GeoVision GV-Cloud Data Encryption & Security

1. Security Overview

GeoVision GV-Cloud is built on a “Security-First” philosophy, providing a highly protected cloud-based Video Management System (VMS) and Access Control platform for enterprises. The security architecture is founded on proactive vulnerability management, stringent identity authentication, and compliant data processing principles to meet internal audits and international privacy regulations.

2. Security Architecture

GV-Cloud utilizes a hybrid cloud architecture designed to minimize the attack surface.

- **Outbound-Only Connectivity**: Edge devices (cameras, controllers, bridges) only require an outbound connection to communicate with the cloud. In most cases, there is no need to open Port-forwarding or configure Inbound routing on the enterprise firewall, significantly reducing exposure to external attacks.
- **Defense-in-Depth**: Separation is maintained across the device, transmission, and application layers to ensure that a compromise at a single point does not propagate throughout the entire network.

3. Authentication Mechanism

Multiple protection measures are implemented to ensure only authorized personnel access sensitive data:

- **Multi-Factor Authentication (MFA/2FA)**: Supports secondary login verification via SMS or Email to prevent unauthorized account access.
- **Strict Password Policy**: Passwords must be at least 8 characters long and include characters from at least three of the following categories: uppercase letters, lowercase letters, numbers, and special characters.

4. Authorization & Access Control

GV-Cloud features a granular Role-Based Access Control (RBAC) system:

- **Multi-Tier Roles**: Includes Master User (full access), Region Manager, and Normal User roles.
- **Regional Privilege Assignment**: Region Managers can be assigned to manage hosts and cameras only within their designated organizational Regions.
- **Feature-Level Permissions**: Access to Live View, Playback, PTZ, Audio, or Download controls can be precisely defined for each user.

5. Data Encryption in Transit

GV-Cloud ensures that all communications between devices and the cloud are encrypted:

- **Encryption Protocols**: TLS 1.2 / TLS 1.3, HTTPS, and Secure WebSocket (WSS) are used to protect live streaming and platform communications.

6. Data Encryption at Rest

- **Cloud Data Protection**: All video clips stored in the cloud data centers are encrypted.
- **Encryption Algorithms**: AES-256 is used for data at rest.

7. Data Storage Protection

- **Data Residency**: Regional data centers are located in the US and the EU. The system automatically detects the IP location of the connecting device and stores data in the nearest appropriate compliant region.
- **Lifecycle Management**: Video and logs are cyclic-overwritten or permanently deleted based on authorized retention plans (e.g., 3/7/15/30-day video or 90/180/365-day log retention).

8. Audit Logging

GV-Cloud provides comprehensive audit tracking:

- **Audit Log**: Detailed records of all administrator activities, including login/logout times, source IP addresses, password changes, and privilege adjustments.
- **Access Event Auditing**: Preserves all access card events, alarm triggers, and video viewing records to ensure full traceability.

9. Security Monitoring

- **System Health Monitoring**: Real-time monitoring of connection status, storage status, and hardware operational health.

10. Vulnerability Management

As a **CVE Numbering Authority (CNA)**, GeoVision possesses world-class vulnerability handling capabilities:

- **4-Stage Lifecycle**: Discover > Analyze > Prioritize > Solution Update.
- **Rapid Updates**: Based on GeoVision's CNA-level cybersecurity policy, edge devices quickly receive security patches and firmware enhancements to maintain a secure operational state.

11. Incident Response

- **Dedicated Security Team**: A specialized email (security@geovision.com.tw) is available for external vulnerability reporting.
- **Emergency Response**: Supports "Lockdown" to reject all access requests during security incidents, and "Force Authentication Mode" to override default unlocked settings.

12. Security Best Practices

To ensure maximum security, enterprise customers are encouraged to:

1. Enforce 2FA/MFA for all users.
2. Regularly review Audit Logs and user permission assignments.
3. Issue time-limited "Dynamic QR Codes" for visitors.