

Client Security Requirements

Revision History

Version	Date	Author	Revision
1.0	2025-10-16	WNE	Initial draft

Document Information

Title	Client Security Requirements
Author	Information Security
Document Owner	Information Security
Document Approver	TBD
Document type	Policy
Target audience	Cleverbridge Clients
Classification	Public

Table of Contents

Purpose and scope	3
Authentication and credential management	3
Password handling	3
API key and token handling	4
Access control and user management.....	4
Principle of least privilege	4
User onboarding and offboarding	4
Network and system security	5
Secure Communications.....	5
Secure coding and integration practices	5
Input validation and sanitization.....	5
Logging and monitoring	5
Data protection and privacy.....	6
Data minimization	6
Encryption	6
Data retention.....	6
Incident response and reporting	6

Purpose and scope

This policy defines security controls and practices that all Cleverbridge clients must implement when interacting with Cleverbridge systems (Applications, APIs, and services). It applies to all client-operated systems, personnel, and applications that process, transmit, or store data exchanged with Cleverbridge. Failure to implement these controls and practices constitutes misuse of the Online Store and a security failure under the Agreement.

Authentication and credential management

Password handling

- All users with access to Cleverbridge systems must use unique, strong passwords for these systems. The passwords must satisfy the following requirements:
 - At least 12 characters long.
 - Complex (mixture of uppercase- and lowercase letters, numbers and special characters).
- Alternatively, the user can employ a unique and strong passphrase that satisfies the following requirements:
 - Contain at least four unrelated words forming a minimum length of 20 characters.
 - Is easy for the user to remember but hard for others to guess.
 - Avoids the use of personal information, predictable sequences, or common phrases.
- Passwords must never be transmitted, logged, or stored in plaintext, including within scripts or client-side code.
- A password manager (e.g., 1Password, Bitwarden, or similar enterprise SSO vaults) must be used to store the password or passphrase securely.
- Credentials must **not** be shared between users; each user must have a unique account.
- Passwords must be rotated or changed immediately if compromise is suspected.
- Passwords should be rotated or changed at least annually.
- Clients must not hardcode passwords into scripts, integration logic unless necessary.

- Cleverbridge suggests following identity management/password security best practices like NIST SP 800-63B.

API key and token handling

- API keys/tokens that allow access to Cleverbridge systems and/or data:
 - Must be stored securely (never in source code or version control).
 - Should use environment variables, secure configuration files, or secret vaults (e.g., AWS Secrets Manager, HashiCorp Vault, Azure Key Vault).
 - Should be rotated at least every 90 days.
 - Must be rotated immediately upon personnel changes, if those personnel had access to the API key/token.
 - Must be transmitted only over HTTPS (TLS 1.2 or higher).
- API credentials and interactive login credentials should be logically separated to reduce misuse risk.
- Cleverbridge advises using individual API credentials for separate integrations or workflows. Each credential should grant only the access required for its specific function, aligning with the principle of least privilege.
- The client must immediately revoke and replace credentials suspected of compromise and immediately inform Cleverbridge of any suspected compromise.

Access control and user management

Principle of least privilege

- Access to systems (e.g., CA/SCM) and data must be restricted to individuals whose roles require it.
- Administrative access should be separated from normal user accounts and should be granted only on a need-to-know basis.
- Administrative accounts should not be used for day-to-day operations.

User onboarding and offboarding

- Clients are required to:

- Maintain an access control list of users authorized to interact with Cleverbridge.
- Immediately revoke access (API keys, credentials, SSO, etc.) upon employee departure or role change (given the role change alters the required access to Cleverbridge systems).
- Perform bi-annual reviews of all user accounts and permissions.

Network and system security

Secure Communications

- All client-to-server communication must occur over **TLS 1.2 or higher**.
- Deprecated or insecure protocols (e.g., SSL, TLS 1.0/1.1, HTTP without TLS) are prohibited.
- Certificates must be issued by trusted Certificate Authorities and renewed before expiration.
- Certificate validation must not be disabled, to avoid man-in-the-middle attacks.

Secure coding and integration practices

Input validation and sanitization

- Client systems must validate and sanitize all data before sending to Cleverbridge to prevent injection, deserialization, or cross-site scripting attacks.

Logging and monitoring

- Logs must not contain credentials, API keys/tokens, or personal data unless absolutely necessary for troubleshooting.
- Access and authentication events should be logged and monitored for anomalies.

Data protection and privacy

Data minimization

- Clients must only collect and transmit data necessary for their integration or transaction purpose.
- Unnecessary storage or replication of sensitive data should be avoided.

Encryption

- Sensitive data at rest must be encrypted using AES-256 or an encryption standard with equivalent security.
- Data in transit must always use HTTPS/TLS.
- Encryption keys must be managed and stored securely, separate from encrypted data.

Data retention

- When processing Cleverbridge data, the Client must:
 - Retain the data only as long as required for operational or regulatory purposes.
 - Implement secure deletion processes for obsolete or expired data.

Incident response and reporting

- Clients are required to:
 - Notify Cleverbridge within 24 hours of discovering a security incident that may affect systems or data related to Cleverbridge.
 - Cooperate fully in incident investigation and remediation.
 - Provide audit logs and relevant data upon request for incident validation.
- Clients should maintain an internal incident response plan aligned with industry standards.