Information Security Framework

Protective measures create peace of mind.

Technology Brief

Protecting Your Data Is Our Goal

At GTL, we take information security and data protection very seriously. That's why we've gone to exceptional lengths to safeguard each customer's data and private information that is generated through the course of their relationship with us. Our security architecture provides our customers the reassurance that their data won't fall into the wrong hands.

Data Access

Correctional facilities access their call detail records (CDR) and call recording data through GTL's facility management system. This web-based, graphic user interface (GUI) requires a username and password for access. Once logged in, each account has an associated Security Level which defines the capabilities of that user. This permits correctional facilities to control employees' access to data.

Two-factor authentication is required for access to the cardholder data environment (CDE). This means that beyond the use of a username and password, employees attempting to access this environment must also have an Authentication Matrix card that requires them to engage a matrix for challenge and response security questions. This ensures that access to the CDE is still protected even if an authorized employee's username and password is stolen because the attacker would also need access to the employee's physical security card.

GTL is always working to improve its Security Architecture, and the following efforts are currently underway to further expand its user access security controls:

- **two-factor authentication for all remote access to GTL networks**
- **host integrity checks on all remotely connecting devices to ensure specific security controls are in place on the connecting device**
- **two-factor authentication for accessing corporate data**

Data Transport

Consistent with industry best practice, all data stored and retrieved using the GTL Facility Management System is transported using Transport Layer Security (TLS) that encrypts inbound and outbound data during transmission.

Data Center Electronic Access

Electronic access to GTL Data Centers is limited exclusively to GTL customers. In addition, controls are in place to limit access only from specific IP addresses. This means that access to customer data will be denied if a request is from an unknown IP address.

Furthermore, multiple layers of 128-bit encryption and perimeter firewall protection prevent unauthorized access from the Internet. The encryption of data streams also keeps inmate information, recordings, and customer data from being compromised while in transit.

Data Center Physical Access

All GTL Data Center access is restricted by a centralized badge system that uses 26-bit access badges. These badges are unmarked to ensure that if one is lost it could not be associated with GTL systems. Only employees are permitted access to GTL Data Centers. Furthermore, administrator access to the badge system is only provided to a select group of employees who are responsible for managing facility and data center access.

In addition to controlled access, all ingress and egress doors at GTL Data Centers are monitored by CCTV cameras that record 24/7 to a centralized DVR management system. The centralized DVR system stores at least three months of recordings of all data centers and facilities. Cameras are also located in GTL Data Centers to monitor activities inside the data center.

CDRs and Recordings

CDRs and call audio recordings are separated and stored on independent and diverse enterprise storage devices. These storage devices only interact with certain servers within the data center. Finally, user names and passwords are used with the storage devices wherever possible.

Monitoring, Logging, and Scanning

The GTL Facility Management System Solution tracks and logs all access to the inmate telephone platform, media storage system, and WAN. The firewall that protects the WAN logs any sessions coming through a GTL server, and the networking software logs any user sessions at the application level. This permits management and tracking of all logins. Any login attempts that are not authorized are immediately flagged and checked against the approved user list.

A robust centralized log monitoring solution provides alerts to the GTL Information Security Department based on predefined and internally developed alarm rules. This application is monitored to detect other anomalies that might indicate inappropriate use of GTL assets. Any time a user logs into the system, the system notes the event and the user's identity in the system's electronic Log Book. An Audit Log Report is used by GTL to track and investigate user access and record all system changes and activities that take place while each user is logged into the system.

Monthly internal and external vulnerability scanning and annual penetration testing is performed by the GTL Information Security Department and a PCI-approved scanning vendor. Vulnerabilities are promptly remediated based on level of risk. Risk is determined through the use of the Common Vulnerability Scoring System rating and knowledge of the systems. While Payment Card Industry Data Security Standard (PCI-DSS) Compliance requirements only require that GTL perform this testing quarterly, GTL goes the extra mile and performs the testing on a monthly basis.

GTL uses industry accepted log monitoring software to perform file integrity monitoring and to provide real time monitoring of application, security, and system event logs. Using this log monitoring software, the GTL Information Security Department monitors log events 24/7 and investigates all alerts.

Processes and Procedures

Among other responsibilities, GTL's Network Operations Center and Information Security Department ensure:

- **The technology platform behind our Offender Management System (OMS)—as well as all our any changes to firewall hardware or software or security rules are approved by GTL's Information Security Department, follow all change control policies and procedures, and are properly documented;**
- **vulnerability scans are performed on all servers before they are moved into a production environment and prior to the approval of any network access control lists (ACLs);**
- **after any change, network diagrams are reviewed and updated to ensure they accurately describe all connections to confidential or sensitive information and critical network protection mechanisms;**
- **active daily monitoring of the logs that report security events;**
- **active daily monitoring of system and application-specific alerts on critical systems; and**
- **notification of the appropriate parties and execution of appropriate procedures in the event of a security system failure or a security event.**

Network and Data Security

All sites are protected by a "stateful" packet inspection firewall. In addition, access control lists (ACLs) limit all inbound and outbound traffic to GTL-specific networks, which include the IP address for GTL Data Centers, GTL web applications, and customer-specific network IP addresses.

GTL creates a virtual private network for all facilities, using Internet Protocol Virtual Private Network (IP VPN) technology. All sites are connected to the data centers using 128-bit AES or 3DES encrypted data links so that all validation, call records, and recordings are encrypted when they traverse this network.
Facilities with remote workstations or cellular wireless broadband networks also use IP VPN and are protected by a firewall.

The Internet-facing Facility Management system is only available over a Secure Sockets Layer (SSLv3) to ensure that all traffic is encrypted and meets security best practices. Controls are also available to allow access only to specific IP addresses. This allows control over access to the GTL's Facility Management system by outside agencies and individuals.

GTL's robust network topology prevents intrusion from external sources:

- **Intrusion Prevention Systems are deployed to alert the GTL Information Security Department to potential attacks and automatically block such attacks.**
- **Firewalls use ACL rules to manage network traffic and block unauthorized access.**
- **A Wireless Intrusion Prevention System is deployed at all GTL office locations throughout the country to alert and prevent against the installation of rogue wireless access points. This system also ensures that only authorized employees have access to GTL wireless networks. No wireless networks are permitted to be attached to the LAN. Wireless networks are strictly used to provide guest Internet access.**

All backup tapes are encrypted before they are sent for off-site storage. It should be noted that PCI only requires that tapes are stored in a "secure location." Taking the extra step of encrypting the tapes ensures that regardless of its location, the data on the tapes is not accessible to unauthorized persons.

Credit Card Data

When GTL stores its most critical information, this data is encrypted at rest using an industry best practice Key Encryption Appliance. The keys used to encrypt the data never leave the appliance, which means that data can only be decrypted programmatically through the use of multiple layers of authentication.

File integrity monitoring is in place on all servers that process, transmit, or store credit card information. This ensures that the GTL Information Security Department is alerted to all unauthorized modifications of critical system files and internally developed software.

Virus and Malware Security

Anti-virus detection is installed on all internal GTL servers and workstations. This anti-virus solution is centrally managed and alerts the Technology Group and GTL's third-party monitoring company when viruses are detected or security policies are not adhered to.

Intrusion Prevention Systems are deployed to alert the GTL Information Security Department to potential attacks and automatically block such attacks. Many companies choose to rely on an Intrusion Detection System that simply alerts of potential attacks, but GTL's systems automatically block suspected malicious traffic.

A robust centralized log monitoring solution provides alerts to the GTL Information Security Department based on predefined and internally developed alarm rules. This application is monitored daily to detect other anomalies that might indicate inappropriate use of GTL assets.

Equipment

All GTL equipment is hardened to ensure it comports with today's security best practices. This includes operating system hardening, point-to-point credit card data encryption, application source code auditing, log monitoring, automated patching, anti-virus, and physical security controls.

Knowledge and Training

GTL is one of the first organizations in the country with employees who have been certified by the Payment Card Industry (PCI) Security Standards Council as Internal Security Assessors (ISA). This ensures that GTL's system operations security, system access security, and PCI compliance security efforts are held to the highest benchmarks and that PCI security standards are designed into GTL applications and not merely applied ad hoc after the fact. In addition, all GTL employees are required to attend annual security awareness training to reinforce all GTL policies and procedures.