR, CCPA, HIPAA, etc.).
  * Business continuity and disaster recovery capabilities.
  * Incident response procedures and breach notification history/capability.
  * Relevant security certifications (e.g., SOC 2 Type II, ISO 27001) or independent audit reports.
  * Financial stability and reputation.
  * Subcontractor (fourth-party) risk management practices.
* **Risk Tiering:** Vendors should be categorized into risk tiers (e.g., High, Medium, Low) based on the assessment results to determine the required level of ongoing monitoring and contract scrutiny.
* **Approval:** Engagement with new vendors, particularly those in higher risk tiers, requires approval from designated authorities (e.g., Security Team, Compliance, Legal, Senior Management) based on the satisfactory completion of due diligence.

3.3 Contractual Requirements

* Contracts with vendors falling under this policy must include specific clauses addressing information security and data privacy obligations, including:
  * Confidentiality requirements for Precision Computer and client data.
  * Data protection measures (encryption, access controls).
  * Breach notification timelines and procedures.
  * Right to audit or assess vendor controls (or review independent audit reports).
  * Compliance with applicable laws and regulations.
  * Limitations on liability.
  * Data handling upon contract termination (return/destruction).
  * Requirements for managing their own subcontractors (fourth-party risk).
* Contracts must be reviewed by Precision Computer's Legal counsel and Information Security representatives before finalization, especially for high-risk vendors.

3.4 Ongoing Monitoring

* Vendors, particularly those in higher risk tiers or providing critical services, must be subject to ongoing monitoring and periodic reassessment.
* Monitoring activities may include:
  * Reviewing updated SOC reports, security certifications, or penetration test results annually.
  * Monitoring vendor performance against SLAs.
  * Reviewing vendor security questionnaires periodically.
  * Tracking vendor security incidents or public breaches.
  * Conducting periodic risk reassessments (e.g., annually for high-risk vendors).

3.5 Vendor Access Control

* If a vendor requires access to Precision Computer or client systems/data, such access must be strictly controlled according to the principles of least privilege, using secure authentication

methods (including MFA where applicable), and subject to logging and monitoring, as defined in the relevant Access Control policies.

3.6 Incident Response Coordination

* Procedures must be in place to coordinate incident response activities with vendors in the event of a security breach or service disruption originating from or affecting the vendor.
* Contractual obligations regarding vendor cooperation during incidents must be clear.

3.7 Vendor Offboarding

* When a vendor relationship terminates, a formal offboarding process must be followed.
* This process must include:
  * Revocation of all vendor access to Precision Computer and client systems/data.
  * Confirmation of secure data return or destruction by the vendor according to contractual terms.
  * Final settlement of accounts.
  * Updating the vendor inventory.

4.0 Roles and Responsibilities

* **Vendor Relationship Owner (e.g., Department Head, Project Manager):** Responsible for initiating vendor engagement, managing the ongoing relationship, participating in risk assessments, and coordinating offboarding.
* **Procurement Department:** Responsible for managing the vendor inventory, facilitating contracts, and supporting due diligence.
* **Information Security Team:** Responsible for defining security requirements, conducting or reviewing security risk assessments, approving security controls, and reviewing security clauses in contracts.
* **Legal Department:** Responsible for reviewing and approving contract terms and conditions.
* **Compliance Department (if applicable):** Responsible for ensuring vendor compliance with relevant regulations.
* **All Personnel:** Responsible for reporting any unapproved vendor usage or observed vendor security concerns.

5.0 Compliance

5.1 Compliance Measurement: Compliance will be verified through audits of the vendor inventory, review of due diligence documentation and risk assessments, examination of vendor contracts, review of ongoing monitoring activities, and assessment of vendor incident handling.
5.2 Exceptions: Exceptions to this policy require documented justification, risk assessment, and formal approval from designated senior management and the Information Security Team.
5.3 Enforcement: Failure to follow this policy may expose Precision Computer and its clients to significant risk. Non-compliance by personnel may result in disciplinary action, up to and including termination.

6.0 Related Policies

*   Information Security Policy (Overall)
*   Data Classification Policy
*   Client Data Management Policy
*   Access Control Policy / Client System Access Control Policy
*   Procurement Policy
*   Incident Response Policy / Data Breach Response Policy
*   Business Continuity / Disaster Recovery Policy

7.0 Definitions

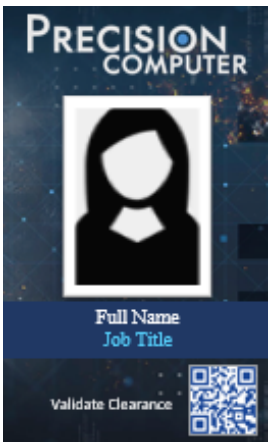
*   **Third-Party Vendor:** An external entity providing goods or services to Precision Computer.
*   **Due Diligence:** The process of investigation and analysis performed prior to entering into an agreement with a third party to assess potential risks.
*   **Risk Assessment:** The process of identifying, analyzing, and evaluating risks associated with a third-party relationship.
*   **SOC 2 (System and Organization Controls 2):** An auditing procedure ensuring service providers securely manage data to protect the interests of their organization and the privacy of its clients.
*   **ISO 27001:** An international standard for information security management systems (ISMS).

Verify Technicians on Arrival

We want to remind you of an important safety procedure, we take it seriously and ask all clients to follow our established identity verification protocol.

? **Please remember:**

- **Every technician** from Precision Computer is required to carry a **company-issued badge**
- Each badge includes a **photo and QR code** linking to their profile on our website https://precision-computer.com along with their level of access or permission.



- You can also verify any technician by calling us directly at **1-855-994-2900 or 1-660-827-1500**

? **Even if you recognize the technician**

— please still confirm their identity. Team members may change roles or leave the company, and someone familiar may **no longer be authorized to represent us**.

? If someone cannot be verified:

- **Do not allow them access**
- Ask them to return once their identity has been confirmed
- Notify us immediately

Your continued cooperation helps ensure the safety and security of everyone involved.

Thank you for your attention and support.

Web Application Security Policy

1.0 Purpose

Web application vulnerabilities represent a primary attack vector and pose significant risks to organizational security. Identifying and remediating vulnerabilities resulting from misconfigurations, coding errors, weak authentication, improper error handling, or information leakage is crucial before applications are deployed or updated. The purpose of this policy is to define the mandatory requirements for conducting web application security assessments within the organization. This policy aims to ensure that potential weaknesses are identified and mitigated, limiting the attack surface of web applications and services, protecting organizational data, and ensuring compliance with relevant security standards and change control processes.

2.0 Scope

This policy applies to all web applications developed, deployed, hosted, or managed by the organization, whether internal or external-facing. It applies to all individuals, groups, departments, and third-party vendors involved in the development, deployment, management, or assessment of these web applications. All web application security assessments requested or performed within the organization fall under the scope of this policy.

3.0 Policy Statements

3.1 Assessment Requirement and Authority

* All web applications within the scope of this policy are subject to security assessments as defined herein.
* Web application security assessments must be performed only by designated and qualified security personnel, either employed or contracted by the organization (hereafter referred to as the "Assessment Team").
* Assessment findings are considered confidential organizational information and must be distributed strictly on a "need-to-know" basis to personnel involved in the application's development, management, or remediation efforts. External distribution is prohibited without explicit executive approval (e.g., Chief Information Officer).

3.2 Assessment Triggers and Scope

Web applications must undergo security assessments based on the following criteria:

*   **New or Major Application Release:** A **Full Assessment** is required *before* final approval in the change control process and deployment into the production environment.
*   **Third-Party or Acquired Web Application:** A **Full Assessment** is required before integration into the organization's environment or network. Post-assessment, the application is subject to all requirements of this policy.
*   **Point Releases (Minor Functional Changes):** An appropriate assessment level (**Targeted** or **Quick**, potentially **Full** depending on risk) is required, determined by the Assessment Team based on the scope and potential security impact of the changes.
*   **Patch Releases (Bug Fixes, Minor Updates):** An appropriate assessment level (**Targeted** or **Quick**) is required, determined by the Assessment Team based on the risk associated with the patches or fixes. Security patches addressing known vulnerabilities require **Targeted** validation testing.
*   **Emergency Releases:** In documented emergency situations requiring immediate deployment, a security assessment may be temporarily bypassed with explicit approval from designated executive leadership (e.g., Chief Information Officer or delegated authority). However, the application carries assumed risk, and a **Full Assessment** must be scheduled and performed as soon as practicably possible post-deployment (e.g., within 30 days).

*   **Scoping:** Assessments will include all components and tiers of the application identified during scoping unless explicitly limited with documented justification approved before the assessment begins.

3.3 Risk Rating and Remediation

Security vulnerabilities identified during assessments will be risk-rated based on a standard methodology (e.g., OWASP Risk Rating Methodology). Remediation must occur according to the following requirements:

*   **High Risk:** Vulnerabilities rated as High must be remediated, or effective compensating controls must be implemented and approved by the Assessment Team/Information Security, **before** the application is deployed or allowed to remain in production. Failure to address High-risk issues may result in the application being denied deployment or taken offline immediately. Remediation validation testing is mandatory.
*   **Medium Risk:** Vulnerabilities rated as Medium must be reviewed, and a remediation plan with timelines must be developed and approved. Remediation should typically occur within the next planned release cycle (e.g., point/patch release) or within a defined timeframe (e.g., 60-90 days). Depending on the number and nature of Medium-risk findings, the Assessment Team/Information Security may require mitigation or delayed deployment. Remediation validation testing is mandatory.
*   **Low Risk:** Vulnerabilities rated as Low should be reviewed, documented, and scheduled for remediation as part of regular maintenance cycles or future releases based on available resources.

3.4 Assessment Levels

The Assessment Team will perform assessments at the following levels, as appropriate:

*   **Full Assessment:** Comprehensive testing for a wide range of known web application vulnerabilities (e.g., based on OWASP Testing Guide, OWASP Top Ten, SANS Top 25) using a combination of automated scanning tools and in-depth manual penetration testing techniques to validate findings and assess actual risk.
*   **Quick Assessment:** Primarily automated vulnerability scanning focused on common high-impact vulnerabilities (e.g., OWASP Top Ten) to provide a rapid risk overview. Manual validation may be limited.
*   **Targeted Assessment:** Focused testing on specific vulnerabilities (e.g., for remediation validation) or specific new/changed application functionality.

3.5 Approved Tools and Techniques

*   The Assessment Team will utilize a set of approved automated scanning tools and manual testing methodologies. *(The specific list of approved tools should be maintained internally by the Assessment Team).*
*   The Assessment Team reserves the right to use additional tools or techniques as necessary to investigate potential vulnerabilities, validate findings, and determine overall risk.

4.0 Integration with Change Control

*   Web application security assessments are an integral part of the organization's change control process.
*   Relevant assessment results and remediation status must be documented within the change control records before deployment approval for applicable releases (New, Major, Point, Patch).
*   Applications deployed without adhering to the assessment requirements of this policy may be subject to immediate removal from the production environment at the discretion of Information Security or executive leadership.

5.0 Compliance

5.1 Compliance Measurement

The designated IT authority (e.g., Precision Computer team, Information Security, Internal Audit) will verify compliance with this policy through various methods, including review of change control records, audit of assessment reports and remediation tracking, penetration testing, internal/external audits, and review of application security program documentation.

5.2 Exceptions

Any exception to this policy (e.g., delaying an assessment beyond standard triggers) requires formal, documented justification, risk acceptance by appropriate business and IT leadership, and advance approval from the designated Information Security authority (e.g., Precision Computer Team).

5.3 Enforcement

Failure to comply with this policy may result in deployment delays, applications being taken offline, or other corrective actions. Non-compliance by personnel may lead to disciplinary action, up to and including termination of employment or contract.

6.0 Definitions

*   **Web Application:** A client-server computer program where the client (including the user interface and client-side logic) runs in a web browser.
*   **Vulnerability:** A weakness in a system, application, or process that could be exploited by a threat actor.
*   **OWASP (Open Web Application Security Project):** A non-profit foundation focused on improving software security. Known for resources like the OWASP Top Ten (list of critical web application security risks), Testing Guide, and Risk Rating Methodology.
*   **Penetration Testing:** A simulated cyber attack against a computer system to check for exploitable vulnerabilities.
*   **Remediation:** The process of fixing or mitigating identified vulnerabilities.
*   **Compensating Control:** An alternative security measure put in place when it is not feasible or practical to directly remediate a vulnerability according to standard requirements.

7.0 Related Policies and Standards

*   Change Management Policy
*   Secure Development Lifecycle (SDL) Policy / Standards
*   Vulnerability Management Policy
*   Risk Management Framework / Policy
*   Information Security Policy (Overall)
*   Third-Party Risk Management Policy

Wireless Communication Policy

1.0 Purpose

Wireless networking (Wi-Fi) is prevalent and essential for connectivity using devices like laptops, smartphones, and tablets. However, insecure wireless configurations create significant vulnerabilities that malicious actors can exploit. The purpose of this policy is to establish the minimum security requirements for deploying, configuring, and connecting wireless infrastructure devices (access points, routers) and client devices to the organization's network. This policy aims to protect the confidentiality, integrity, and availability of the organization's information assets by managing the risks associated with wireless technologies.

2.0 Scope

This policy applies to all employees, contractors, consultants, temporary staff, vendors, and other personnel ("Users") at the organization, including affiliates and third parties who manage or use wireless infrastructure or connect devices wirelessly to the organization's network. It covers all wireless infrastructure devices operating on organizational sites or connecting to the network, and all devices (laptops, desktops, mobile phones, tablets, IoT devices, etc.) using wireless communications to access organizational resources. This includes any form of wireless communication capable of transmitting packet data.

3.0 Policy Statements

Access to the organization's network via wireless technology is a privilege conditioned on adherence to the following security requirements:

3.1 General Requirements for Corporate Wireless Networks

All wireless infrastructure devices deployed within organizational facilities that connect to the primary corporate network, or provide access to information classified as Confidential or higher (per the Data Classification Policy), must adhere to the following minimum security standards:

*   **Authentication:** Must utilize strong, enterprise-grade authentication protocols (e.g., WPA2-Enterprise or WPA3-Enterprise using EAP-TLS, PEAP, or other approved EAP types) integrated with the organization's central authentication system (e.g., RADIUS, Active Directory). Pre-shared keys (PSK) are prohibited for primary corporate network access.
*   **Encryption:** Must use strong encryption algorithms (e.g., AES/CCMP). Deprecated protocols like WEP or WPA/TKIP are prohibited.

*   **SSID Management:** Service Set Identifiers (SSIDs) for corporate access must not be broadcast where feasible or required by specific security directives. Guest network SSIDs may be broadcast but must be segregated. Default SSIDs must be changed.
*   **Device Management:** Access points must be centrally managed using organization-approved systems. Default administrative credentials must be changed immediately upon deployment using strong, unique passwords compliant with the Password Policy. Firmware must be kept up-to-date with security patches.
*   **Network Segmentation:** Corporate wireless networks must be appropriately segmented from guest or other less trusted networks using VLANs and firewall rules.
*   **Rogue AP Detection:** Mechanisms must be in place to detect and mitigate unauthorized (rogue) wireless access points connected to the corporate network.
*   **(Placeholder: Add any other specific requirements, e.g., specific configuration settings, physical security of APs).**

3.2 Requirements for Laboratory or Isolated Wireless Networks

Wireless networks deployed in laboratory or other isolated environments that **do** provide access to Confidential or higher organizational data must adhere to the requirements in section 3.1.

Wireless networks within labs or isolated environments that **do not** provide general connectivity to the corporate production network must still meet the following minimum requirements:

*   **Authentication & Encryption:** Must utilize, at minimum, WPA2/WPA3 Personal (PSK) with strong, complex passphrases compliant with the Password Policy. Open (unencrypted/unauthenticated) wireless networks are strictly prohibited if handling any organizational data or connected to any equipment processing such data.
*   **Network Isolation:** Must be demonstrably segregated from the corporate production network (e.g., via air gap or dedicated firewalls configured according to organizational standards). Any connection between lab/isolated networks and the corporate network requires explicit approval and security review by the designated IT authority (e.g., Precision Computer team, Lab Security Group).
*   **Device Management:** Default administrative credentials must be changed. Firmware should be kept updated.
*   **(Placeholder: Add any other specific lab/isolated requirements).** Adherence to specific Lab Security Policies is also required.

3.3 Requirements for Home/Remote Wireless Access

Connecting to the organization's network from a home or remote location via wireless must be done securely:

*   **Direct Network Access:** Wireless infrastructure devices (home routers) providing *direct* authenticated access to the organization's corporate network (e.g., via a hardware VPN tunnel directly terminating on the home router) must themselves be secured according to standards defined by the designated IT authority. This typically includes using WPA2/WPA3 Personal (PSK) with a strong passphrase, changing default admin credentials, disabling insecure features (like WPS

PIN), and keeping firmware updated. *(Refer to a detailed "Home Wireless Standard" or similar document if available, or detail specific requirements here).*
*   **Standard Remote Access:** If a home wireless network does not meet the standards for direct corporate access, connections to the organizational network must only occur via the standard, organization-approved remote access solution (e.g., software VPN client running on the endpoint device). The security of the home Wi-Fi (using at least WPA2-PSK with a strong password) remains the user's responsibility but does not directly impact the corporate network in this scenario due to the VPN tunnel originating from the endpoint.

3.4 Unauthorized Devices

Connecting unauthorized wireless access points or routers to the organization's wired network is strictly prohibited. Personal devices acting as Wi-Fi hotspots must not be connected to the corporate wired network.

4.0 Compliance

4.1 Compliance Measurement

The designated IT authority (e.g., Precision Computer team) will verify compliance with this policy through various methods, including but not limited to, wireless network scanning, rogue AP detection systems, configuration audits of managed devices, security assessments, review of network logs, and investigation of reported incidents.

4.2 Exceptions

Any exception to the standards specified in this policy requires formal, documented justification, risk assessment, and advance approval from the designated IT authority (e.g., Precision Computer team or Information Security).

4.3 Enforcement

Non-compliant wireless devices may be disconnected from the network without notice. Violations of this policy by personnel may result in disciplinary action, up to and including termination of employment or contract, consistent with organizational procedures.

5.0 Definitions

*   **MAC Address (Media Access Control Address):** A unique identifier assigned to network interface controllers for communications at the data link layer. (While relevant to some wireless controls like MAC filtering, it's not a primary security mechanism required by this policy template).
*   **SSID (Service Set Identifier):** A name that identifies a specific wireless network.
*   **WPA2/WPA3 (Wi-Fi Protected Access versions 2 & 3):** Security protocols used to secure wireless networks. Enterprise modes use individual credentials via RADIUS; Personal modes use a Pre-Shared Key (PSK).
*   **EAP (Extensible Authentication Protocol):** An authentication framework used in WPA/WPA2/WPA3 Enterprise networks (e.g., EAP-TLS, PEAP).

*   **AES (Advanced Encryption Standard):** A strong encryption algorithm used within WPA2/WPA3.
*   **Rogue Access Point:** An unauthorized wireless access point connected to a network.

6.0 Related Policies

*   Acceptable Use Policy (AUP)
*   Password Policy
*   Remote Access Policy
*   Data Classification Policy
*   Lab Security Policy (if applicable)
*   Information Security Policy (Overall)
*   Baseline Workstation Configuration Standard (for client-side settings)

Wireless Communication Standard

1.0 Purpose

This standard defines the minimum technical requirements that wireless infrastructure devices (e.g., access points, routers) must meet to be authorized for connection to the organization's network. The objective is to ensure the security and integrity of the network by controlling wireless access and mitigating associated risks. Only devices meeting these standards, or those granted a formal exception, are permitted.

2.0 Scope

This standard applies to all employees, contractors, consultants, temporary staff, and other personnel of the organization and its subsidiaries. It covers any individual who installs, manages, or utilizes wireless infrastructure devices that connect to, or provide connectivity to, the organization's network infrastructure. This includes both corporate-managed and user-managed (e.g., home) wireless devices used for accessing organizational resources.

3.0 Policy Statements

The following technical standards and requirements apply to all wireless infrastructure devices connecting to the organization's network:

3.1 General Requirements for Corporate Wireless Devices

All wireless infrastructure devices managed by the organization or connecting directly to the corporate network infrastructure, particularly those providing access to Confidential, Highly Confidential, or Restricted information (as defined by the organization's Data Classification Policy), must adhere to the following minimum security configurations:

*   **(Placeholder: Specific requirements need to be detailed here.** Examples might include: WPA2/WPA3 Enterprise authentication, specific EAP types like EAP-TLS or PEAP, disabling SSID broadcast for certain networks, strong administrative credentials, regular firmware updates, physical security considerations, prohibition of open/guest networks without proper segmentation, etc.)

3.2 Requirements for Home/Remote Wireless Devices Accessing Corporate Network

Wireless infrastructure devices located in remote or home environments that provide direct access to the organization's internal network (e.g., supporting hardware VPN connections or specific

teleworker solutions) must meet the following minimum security standards:

* **(Placeholder: Specific requirements need to be detailed here.** Examples might include: WPA2/WPA3 Personal (PSK) with strong, complex passphrases, changing default administrative credentials, enabling network encryption, disabling UPnP, keeping firmware updated, ensuring the device is physically secure, etc.)

3.3 Approval and Exceptions

Only wireless infrastructure devices that meet the requirements specified in this standard are approved for connectivity. Any exception must be formally documented, justified, and approved in advance by the designated IT authority (e.g., Precision Computer Team).

4.0 Compliance

4.1 Compliance Measurement

The designated IT authority (e.g., Precision Computer Team) will verify compliance with this standard through various methods, including but not limited to network scanning, device configuration audits, log reviews, physical inspections, and analysis of security tool reports. Findings will be reported to the policy owner and relevant management.

4.2 Exceptions

As stated in section 3.3, any exception to this standard requires formal, documented justification and advance approval from the designated IT authority (e.g., Precision Computer Team).

4.3 Enforcement

Failure to comply with this standard may result in the disconnection of non-compliant devices from the network. Violations by personnel may lead to disciplinary action, up to and including termination of employment or contract, consistent with organizational procedures.

5.0 Definitions

For clarity, the following terms are relevant to this standard. Further definitions can often be found in established industry security glossaries:

* **AES (Advanced Encryption Standard):** A strong symmetric block cipher algorithm used for data encryption.
* **EAP (Extensible Authentication Protocol):** An authentication framework often used in wireless networks (e.g., EAP-FAST, EAP-TLS, PEAP).
    * **EAP-FAST (Flexible Authentication via Secure Tunneling)**
    * **EAP-TLS (Transport Layer Security)**
    * **PEAP (Protected Extensible Authentication Protocol)**
* **SSID (Service Set Identifier):** A name that identifies a wireless network.
* **TKIP (Temporal Key Integrity Protocol):** An older encryption protocol used with WPA; now

considered less secure than AES.
*   **WPA-PSK (Wi-Fi Protected Access - Pre-Shared Key):** A security protocol using a shared key for authentication, commonly used in home networks (also known as WPA/WPA2/WPA3 Personal).

Workstation Security (For HIPAA) Policy

1.0 Purpose

The purpose of this policy is to establish security standards and provide guidance for the use of all workstations accessing organizational resources. The objectives are to ensure the confidentiality, integrity, and availability of information processed or accessed by workstations, including sensitive data such as Protected Health Information (PHI). This policy also aims to ensure compliance with relevant regulatory requirements, such as the workstation security standards mandated by the HIPAA Security Rule (164.310(c)), where applicable.

2.0 Scope

This policy applies to all employees, contractors, workforce members, vendors, and agents of the organization utilizing any workstation (whether organization-owned or personally-owned) that connects to the organization's network or is used to access, process, or store organizational information.

3.0 Policy Statements

All individuals subject to this policy must adhere to the following workstation security requirements:

3.1 General Security Awareness and Responsibility

* Users must always consider the sensitivity of the information being accessed or displayed on their workstation, particularly PHI or other confidential data, and take active steps to prevent unauthorized viewing or access.
* Workstations are provided for authorized organizational business purposes only. Personal use should be minimal and comply with the Acceptable Use Policy.

3.2 Access Control and Physical Security

* Workstations must be physically positioned and secured to minimize the risk of unauthorized access or viewing of sensitive information. Consider the use of privacy screen filters or other physical barriers where appropriate.
* Physical access to workstations must be restricted to authorized personnel only.
* Workstations must be secured (e.g., screen locked or logged out) whenever the user leaves the immediate vicinity, even for brief periods.
* A password-protected screen saver with a short inactivity timeout period must be enabled.

Passwords must comply with the organization's Password Policy.
* Laptops containing sensitive information must be physically secured when unattended, using methods such as cable locks or storing them in locked drawers or cabinets.

3.3 Technical Safeguards and Configuration

* All workstations must comply with the organization's Baseline Workstation Configuration Standard.
* Only organization-approved software may be installed on workstations. Installation of unauthorized software is strictly prohibited.
* Sensitive information, including PHI, should primarily be stored on designated, secure network servers, not local workstation drives, unless explicitly permitted and adequately protected (e.g., through encryption).
* Workstations must comply with the Portable Workstation Encryption Policy, ensuring sensitive data stored locally is encrypted.
* Workstations must utilize appropriate power protection, such as a surge protector or an uninterruptible power supply (UPS/battery backup).
* If wireless network access is used, it must adhere to the security requirements outlined in the Wireless Communication Policy.

3.4 User Practices

* Keep food and liquids away from workstations to prevent accidental damage.
* Before leaving for extended periods (e.g., end of day), users should exit running applications and close open documents where practical, and ensure the workstation is left powered on but logged off to facilitate necessary after-hours maintenance and updates by IT personnel.

4.0 Compliance

4.1 Compliance Measurement

The designated IT authority (e.g., Precision Computer team) will verify compliance with this policy through various methods. These may include, but are not limited to, periodic physical inspections (walk-thrus), review of system logs and configuration settings, security audits (internal and external), and analysis of reports from security tools. Feedback will be provided to the policy owner and relevant management.

4.2 Exceptions

Any exception to this policy requires formal, documented justification and advance approval from the designated IT authority (e.g., Precision Computer team).

4.3 Enforcement

Failure by any individual subject to this policy to adhere to its requirements may result in disciplinary action, up to and including termination of employment or contract, consistent with organizational procedures. Access privileges may also be modified or revoked.

5.0 Related Policies and Standards

Users should familiarize themselves with the following related organizational documents:

* Acceptable Use Policy
* Password Policy
* Portable Workstation Encryption Policy
* Wireless Communication Policy
* Baseline Workstation Configuration Standard
* Data Classification Policy (Implied reference via "sensitive information")