Data Protection Policy

CurrentClient

Purpose

This policy outlines many of the procedures and technical controls in support of data protection.

Scope

Production systems that create, receive, store, or transmit CurrentClient customer data (hereafter "Production Systems") must follow the requirements and guidelines described in this policy.

Roles and Responsibilities

- The COO is responsible for updating, reviewing, and maintaining this policy.
- The COO and CTO are both responsible for the implementation of data safeguards.
- The COO and CTO are both responsible for log management.
- The COO is responsible for enforcing the requirements of this policy.

Policy

CurrentClient policy requires that:

- Data must be handled and protected according to its classification requirements and following approved encryption standards, if applicable.
- Whenever possible, store data of the same classification in a given data repository and avoid mixing sensitive and non-sensitive data in the same repository. Security controls, including authentication, authorization, data encryption, and auditing, should be applied according to the highest classification of data in a given repository.
- All Production Systems must disable services that are not required to achieve the business purpose or function of the system.
- All access to Production Systems must be logged.
- All Production Systems must have security monitoring enabled, including activity and file integrity monitoring, vulnerability scanning, and/or malware detection, as applicable.

Data Protection Implementation and Processes

Customer Data Protection

CurrentClient hosts on Amazon Web Services (AWS) in the U.S. Oregon region by default. The U.S. N. Virginia region is also used for certain services such as content delivery. Data is replicated across multiple availability zones for redundancy and disaster recovery.

All CurrentClient employees adhere to the following processes to reduce the risk of compromising Production Data:

- Implement and/or review controls designed to protect Production Data from improper alteration or destruction.
- Ensure that confidential data is stored in a manner that supports user access logs and automated monitoring for potential security incidents.
- Ensure CurrentClient Customer Production Data is segmented and only accessible to Customers authorized to access data.
- All Production Data at rest is stored on encrypted volumes using encryption keys managed by AWS.
- Volume encryption keys and machines that generate volume encryption keys are protected from unauthorized access. Volume encryption key material is protected with access controls such that the key material is only accessible by privileged accounts.

Separation

Customer data will be logically separated at the database/datastore level using a unique identifier for the customer. The separation is enforced at the API layer where the client must authenticate with a chosen account and then the customer unique identifier is included in the access token and used by the API to restrict access to data to the account. All database/datastore queries then include the account identifier.

Data Leakage Prevention

CurrentClient will implement data leakage prevention mechanisms to systems that process, store or transmit sensitive information. These mechanisms will be configured to prevent data leakage (e.g., through email or other messaging technologies) and generate audit logs and alerts.

Monitoring

CurrentClient uses services provided by AWS such as CloudWatch, CloudTrail, and Config to monitor the entire cloud service operation (monitoring and internal reporting capabilities are used to report on cryptographic operations, encryption, and key management policies, processes, procedures, and controls). If a system failure and alarm is triggered, key personnel are notified by text, chat, and/or email message in order to take appropriate corrective action.

Confidentiality/Non-Disclosure Agreement (NDA)

CurrentClient uses confidentiality or non-disclosure agreements to protect confidential information using legally enforceable terms. NDAs are applicable to both internal and external parties. NDAs will have the following elements:

- Definition of the information to be protected
- Duration of the agreement
- Required actions upon termination of agreement
- Responsibilities and actions to avoid unauthorized disclosure
- Ownership of information, trade secrets and intellectual property
- Permitted use of the confidential information and rights to use information
- Audit and monitor activities that involve confidential information
- Process of notification and reporting of unauthorized disclosure or information leakage
- Information return or destruction terms when agreement is terminated
- Actions in case of breach of agreement

- Periodic review

Data At Rest

Encryption

All databases, data stores, and file systems are encrypted according to CurrentClient's *Encryption Policy*.

Data in Transit

Necessity

Data will only be transferred where strictly necessary for effective business processes.

Encryption

To ensure the safety of data in transit:

- All internet and intranet connections are encrypted and authenticated using a strong protocol, a strong key exchange, and a strong cipher.

Movement of Media

- Media with sensitive data sent outside the company's facilities will be logged, securely transmitted (e.g., via secure courier or other trackable method), and captured within offsite tracking logs to include details about media location.
- Management will approve all media with sensitive data that is moved outside the facility (including when media is distributed to individuals). Documentation of management's approval for the movement of media will be retained.
- Packaging of media will be sufficient to protect the contents from any physical damage during transport and in accordance with any manufacturers' specifications.
- Inventory logs of all electronic media with sensitive data will be maintained.
- Removable media devices, such as USB drives, digital video disks, compact disks, external or removable hard disks, etc., that contain sensitive data will be encrypted to protect the confidentiality of the information during movement.

End-user Messaging Channels

- Restricted and sensitive data is not allowed to be sent over electronic end-user messaging channels such as email or chat, unless end-to-end encryption is enabled.

Revision History

Version	Date	Editor	Approver	Description of Changes	Format
V1	5/15/25	Andrew Clark	Andrew Clark	Initial policy.	.PDF

V1.1	7/22/25	Andrew Clark	Andrew Clark	Updates to roles and responsibilities, removed data deletion section.	.PDF