Nimsoft ITMaaS

Security and Operations Policy Reference

The Nimsoft service team has implemented processes and controls in its Nimsoft IT Management-as-a-Service offerings that help protect customer infrastructure, prevent disclosure of customer data to third parties and guard against malicious access and exploits.

Nimsoft understands that an effective security strategy is a key factor in a customer's decision to utilize Nimsoft ITMaaS. For this reason, Nimsoft has implemented a set of procedures designed to protect the security and confidentiality of a customer's monitoring data and any identifiable customer information. To ensure its safeguards keep pace with evolving threats and technologies, Nimsoft continually fine tunes and enhances its policies, processes, tools and controls.

What does Nimsoft do to protect the data of customers using Nimsoft ITMaaS? Following is an overview of some the controls and policies in place.

Security Procedures

Nimsoft's security policy and procedures include:

- **Information security governance**. This includes maintaining security awareness, enforcing segregation of duties and conducting employee background checks. In addition, we'll continue to normalize and implement policies and procedures, update controls to mitigate risks, and assess internal controls to verify compliance.
- **Logical access**. This entails managing user access requests, password complexity guidelines, user access monitoring and account termination.
- **Physical access**. This includes enforcing policies for data center visits.
- **Network security**. This refers to such activities as firewall administration, intrusion detection/prevention, vulnerability and penetration testing, anti-virus implementation, security incident monitoring and escalation, patching and encryption.

Firewalls and Intrusion Detection

Nimsoft data centers utilize application switches to provide firewall capabilities. These application switches support stateful firewall access control lists, block malicious attacks, protect against protocol attacks and denial-of-service (DoS) attacks and encrypt mission-critical content. Application switches also perform protocol compliance inspection, filtering and fix-up for data center protocols such as DNS and FTP.

The data center's IDS (intrusion detection system) solution utilizes a rules-based language, which combines the benefits of signature-, protocol- and anomaly-based inspection methods. Rules are used to examine packets at both the IP protocol level and at the application level and can be set to look for specific occurrences of attacks against a protocol or for the conditions associated with an attack.

Anti-virus

Nimsoft ITMaaS data centers utilize anti-virus on all production systems.

Physical Security

Before a visit to any data center is permitted, a customer has to initiate a ticket in advance in order to inform data center staff. Visitors are required to present valid, government-issued identification prior to sign in, and are provided badges and escorted by a security officer until they exit the facility. Entry to all areas and access points are controlled by biometric hand scanners and monitored and recorded using CCTV. Each facility is staffed around-the-clock by security officers.

Security

Nimsoft adheres to strict standards and guidelines for information security. The company's policies form a framework for all information security procedures and controls, helping ensure that Nimsoft internal business and compliance requirements are consistently met.

Nimsoft leverages corporate compliance, security and support groups within CA Technologies—such as Global Information Services (GIS), Internal Audit, Global Security, Support and Legal—for developing and refining its policies, standards, guidelines and procedures.

Security Risk Assessments

The Nimsoft internal security and compliance team performs risk assessments on infrastructure and applications. Nimsoft also works with a third-party provider to execute vulnerability and penetration testing on a periodic basis. The controls in place are designed to mitigate risks uncovered by the risk assessment process.

Roles and Responsibilities

Nimsoft has implemented a segregation of duties matrix in order to prevent the possibility of one individual being able to initiate, approve or make changes to the production environment.

The Nimsoft Internal Support Organization

The Nimsoft internal support organization coordinates with its corporate parent, CA Technologies, and specifically the Global Information Security and SaaS Infrastructure Security groups, to design and implement security architectures, policies and procedures. Nimsoft intends to continue to utilize corporate security policies and procedures of CA Technologies to assist in the implementation of security risk assessments and controls.

Security Incidents

Nimsoft has established a security incident response team ("SIRT") as its authority in developing plans for responding to serious IT security incidents. The SIRT receives reports of IT security incidents and then follows established protocols in determining appropriate actions and responses. Based on the nature and severity of the incident, a determination is made whether to assign incidents to a given operational team or to security specialists within the SIRT.

In some cases, the SIRT may escalate the incident to law enforcement and/or executive management. Individual incident response plans and notification procedures may also be developed with specific customers. Any customer-specific escalation matrices are kept in each customer's wiki space, and are accessible by the customer.

Backups

Nimsoft ITMaaS offers offsite backup protection, leveraging a second site that is owned and operated by the provider of the primary site. Compliance processes are in place to ensure a successful backup.

Retention of Data

Backups are maintained for a rolling 28 days.

Backup Objective

Nimsoft's objective is to backup the customer's data on a daily basis.

Facility Locations

In the USA, Nimsoft's third-party data center provider has two separate locations in different states.

Computing Environment

Nimsoft provides its customers with a production instance running in physical and virtualized environments that provide a high level of availability, reliability and recoverability. Standard lifecycle management, such as hardware maintenance and end of life replacement, is performed on an appropriate schedule.

Data Management

Customer instances and data are isolated in the data center in order to ensure that changes in one customer's environment don't have an adverse affect on another customer's. The data center is designed to enable infrastructure resources to be flexed as needed to meet demand. In the decommissioning phase, disks are formatted to remove data from the previous deployment. The data center utilizes secure erase technologies and procedures that overwrite disks multiple times before they are reused for additional customers.

Third-party Suppliers

Nimsoft has contracted with a third-party supplier to deliver services through a SaaS model. Nimsoft holds third-party vendors to very stringent performance, response and compliance standards. Details regarding these data centers' physical structure and security measures are available upon request.

Service Level Agreement

The Nimsoft customer agreement addresses the nature and extent of Nimsoft's service level agreement.

Staff Vetting and Management

Background Checks

Nimsoft and its third-party data center provider perform background checks on full-time and part-time employees at the time of an employment offer. These checks cover the areas of credit, criminal record and general background information, including former address, alias and education.

Background screening includes, at a minimum:

- Two full reference verifications
- A five year county criminal check
- Social security number verification

Security Training

Education is a key part of a solid protection framework. Consequently, all employees working on customer data are required to take additional security training based on ITIL V3, as well as the standard Nimsoft training curriculum.

Additionally, the signing of confidentiality and non-disclosure agreements are conditions of employment at Nimsoft and Nimsoft's third party.

About Nimsoft

Nimsoft provides leading IT Management-as-a-Service solutions within the CA Technologies portfolio. Companies and service providers of all sizes use Nimsoft to rapidly and easily implement essential monitoring and service desk capabilities necessary to manage today's dynamic computing environments. Learn more at www.nimsoft.com.

North America Headquarters

U.S. toll free:
1 877 SLA MGMT (752 6468) 1 408 796 3400

Email: info@nimsoft.com
Web: www.nimsoft.com

EMEA Email:
NimsoftEMEA@ca.com

United Kingdom
+44 (0) 845 456 7091

Norway & Northern Europe
+47 22 62 71 60

France
+33 149 025 226

Germany
+49 (0)89-99 61 90 60

Italy
+39 02 904 641

Austria
+43 664 8 59 74 39

Switzerland
+41 (44) 804-78 23

Spain and Portugal
+34 93 492 7511

Australia
+61 (0)2 8898 2943

Brazil
+5511 5503 6243

Mexico City
+52 (55) 5387 5406

Singapore
+65 64328600