US SIGNAL®

SECURITY & COMPLIANCE

Partnering for More Effective IT Security and Compliance

201 Ionia Ave, Grand Rapids, MI 49503 | 866.2.SIGNAL | ussignal.com

PAGE
1

Table of Contents

v2.0
05.31.17

When you work with US Signal, you work with a partner committed to helping you employ a holistic IT security model. It's a partnership in which both of our companies take on clearly defined responsibilities for specific aspects of the IT infrastructure solutions deployed to help ensure the security and integrity of your company's data and applications. If your company is subject to compliance requirements for HIPAA/HITECH, PCI DSS or others, US Signal can help you with that as well.

Your organization is ultimately responsible for meeting its IT security and compliance requirements. However, that doesn't mean you have to go it alone.

Division of Responsibilities

It starts with communication. Your organization works with US Signal to mutually determine and agree to who will be responsible for each aspect of the IT infrastructure solution as it relates to security and any relevant compliance requirements. This includes defining and fully describing what is entailed for each responsibility and who is responsible; discussing the arrangements to ensure complete understanding on the parts of both parties; and then agreeing to the division of responsibilities in writing.

Customer Responsibilities

Your organization is responsible for managing the security of your data, applications and the operating system, as well as any of your equipment located in a US Signal data center.

Responsibilities include:

- Limiting access to the root account
- Encrypting data at rest and in transit
- Managing and controlling your encryption keys
- Abiding by US Signal security protocols at our data centers
- Managing the data center access list for your employees and vendors

**Customer-owned equipment refers your organization's hardware and other IT assets that may be colocated in a US Signal data center. US Signal is responsible for the physical security of our data centers but you are responsible for ensuring your equipment is secured within the data center and access to it is monitored. Responsibilities may vary if a you procure certain managed services from US Signal. For more information, contact US Signal.*

US Signal Responsibilities

The security of customer data is US Signal's number one priority. With a combined three levels of protection, your applications and data are guarded and defended from unauthorized access, cyber-attacks, and physical forces. Administrative Controls, Data Controls, and Infrastructure Controls work together to form a secure environment that allows you to rest easy.

Administrative Controls

Administrative Controls include compliance audits, internal audits, policies, and employee trainings that relate to the security of customer data. US Signal has undergone several audits and continuously to evaluates their security and compliance procedures.

SOC 1 Type 2

The Service Organization Control (SOC) 1 Type 2 Report is the result of an independent audit based on the SSAE 18 attestation standards developed by the American Institute of Certified Public Accountants (AICPA). The auditor tests and renders an opinion on the service organization's description of its systems, the suitability of the design, and operating effectiveness of controls over a period of time. US Signal completes a SOC 1 Type 2 audit annually. The most recent report was completed June 30, 2016, covering the previous 12 month period, with zero exceptions.

HIPAA

The Health Information Portability and Accessibility Act (HIPAA) stipulates over 100 controls that must be in place in order to be deemed compliant to the law. US Signal completes an independent audit yearly. A Report on Compliance (ROC) is issued, stating that US Signal's administrative, technical, and privacy controls align with HIPAA's security and privacy rules, and corroborates US Signal as a HIPAA Compliant organization. US Signal as appropriate signs Business Associate Agreements (BAA) with customers and vendors to formally agree upon and attest to compliance with the requirements of HIPAA Laws and Regulations.

PCI

The Payment Card Industry Data Security Standards (PCI DSS) are technical, administrative, and operational requirements which apply to all organizations that store, process, or transmit card holder data. US Signal has an annual audit with a PCI Security Standards Council certified Qualified Security Assessor (QSA) who validates adherence to all requirements of PCI DSS compliance, and the audit process result is a Report on Compliance (ROC). The ROC allows US Signal clients to navigate their compliance process with ease, since they are using the validated controls of US Signal to support their own audit process.

US Signal has developed an internal Vulnerability Management program and Internal Audit team to ensure compliance is maintained even when external auditors are not on-site. The Vulnerability Management program includes monitoring industry and vendor specific security feeds to ensure any recently released zero day or system security alerts are evaluated and patched appropriately. In addition, US Signal deploys Tenable's Security Center Continuous View and Nessus vulnerability scanner to internally conduct vulnerability scanning. All external sites are scanned by a PCI Approved Scan Vendor (ASV). All Vulnerability data is aggregated and reviewed utilizing the Kenna Security Intelligence platform combining 8 threat feeds to prioritize vulnerabilities against real world attack data.

US Signal employees receive recurring security and policy training, and monthly phishing assessments are conducted to keep employees educated about modern threats. All teams within US Signal that operate IT systems have patch management, change management, and hardening procedures defined for their specific team to ensure systems are current and secure. The internal audit team conducts physical site security audits, physical access audits, and risk assessment based IT system audits.

Internal Monitoring and Maintenance

US Signal has staffed an internal Security Operations Desk that is responsible for the day to day monitoring and response to potential security events. Information Security Analysts utilize the Log Rhythm SIEM platform along with other centralized logging and Anti-X monitoring platforms to detect potential threats and respond appropriately. IPS/IDS, Wireless Perimeter security, and physical security logging and monitoring are also monitored by the team. Hypervisors, portals, storage, networking, user activity, and firewalls are monitored via the SIEM platform for anomalous activity. An Incident Response Policy and Incident Response Team have been implemented and tested should an event escalate into an incident. The US Signal NOC Surveillance team also monitors for hardware or software failures and responds to any events detected.

Business Continuity and Disaster Recovery Plan

US Signal maintains a comprehensive BCDR plan that encompasses Incident Response, Business Continuance, and Disaster Recovery policies for Network, Cloud, and Enterprise environments. The policies are reviewed monthly and each component is exercised at least once annually including post event analysis, improvement discussions, and documentation updates. US Signal also deploys five BCDR trailers completely outfitted with supporting equipment in addition to having portable high watt generators so that equipment is able to be deployed 24/7/365 across their entire footprint should a disaster occur. A BCDR NOC is maintained in a separate physical location from the primary NOC and is able to be brought online in support of or in place of the primary NOC facility

Data Controls

Data Controls include the functions and actions that help support the confidentiality, integrity, and availability of US Signal and customer data. Least privilege access and role based access control are utilized to provide only the needed access for employees to complete their jobs. Data Retention and Destruction policies are maintained and employees are trained on the policies.

Encryption Support

US Signal encourages customer use of industry best practices to protect sensitive data and business critical information.

Customers are encouraged to reference the National Institute of Standards and Technology (NIST) developed special publications for encryption of data at rest and in-transit.

- NIST 800-111 standard for data at rest
- NIST 800-52 standard for data in transit

The storage that hosts US Signal Resource Pools utilizes Data At Rest Encryption at the hardware level so there is no taxation on your purchased resources. Furthermore, US Signal Hosted Private Cloud allows for an additional layer of encryption with optional self-encrypting drives that won't tax a customer's dedicated resources. Compliant customers should always encrypt their data separate from US Signal provided encryption.

Cloud Self-Administration

US Signal's Resource Pools are controlled by the customer through VMware's vCloud Director. This portal provides common sense security by enabling the customer to set the proper user roles and level of access for a business unit, department, or specific individual. Whether it is to the Resource Pool, groups of virtual machines or a single virtual machine, the granular controls allow the customer to be in control of who has specific access.

- Software-Defined Infrastructure - Create, provision, and manage your own virtual machines and virtual networks.
- Role-Based Access Control – Customers can utilize least privilege access principles and role based access to restrict or enable access rights based on job duties.
- Cloud User Logs - Task and event-based logging
- TOC Support- Compliance customers are required to provide additional authentication to access Technical Operations Center (TOC) support services.
- User Authentication - Supports Active Directory Federated Services which enables the customer to utilize their two factor authentication provider.

Architecture Fortification

US Signal's core network, fiber routes, and cloud infrastructure are built on redundant topologies to withstand multiple failures in both isolated and geographically diverse emergencies.

- DoS/DDoS Mitigation – Congestion-control mechanisms in place to protect nodes from failure during an attack.
- Natural Disaster – Proven and effective Disaster Recovery plan in place
- High Availability – Redundant and meshed systems in place to minimize customer downtime
- Data Destruction – Data Destruction meets compliance standards and is defined in each customers contract.

Infrastructure Controls

Infrastructure Controls include the infrastructure stability and environmental controls that protect the core of US Signal's network. The network is fully redundant and is housed in secure, alarmed facilities that meet HIPAA, PCI, and SSAE SOC 1 standards

- Data centers, Infrastructure, and networks are monitored 24/7/365 by a fully staffed Technical Operations Center (TOC)
- Equipment is housed in low profile, remotely located concrete and brick buildings
- Cloud Services are segregated in separate secure cages with restricted access.
- Access to all data centers is controlled using electronic key card or biometrics.
- All access activity is logged for 1 year and is monitored by the TOC and Security Operations Center (TOC).
- Visitor access is logged and stored for 1 year.
- 247 video cameras providing video surveillance logging for 1 year across all data centers.
- Integrated heat, fire, water, and smoke detection with dry agent fire suppression
- US Signal TOC 24x7 monitoring of fire, intrusion, water, and environmental alarms.
- Automated humidity and temperature controls with alarming
- UPS Battery Backup and DC Battery Plant
- Dual power grid feeds • Diverse fiber entrances and diverse laterals
- Full generator backup with auto start and auto transfer capabilities
- Minimum of 24-hour generator run time fuel capacity with guaranteed fuel delivery contracts

FAQs

The following are some of the questions we commonly receive from customers regarding our compliance and security programs. If you have a question that isn't covered here, don't hesitate to contact us.

How does US Signal ensure it is "compliant"?

Compliance requirements can vary greatly. To cover all bases, US Signal embeds compliance in our operational structure and processes.

- **Governance, Risk and Compliance (GRC) program** — features a designated executive security team that provides direction to the information security and compliance (ISC) officer who is accountable for the day-to-day physical, logical and cyber security of our entire company.
- **Internal vulnerability management program** — ensures compliance is maintained even when external auditors are not on-site. The vulnerability management program includes monitoring industry-and vendor-specific security feeds to ensure any recently released zero day or system security alerts are evaluated and patched appropriately.
- **Internal audit team** — conducts risk based audits of physical sites, IT systems, processes, to critical controls and system access audits quarterly.
- **Internal vulnerability scanning** — external approved scan vendor conducts quarterly vulnerability scans; penetration testing is conducted annually by a certified third party.
- **Employee security training** — all US Signal employees receive recurrent IT security training, and monthly phishing assessments are conducted to keep them up-to-date on current and emerging threats; all teams that operate IT systems have patch management, change management and hardening procedures defined for their specific teams to ensure systems are current and secure.

How does US Signal monitor and maintain its internal environment?

US Signal treats its internal environment like Fort Knox, employing tools and processes such as:

- An internal security operations desk that is responsible for the day-to-day monitoring of all US Signal systems and for responding to and/or mitigating potential security events.
- Highly trained information security analysts that utilize the Log Rhythm SIEM platform, along with other centralized logging and centralized anti-X monitoring platforms, to detect threats and respond appropriately.
- Host based intrusion detection, wireless perimeter security and physical security logging and monitoring with hypervisors, portals, storage, networking and firewalls monitored via the SIEM platform for anomalous activity.
- An incident response policy and incident response team, with tested procedures to help ensure that if an event escalates into an incident, the situation will be successfully handled.
- US Signal Network Operations Center (NOC) surveillance team, which monitors for hardware or software failures and responds to any events detected.

How does US Signal handle DDOS mitigation?

US Signal uses internal monitoring tools to constantly monitor our network. If it is believed that a DDOS event is occurring, engineers will initiate routing changes to protect the network and customers from a DDOS event.

Disclaimer: US Signal provides highly customizable IT infrastructure solutions. The inclusion of managed services or other factors may affect security and/or compliance responsibilities. Please contact US Signal for details.