Privacy Policy

Introduction

The SCE Group ("SCE") is a cybersecurity company committed to providing confidence in our customer's cybersecurity strategy, and expert level guidance with respect to the intricacies of identity and access.

The purpose of this Privacy Policy is to provide the recipient with an understanding of the Information Security and Contingency Planning Infrastructure (InfoSec) in place at SCE. The information contained in this Security Statement is for informational purposes only. This Security Statement does not and is not intended to create, add to or change any agreement between SCE and its clients, technology partners or vendors. Any binding terms, obligations, or warranties related to SCE products and/or services shall be in the form of signed, written agreements between SCE and its clients and technology partners. SCE reserves the right to make changes to this Security Statement and the topics covered any time without notice to existing or prospective clients and technology partners, unless otherwise stated in a signed, written agreement.

Services and Third-Party Service Organizations

SCE contracts with third parties to host its website. Customers host SCE's software. Third party VAR partners host their own services as do their Customers and End Users. This Security Statement only addresses SCE's InfoSec infrastructure and does not address or include descriptions of any other-service organizations' information security and contingency planning infrastructure that SCE's Customers or Technology Partners provide or utilize.

Personal Data Privacy

Our services do not collect, store or manipulate any personal information. Our corporate network also does not collect, store or manipulate any personal information. We do not purchase personal information from third parties, store it or send it out for marketing or sales purposes. The nature of the services provided by SCE does not expose SCE to personal data. SCE's Services are not intended or designed to access, transmit, transfer, touch, host and store any "personal data" as defined by applicable laws or regulations (such as without limitation, social security numbers, credit card data, driver's license numbers, national ID numbers, bank account numbers, health/medical information or any other personally identifying information). As a result, SCE requires that its Resellers, Customers and its Customers' End Users be prohibited from storing such private data with or in connection with SCE's Services. All private data accessible or stored by such third parties are limited to their respective servers and related equipment, and not those belonging to SCE.

SCE is not exposed to international private data which would otherwise be subjected to the General Data Protection Regulation 2016/679 of the European Union (as in force on the date of this Supplement and as amended from time to time hereafter, the "GDPR"). In the event any such personal data is disclosed in an unauthorized manner, or stored in a manner that is contrary to the above or contrary to any laws or regulations pursuant to federal, state, local or international laws or regulations, SCE has protocols in place to provide, as quickly as possible, notice and other necessary communications to the other party responsible for the unauthorized disclosure. In the event that personal data is disclosed outside of SCE's Services, such as payment or information requests, such data shall be stored, or deleted, pursuant to applicable laws and regulations.

In preparation for the upcoming GDPR effective date, SCE also conducted a thorough internal review on a department by department basis of processes, systems and policies, as well as scanned our internal systems for any personal data that fell within GDPR definitions. No applicable personal data was discovered or disclosed. Despite not falling within GDPR, SCE is conducting an in-depth reassessment and update of its InfoSec policies and procedures, including without limitation, data handling policies, data security, employee usage policies, network & application security, audits and remediation, device and physical security and access controls, disaster recovery, business continuity, and training to ensure SCE applies best practices.

Managerial Controls

1.1 Information Security Staff

SCE's Security Team is led by our Chief Information Officer. He supervises our security team, security infrastructure, security and related policy training, testing, and audit, which teams are comprised of the Vice President of Solutions Delivery and our Professional Services Engineers. The information security staff responsibilities include prevention, monitoring, reporting, maintaining, testing, and remediation.

1.2 Security policies, standards and maintenance

This Security Statement summarizes many of SCE’s security practices; but, is not an exhaustive list of practices. SCE has a formally documented set of security policies and guidelines. These policies have been approved and adopted by senior management and are published for all SCE employees to review and learn. As a condition of employment with SCE, all employees must agree to comply with and successfully be trained on these polices once per year. The security policies are reviewed on an annual basis for changes reflecting new technologies, business processes, best practices or changes in laws or regulations.

1.3 Employee provisioning and termination

SCE conducts background checks on all employees. Each position at SCE has an approved, written specific job description that allows for the proper level of access to be granted to the employee. Formal termination procedures, which apply to all employees when their employment with SCE ends, require immediate disabling of their access to SCE’s systems to reduce risk to the organization.

Operational Controls

1.4 Access Controls

SCE uses a combination of access restrictions to secure access to its data center and office buildings. SCE is currently developing a program to move all systems into a cloud-based system, to ensure that all activity is monitored centrally.

1.5 Environmental Protections

SCE requires several general practices for environmental controls of its equipment. Fire extinguishers, fire alarms, smoke detectors and battery backup systems are used.

1.6 Change Management

SCE maintains a formal change control process where all changes are tested, scheduled and approved by the proper management chain, along with project scheduling and management by our PMO.

1.7 Audit and log review

As a part of its commitment to a 100% cloud environment, SCE relies on the cloud provider's log monitoring and notification systems as a part of its audit and review activities. All active logs are logged and monitored by the cloud provider systems and then archived on a regular basis.

1.8 Risk Assessments

An SCE risk assessment (the "Review") is conducted by SCE's Professional Services Engineers. The CIO then reviews, analyzes and identifies enterprise-wide risks as defined by the Engineers. Risks are identified as well as any remediating factors that lessen risk. Key personnel throughout the technology department may be assigned to complete the review, alongside the CIO. Critical risks are presented to the Management Team for processing and resolution.

1.9 Business Continuity

As part of SCE's commitment to cloud computing, SCE's cloud architecture relies on deploying virtual computing resources in the cloud provider's multiple, physically separated and isolated data centers for disaster recovery and business continuity purposes, which makes SCE resources more highly available, fault tolerant, and scalable than traditional single data center infrastructures by utilizing physical and logical redundancy and backup as provided by the cloud provider itself.

1.10 Incident Response Team

SCE has assigned specific individuals to deal with incidents. This formal incident response team follows a detailed process and has documented procedures. The response plan addresses intruders, detection, communications, legal issues, containment strategies and lessons learned activities. Employees are trained to report incidents.

1.11 Compliance Efforts

In order to meet its applicable compliance obligations, SCE conducts an annual information security audit. Outstanding issues identified during an audit are prioritized for remediation.

Technical Controls

1.12 Network Infrastructure:

The network infrastructure for SCE systems is a hybrid enterprise class environment deployed in the cloud provider's multiple, physically separated and isolated data centers in a low latency, high throughput, and highly redundant networking. The hybrid network consists of multiple virtual private cloud networks for internal and external segments protected by the cloud provider's NAC technologies.

1.13 Internet and Remote Access

SCE has multiple internet carriers to support redundancy. Ingress/egress to the internet is protected by enterprise class, next generation firewalls. The least access principle is utilized to design any change in the rule base maintained by the security team. The firewall infrastructure provides egress URL filtering, file blocking and antivirus for IP conversations crossing its interfaces.

SCE uses an anytime/anywhere remote access via SSL VPN, which offers secure access the SCE cloud resources via multi-factor authentication, authorization, and enhanced endpoint inspection.

VPN connections are managed by an enterprise class VPN solution. Each VPN connection undergoes profiling and security checks before allowing a connection to its approved destination. Contractors use a separate VPN connection and are segmented from corporate users. VPN connections for contractors are firewalled to allow only explicitly defined conversations. Dial-up is not deployed in the environment. All VPN conversations are encrypted, regulated and closely monitored.

1.14 Information Security

The SCE Security Strategy is generally modeled after the SANS institute's 20 critical controls framework. Security infrastructure, processes and procedures are implemented and maintained to meet each objective of the framework. The security controls are frequently evaluated for gaps or advances in technology that could be addressed.

- **Inventory of Authorized and Unauthorized Devices**. SCE uses asset discovery tools, corporate approved images, network access controls, vulnerability assessment and auditing in order to control devices.
- **Inventory of Authorized and Unauthorized Software**. SCE uses an enterprise software delivery mechanism, census tools and a formal software licensing process to control software installations.

- **Secure Configurations for Hardware and Software on Workstations and Servers.** Endpoints are configured with an approved image. Each technology is secured by a crafted hardening guide. The Microsoft® GPO feature is used to both deploy and maintain security configurations on workstations and servers in the SCE environment. Auditing activities ensure hardening settings are maintained.
- **Secure Configurations for Network Devices.** Network devices are configured according to industry-based hardening guides. RADIUS-based authentication is used for all devices and vulnerability assessment procedures highlight any misconfigurations when equipment is deployed. Insecure protocols are not used.
- **Boundary Defense.** SCE uses enterprise-class firewalls in its boundary defenses.
- **Maintenance and Monitoring of Audit Logs.** SCE uses log collaboration and correlation technologies for events from production systems and network.
- **Application Software** SCE performs periodic web application penetration testing and automated vulnerability assessments against externally facing applications.
- **Controlled Use of Administrative Privileges.** SCE tightly controls the use of administrative privileges. Corporate assets are not deployed with users having extraordinary rights. Quarterly audit reporting is used to control any rights that were granted and not later revoked.
- **Controlled Access Based on Need to** SCE uses granular controls to allow for adequate separation of duties based upon each employee's role in the company. A formal provisioning team is established for administering rights.
- **Vulnerability Assessment and Remediation.** SCE uses a formal vulnerability assessment program in addition to a formal patch management program. Criticality of the findings from the assessment program are assigned by the security team and passed to the patching teams.
- **User Account Monitoring and Control.** The provisioning team uses written procedures for managing users. This process is continually audited.
- **Malware Defenses.** Several malware defenses are deployed: firewalls, IPS, IDS, on the network and at the endpoint. Malware logs are generated and centrally collected for actions if applicable.
- **Limitation and Control of Network Ports, Protocols and** SCE uses host based firewalls and hardening guides to limit and control network ports and services.

- **Wireless Device Control.** WPA2 enabled wireless network is available for corporate assets. Foreign devices will have “guest only” internet access available. NAC technology negates the installation of rogue access points.
- **Data Loss** Full disk encryption is used on SCE endpoints. In addition to encryption, SCE used de-identification technologies for data in testing environments.
- **Incident Response Capability.** A formalized SCE incident response team is in place to properly react to reported or discovered incidents. The team consists of core management from throughout the company.
- **Data Recovery Capability.** A formal backup program is in place. Data is replicated in a near real-time fashion to an alternate data center. This ensures that redundant copies are available in the event of a disaster. SCE tests its complete disaster recovery plan at least once per year to ensure systems run correctly at the redundant site and that staff is properly trained to handle potential disasters.
- **Security Skills Assessment and** Each employee, at the time of hiring and every following year, is required to complete security and awareness training.

Contact Information

If you have any questions, feel free to reach out to us at the contact information below:
The SCE, Inc.
500 Linwood Drive, Suite 1J
Fort Lee, New Jersey 07052