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.

Revision #1
Created 1 May 2025 19:57:22 by Travis Woolery
Updated 16 September 2025 22:10:08 by Travis Woolery