SolarWinds Security Statement

This Security Statement is aimed at providing you with more information about our security infrastructure and practices. Our privacy policy contains more information on how we handle data that we collect.

Information Security Policy

SolarWinds maintains a written Information Security policy that defines employee's responsibilities and acceptable use of information system resources. The organization receives signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior, before providing authorized access to SolarWinds information systems. This policy is periodically reviewed and updated as necessary.

Our security policies cover a wide array of security related topics ranging from general standards with which every employee must comply, such as account, data, and physical security, to more specialized security standards covering internal applications and information systems.

Organizational Security

Information security roles and responsibilities are defined within the organization. The security team focuses on information security, global security auditing and compliance, as well as defining the security controls for protection of SolarWinds' hardware infrastructure.
The security team receives information system security notifications on a regular basis and distributes security alert and advisory information to the organization on a routine basis after assessing the risk and impact as appropriate.

SolarWinds follows the NIST Cybersecurity Framework with layered security controls to help identify, prevent, detect, and respond to security incidents. The information security manager is also responsible for tracking incidents, vulnerability assessments, threat mitigation, and risk management.

Asset Management

SolarWinds' data and information system assets are comprised of customer and end-user assets as well as corporate assets. These asset types are managed under our security policies and procedures. SolarWinds authorized personnel who handle these assets are required to comply with the procedures and guidelines defined by SolarWinds security policies.

Personnel Security

SolarWinds employees are required to conduct themselves in a manner consistent with the company's guidelines, including those regarding confidentiality, business ethics, appropriate usage, and professional standards. All newly hired employees are required to sign confidentiality agreements and to acknowledge the SolarWinds code of conduct policy. The code outlines the company's expectation that every employee will conduct business lawfully, ethically, with integrity, and with respect for each other and the company's users, partners, and competitors. Processes and procedures are in place to address employees who are on-boarded and off-boarded from the company.

Employees are provided with security training as part of new hire orientation. In addition, each SolarWinds employee is required to read, understand, and take a training course on the company's code of conduct.

Physical and Environmental Security

SolarWinds has policies, procedures, and infrastructure to handle both physical security of its data centers as well as the environment from which the data centers operate.

Our information systems and infrastructure are hosted in world-class data centers that are geographically dispersed to provide high availability and redundancy to SolarWinds and its customers. The standard physical security controls implemented at each data center include electronic card access control systems, fire alarm and suppression systems, interior and exterior cameras, and security guards. Physical access is centrally managed and strictly controlled by data center personnel. All visitors and contractors are required to present identification, are required to log in, and be escorted by authorized staff through the data center.

Access to areas where systems, or system components, are installed or stored are segregated from general office and public areas. The cameras and alarms for each of these areas are centrally monitored 24x7 for suspicious activity, and the facilities are routinely patrolled by security guards. Servers have redundant internal and external power supplies. Data centers have backup power supplies, and can draw power from diesel generators and backup batteries. These data centers have completed a Service Organization Controls (SOC) 2 Type II audit and are SSAE16 accredited.

Operational Security

Change Management

SolarWinds maintains a change management process to ensure that all changes made to the production environment are applied in a deliberate manner. Changes to information systems, network devices, and other system components, and physical and environment changes are monitored and controlled through a formal change control process. Changes are reviewed, approved, tested and monitored post-implementation to ensure that the expected changes are operating as intended.

Supplier and Vendor Relationships

SolarWinds likes to partner with suppliers and vendors that operate with the same or similar values around lawfulness, ethics, and integrity that SolarWinds does. As part of its review process, we screen our suppliers and vendors and bind them to appropriate confidentiality and security obligations, especially if they manage customer data.

SolarWinds does not give our suppliers or vendors direct access to network/equipment management responsibility. Our procurement department may perform audits from time to time on SolarWinds suppliers and vendors in an effort to ensure the confidentiality, integrity, and availability of data that our third party suppliers or vendors may handle.

Auditing and Logging

We maintain audit logs on systems. These logs provide an account of which personnel have accessed which systems. Access to our auditing and logging tool is controlled by limiting access to authorized individuals. Security events are logged, monitored, and addressed by trained security team members. Network components, workstations, applications and any monitoring tools are enabled to monitor user activity. Organizational responsibilities for responding to events are defined. Security events that record critical system configuration changes and administrators are alerted at the time of change. Retention schedules for the various logs are defined in our security control guidelines.

Antivirus and Malware Protection

Antivirus and malicious code protection is centrally managed and configured to retrieve the updated signatures and definitions available. Malicious code protection policies automatically apply updates to these protection mechanisms. Anti-virus tools are configured to run scans, virus detection, real-time file write activity and signature file updates. Laptop and remote users are covered under virus protection. Procedures to detect and remove unauthorized or unsupported (e.g. freeware) applications are documented.

System Backups

SolarWinds has backup standards and guidelines and associated procedures for performing backup and restoration of data in a scheduled and timely manner. Controls are established to help safeguard backed up data (onsite and off-site). We also work to ensure that customer data is securely transferred or transported to and from backup locations. Periodic tests are conducted to test whether data can be safely recovered from backup devices.

Network Security

Our infrastructure servers reside behind high-availability firewalls and are monitored for the detection and prevention of various network security threats. Firewalls are utilized to help restrict access to systems from external networks and between systems internally. By default, all access is denied and only explicitly allowed ports and

SolarWinds maintains separate development and production environments. Our next generation firewalls (NGFWs) provide adequate network segmentation through the establishment of security zones that control the flow of network traffic. These traffic flows are defined by strict firewall security policies.

Automated tools are deployed within the network to support near-real-time analysis of events to support of detection of system-level attacks. Next generation firewalls deployed within the data center as well as remote office sites monitor outbound communications for unusual or unauthorized activities, which may be an indicator of the presence of malware (e.g., malicious code, spyware, adware).

Data Protection

SolarWinds continually works to develop products that support the latest recommended secure cipher suites and protocols to encrypt traffic while in transit. We monitor the changing cryptographic landscape closely and work to upgrade our products to respond to new cryptographic weaknesses as they are discovered and implement best practices as they evolve. For encryption in transit, we do this while also balancing the need for compatibility for older clients.

Vulnerability Management

Security assessments are done to identify vulnerabilities and to determine the effectiveness of the patch management program. Each vulnerability is reviewed to determine if it is applicable, ranked based on risk, and assigned to the appropriate team for remediation.

Patch Management

SolarWinds strives to apply the latest security patches and updates to operating systems, applications, and network infrastructure to mitigate exposure to vulnerabilities. Patch management processes are in place to implement security patch updates as they are released by vendors. Patches are tested prior to being deployed into production.

Secure Network Connections

HTTPS encryption is configured for customer web application access. This helps to ensure that user data in transit is safe, secure, and available only to intended recipients. The level of encryption is negotiated to either SSL or TLS encryption and is dependent on what the web browser can support.

Access Controls

Role Based Access

Role based access controls are implemented for access to information systems. Processes and procedures are in place to address employees who are voluntarily or involuntarily terminated. Access controls to sensitive data in our databases, systems, and environments are set on a need-to-know / least privilege necessary basis. Access control lists define the behavior of any user within our information systems, and security policies limit them to authorized behaviors.

Authentication and Authorization

We require that authorized users be provisioned with unique account IDs. Our password policy covers all applicable information systems, applications, and databases. Our password best practices enforce the use of complex passwords that include both alpha and numeric characters, which are deployed to protect against unauthorized use of passwords. Passwords are individually salted and hashed.

SolarWinds employees are granted a limited set of default permissions to access company resources, such as their email, and the corporate intranet. Employees are granted access to certain additional resources based on their specific job function. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as defined by our security guidelines. Approvals are managed by workflow tools that maintain audit records of changes.

Software Development Lifecycle

We follow a defined methodology for developing secure software that is designed to increase the resiliency and trustworthiness of our products. Our products are deployed on an iterative, rapid release development lifecycle. Security and security testing are implemented throughout the entire software development methodology. Quality Assurance is involved at each phase of the lifecycle and security best practices are a mandated aspect of all development activities.

Our secure development lifecycle follows standard security practices including vulnerability testing, regression testing, penetration testing, and product security assessments. The SolarWinds architecture teams review our development methodology regularly to incorporate evolving security awareness, industry practices and to measure its effectiveness.

Incident Management

SolarWinds has a formalized incident response plan (Incident Response Plan) and associated procedures in case of an information security incident. The Incident Response Plan defines the responsibilities of key personnel and identifies processes and procedures for notification. Incident response personnel are trained, and execution of the incident response plan is tested periodically.

An incident response team is responsible for providing an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.

Business Continuity and Disaster Recovery

To minimize service interruption due to hardware failure, natural disaster, or other catastrophe, we implement a disaster recovery program at all our data center locations. This program includes multiple components to minimize the risk of any single point of failure. Application data is replicated to multiple systems within the data center and, in some cases, replicated to secondary or backup data centers that are geographically dispersed to provide adequate redundancy and high availability. High-speed connections between our data centers help to support swift failover.

Data Protection

We apply a common set of personal data management principles to customer data that we may process, handle, and store. We protect personal data using appropriate physical, technical, and organizational security measures.

We give additional attention and care to sensitive personal data and respect local laws and customs, where applicable.

SolarWinds only processes personal information in a way that is compatible with and relevant for the purpose for which it was collected or authorized in accordance with our privacy policy. We take all reasonable steps to protect information we receive from our users from loss, misuse or unauthorized access, disclosure, alteration and/or destruction.