GCI'S SECURITY POSTURE

We take security very seriously.

The control environment at GCI is the foundation for the controls used in support of GCI business operations and customer service. It sets the tone for the organization and influences the control consciousness of its personnel.

As part of the security program, the Enterprise Security Office (ESO) is responsible for 1) identifying all relevant legal and regulatory security controls and staying abreast of any changes, 2) assisting business units in the implementation of required controls, 3) supporting internal and external audits of security controls conducted on at least an annual basis and 4) tracking issues of non-compliance.

Risk Assessment

The ESO is responsible for managing and enforcing the Information Risk Management Policy, which outlines the requirements and frequency of risk management activities.

System Monitoring

Monitoring systems are in place at GCI's data centers to capture customer connectivity, bandwidth utilization, packet loss and latency, and central processing unit (CPU) utilization on core routers and switches. Capacity and performance information is pulled from customer systems on an on-going basis and monitored by GCI personnel. GCI uses network management tools to proactively monitor the network infrastructure services provided by GCI and its affiliated organizations on a 24/7/365 schedule..

Security & Confidentiality Monitoring

Security and confidentiality events are monitored and observed by various means including but not limited to: automated methods using enterpriseclass security tools, analysts monitoring networks and applications, and communication from other GCI departments to the Security Operations Center (SOC). Network monitoring, logging, and email security software are monitored daily by SOC analysts and events are triaged and tracked by the appropriate personnel.

Control Monitoring

All regulatory requirements and laws applicable to GCI, as well as industry best practice standards, are consolidated in the GCI Control Framework. The framework is the foundation for all security policies and controls managed or enforced by the ESO. Maintenance of the framework requires continuous monitoring to ensure the relevance and applicability of included controls. When updates are required due to changes in the environment, legal or regulatory requirements, or identified risks, modifications are made to security policies, processes or controls.

Audits and/or gap assessments of security controls included in the framework are conducted at least annually by the ESO or external entities to measure progress and ensure effectiveness of controls. Audit details, such as scope, are determined based on operational needs, regulatory requirements, and the prioritization of risk. Gaps and issues of noncompliance are tracked by the ESO, communicated to stakeholders and relevant business units, and addressed based on criticality and business constraints.

Policy and Procedure

Formal policies have been developed to communicate accepted standards for technology and behavior. GCI's policies address requirements pertaining to security, confidentiality, privacy and availability of data. The ESO is responsible for the development, maintenance and enforcement of security policies. GCI's security policies include, but are not limited to, the following:

- Acceptable Use Policy
- User Password Policy
- Password Standard
- Confidentiality Policy
- Change Management Policy
- Security Incident Response Policy
- Information Risk Management Policy
- Vulnerability Management Policy
- Third Party Security Risk Management Policy
- Encryption Policy
- Physical Security Policy
- Mobile Devices Policy

Network Security

Firewall systems are in place to filter unauthorized inbound traffic from the internet and deny any types of network connection that is not explicitly authorized. Network monitoring tools are in place to detect unauthorized access to the network. Alerts are monitored daily by the SOC for follow-up and remediation. Logging and monitoring software is used to collect data from system infrastructure components and detect unusual system activity. Information captured by the logging software is reviewed on a daily basis by SOC analysts.

Anti-Virus

Anti-virus software is installed on workstations, laptops, and servers supporting such software. The virus definition lists and software engines are updated automatically and periodically. During the build process, an anti-virus agent and software are installed. Updates are pushed out automatically via the agent.

Software Whitelisting

Application whitelisting software is installed on all workstations to protect GCI information systems from the introduction of unauthorized and/or malicious software. Lists of authorized and unauthorized software is maintained by the SOC and used to configure the whitelisting software. Attempts to install software on the unauthorized list are blocked. Access Control and Authentication

Systems are configured to authenticate users with a unique user account and password, when technically feasible. Infrastructure components and software are configured to use the active directory single sign-on functionality when available. Infrastructure components and software not configured to use the active directory single sign-on functionality require a separate user ID and password.

Remote access by personnel is permitted only through a two-factor encrypted virtual private network (VPN) connection. Vulnerability Management Vulnerability monitoring scans are performed on a scheduled and ad hoc basis, but at least monthly. Timing of patching vulnerabilities is included in the policy. Penetration testing is done at least once a year by a third party. Logging and monitoring software is used to collect data from system infrastructure components.

Incident Response

The Security Incident Response Plan is based on industry standards and is comprised of six phases:

1. **Preparation:** The preparation phase is used to prepare GCI systems and processes to better handle identified security breaches and issues.
2. **Identification:** The identification phase is aimed at determining if a security problem warrants further analysis and constitutes a security incident.
3. **Containment Phase:** The objective during this phase is to identify and notify owners of systems at risk including the target system, whether it is a server, PC or network. The focus is to minimize the impact of the attack on the target system and the effect on similar systems.
4. **Eradication Phase:** During this phase, the cause and symptoms of the incident are identified in order to improve defenses and prevent future exploitation of the subject vulnerability.
5. **Recovery Phase:** The focus of the recovery phase is restoring and validating the integrity of the affected system.
6. **Follow-up Phase:** The follow-up phase is used to identify lessons that will help prevent the same type of attack in the future. The phase supports the continuous improvement of GCI's incident handling capabilities.

Records Management

The Records and Information Management program within GCI identifies vital records and establish record retention schedules based on legal and business requirements. The program implements industry standard records management practices within their business areas including the secure storage, use and disposal of information. Guidelines established ensure the protection of data that is used in development and testing environments. Data classifications are used to note the sensitivity of information and the authorized uses of such information.

Data Protection

An email security solution is in place to monitor all outgoing email content to identify and prevent the unauthorized distribution of GCI or customer data. The email security solution is configured to generate incidents and even quarantine emails when certain criteria are met. Emails that are quarantined generate a notification to the sender alerting them to the unauthorized nature of the attempted message.

Encryption

GCI has an established and documented Encryption Policy that sets the standards for protecting data throughout the organization. This policy describes the security standards to be applied to encrypting sensitive data for which GCI is responsible for maintaining. Policy is in place that prohibits the transmission of PII, which includes PCI and Customer Proprietary Network Information, over non-GCI facilities unless it is encrypted.

Physical Security

Physical Security, within the ESO, manages all aspects of physical security, including the operational procedures, security officer staffing, third party security patrols, badging, video surveillance systems, and physical security designs and improvements for GCI facilities.

GCI employs a variety of physical security measures to provide the level of security necessary to protect its facilities, including the systems that support service to customers and customer-owned hardware. In its multilayered physical security program, GCI relies on security guards, CCTV surveillance, computer-based access control/alarms systems, two factor authentication, and restricted key systems.

Employee Physical Access

GCI badges are issued to employees and contractors as part of onboarding. Badges include a photo and a first name but no GCI-related insignias, logos, or department names so as to appear anonymous if found by a non-GCI party. The sharing of badges between individuals for any purpose whatsoever is strictly prohibited.

Change Management

GCI has an established Change Management Policy that states the requirements for all change management activities throughout the enterprise. Change request for upgrades, conversions, and changes applied to information systems must be documented and requested in a ticketing system or designated change management system. Change requests must include information such as a description of the change, classification based on impact, name of the individual performing the change, a unique change ID number, and the estimated time and date the change will be implemented. Approvals for all changes must be documented as part of the change request.

Third Party Security

GCI's Third Party Security Risk Management Policy states all third parties that will have access to GCI information or information systems must undergo a security review. Security reviews take into account the third party's ability to adhere to GCI's confidentiality requirements and offer an adequate amount of protection for the GCI information to which they will have access to.

2550 Denali St., #1000 | Anchorage, AK 99503
800.800.7754 | gci.com/business

About GCI: GCI provides data, wireless, video, voice and managed services to consumer and business customers throughout Alaska and nationwide. Headquartered in Alaska, GCI has delivered services for nearly 40 years to some of the most remote communities and in some of the most challenging conditions in North America. Learn more about GCI at www.gci.com. GCI is a wholly owned subsidiary of GCI Liberty, Inc. (Nasdaq: GLIBA, GLIBP). Learn more about GCI Liberty at www.gciliberty.com.