Security Whitepaper

NetTec NSI provides a leading SaaS-based managed services platform that to efficiently backup, monitor, and troubleshoot desktops, servers and other endpoints for businesses. Our comprehensive platform provides an intelligent remote monitoring and management (RMM) solution and an advanced backup and disaster recovery (BDR) offering - all integrated with an industry-leading Network Operations Center (NOC) and U.S.- based world-class Help Desk, delivering a single, unified managed services experience.

Clients trust NetTec NSI with remote monitoring and management of their most critical systems. NetTec NSI employees are responsible for managing and analyzing various types of systems and associated logs which process or store sensitive information that must be protected at all times. To ensure this, NetTec NSI has implemented security policies, procedures, and controls for our Network Operations Center (NOC) and Help Desk personnel, which are outlined in the following sections.

NetTec NSI Philosophy

NetTec NSI strives to provide clients with the highest level of security and protection where critical systems and sensitive information are concerned. Because you entrust NetTec NSI with this information and access, we have developed and implemented various layers of security policies, protocols, and controls to be sure sensitive and protected information is secure at all times. These policies, protocols and controls comprise the company's Information Security Management Systems (ISMS) that govern the Help Desk and NOC.

Best Practices

NetTec NSI provides our clients with HIPPA and Massachusetts Privacy Regulation 201 CMR 17.00-compliant products and services. Our commitment to continually improving security is demonstrated by our adherence to the ISO/IEC 27000 series of security standards framework. This allows NetTec NSI to provide evolving industry best practices and standardization of protocols in the realm of information security.

NetTec NSI was found compliant by an independent third-party auditing firm for security posture and controls against the requirements defined in both HIPPA and Massachusetts Privacy Regulation 201 CMR 17.00. To maintain compliance and continually improve the security program, NetTec NSI adopted the ISO 27000 framework.

Employee Security Measures

Background Verification and Standards

Background checks are performed on all NetTec NSI employees, including Help Desk and NOC. In the United States, criminal records search and SSN verifications are done. In India, a criminal records search and verification checks for education and employment are done. All employees are required to sign a Non-Disclosure Agreement as a condition of employment.

Roles and Responsibilities

Every team member has a job description with detailed roles and responsibilities, associated with Standard Operating Procedures (SOPs) that are used daily. SOPs are in place to define how each employee must perform their day-to-day work. These procedures are reviewed and updated on a regular basis to take advantage of improvements to our systems and maximize both security and efficiency. This practice restricts exposure to sensitive information and provides guidelines internally to employees coming into contact with sensitive information.

Information Security Training Program

Security awareness is a top priority with regards to NetTec NSI employees. To this end, a rigorous training program has been created and is actively managed by our Chief Information Security Officer. All employees, regardless of position, are required to complete the program and successfully pass all related tests. The comprehensive program includes topics such as Information Security, Anti-Virus Policy, Data Security, Information Sensitivity, Password Policy, and Destruction of Electronic Media. Each module of the program contains both a training document and exam. Refresher courses are required on an annual basis. Records are verified and maintained for course completion and annual refreshers are completed by each employee.

Company Security Measures

Data Center Credentials

For information security, we have applied industry-leading practices and processes. Only a select few individuals have administrative access to our servers and databases. All other access is at the application level. Information sent to our databases is first processed by a forwarding server, and then imported into the database. Our databases are not directly accessible from the Internet.

NetTec NSI’s RMM infrastructure is hosted in Markely Group’s Data Center, a SSAE-16 certified facility. This data center is a fully redundant facility. A copy of the SSAE-16 report is available upon request.

Secure Remote Connection Feature

Access to our managed systems is performed by using LogMeIn (LMI). LMI remote access products use a proprietary remote desktop protocol that is transmitted via Secure Socket Layer (SSL). An SSL certificate is created for each remote desktop and is used to cryptographically secure communications between the remote desktop and the accessing computer. Additional LMI security information can be found here https://secure.logmein.com/products/pro/security.aspx.

NetTec NSI embeds LMI into the NOC Portal used by the Help Desk, providing additional auditing capabilities, as each technician has their own credentials for the portal, and all entries are time-stamped.

System Updates

All NOC and Help Desk systems are updated regularly with Microsoft Patches, third party software and definitions for Antivirus and Anti-malware Solutions. Our agents ensure that antivirus software is properly installed and verify, and that the latest antivirus definition files have been updated and applied. The RMM agents also monitor to ensure Malwarebytes is installed and current on all end user devices. If Malwarebytes definitions have not been updated in the past 7 days, an alert will be raised.

NetTec NSI's Preventative Maintenance Team tests all security patches. Once tested, Microsoft security patches are classified as Whitelisted (passed), Blacklisted (failed and not recommended for installation) Conditional Blacklisted (failed under certain conditions and not recommended for installation) and In Progress (undergoing testing). A Patch Evaluation Report provides Partners with the classification.

Security Audit Program

As stated previously, NetTec NSI was found Compliant by an independent, 3rd party auditing firm, for security posture and controls against the requirements defined in both HIPAA and Massachusetts Privacy Regulation 201 CMR 17.00. In order to maintain compliance, and to continually improve upon the security program in place, NetTec NSI has adopted the ISO 27000 framework. NetTec NSI will also schedule additional 3rd party audits annually to remain in compliance going forward.

Access Control

NetTec NSI provides all employees, contractors, and third parties with the information they need to carry out their responsibilities effectively and efficiently. Access is granted through IT account request procedures, based on the principle of least privilege, and approved by NetTec NSI management before granting access. When an employee separates from NetTec NSI, Human Resources notifies IT to remove access at the end of the employee's last day.

In addition to controlling access to sensitive information, NetTec NSI has a strict Password Management Policy that is applied and enforced for all NetTec NSI users.

This policy is in force for Active Directory domains, hosted applications, internal and customer facing portals. Users are required to have a minimum password length which includes complexity and expires every 90 days.

Product Security Measures

Our various product offerings each house their own set of security features and measures that provide customers with confidence where information security is concerned.

ITSupport Portal

NetTec NSI uses state-of-the-art firewalls and only allows incoming traffic on ports 80 and 443. Our firewalls are multi-threat security systems which enable secure communications and deliver the best security and performance.

Our RMM platform operates entirely over secured connections. Our agents send only asset data and performance information to our data center. All agent information is sent either over https or encrypted using AES 128 bit encryption.

Agents communicate with the data center by using a local system account. The server agents send a keep-alive request to the data center every one minute over port 80.

All data sent from the agents to the data center is compressed at the client side using a compression key, encrypted and then sent over a secure 128-bit encrypted tunnel.

- **LogMeIn** - NetTec NSI currently uses LogMeIn and LogMeIn Rescue to remotely access servers and workstations. LogMeIn products are architected with security being the most important design objective. Data centers and source code are continually reviewed by independent, accredited third party audit firms to ensure data, verifying that information remains confidential.
- **Remote Management Console** - The remote management console allows only authorized NetTec NSI employees to connect securely and take remote control over client machines in the event that LogMeIn is unavailable. This connection is established using a Secure Shell 2 (ssh2) tunnel over port 443. The RDP protocol is used through this tunnel for remote access to end points. The support engineer’s machine initiates the connection and generates the encryption key. The connection is routed through our data center, which acts as a pass-through tunnel, and the connection is then made to the end point.
- **Password Vault (Secure Information Store)** - The Secure Information Store is a web-based password vault designed to help our engineers securely store and manage sensitive information. The Secure Information Store allows for the secure transfer of server credentials to the NOC and desktop credentials to the Help Desk. Additionally, the Secure Information Store provides secure storage of critical client information for access by onsite technicians, secure storage of Lights Out Management credentials for

remotely re-starting downed servers and secure storage of Vault encryption passphrases, for decrypting and troubleshooting Vault backups.

The Secure Information Store password vault resides in house, on our servers. Data stored within the Secured Information Store is delivered securely by HTTPS or by 256-bit AES encryption at both the database and column level, the same technology used in banks, credit card processors, hospitals and government agencies.

The Secured Information Store allows secure transfer of credentials to NOC and Help Desk technicians and provides a secure central location for technicians to access vital information on their your networks. When a technician accesses these credentials, information such as user name, date/time, system IP address, and any additional information provided by the technician is captured and logged for accountability.

NetTec NSI Cloud Console (C3)

C3 is a management console available from the ITSupport Portal that allows you to manage Amazon Web Services' (AWS) Infrastructure as a Service (IaaS). AWS provides security up to the hypervisor, meaning that they will address security controls such as physical security, environmental security, and virtualization security.

Security Groups are used to act as a virtual firewall for your instance, to control inbound and outbound traffic. Security Groups act at the instance level, not the subnet level. The default security group is:

Inbound:

1. Deny all TCP & UDP from any
2. Permit TCP 22, 80, 443, 3389 (ssh, http, https, rdp) from any

Outbound:

1. Permit all TCP & UDP to any
2. ICMP – disabled

All actions performed on VMs in the C3 environment are captured in an Activity Log. This log records a list of C3 VM actions and tracks them by user, date and time the action was performed and the VM instance the action was performed on.

Payment transactions in C3:

NetTec NSI has partnered with a top, PCI-compliant payment processing company to handle the ACH and credit card transactions for our services. NetTec NSI does not store or handle your credit card or ACH information directly.

For more information about the Architecture and Security in C3, visit the Partner Support Portal.

Sync247

Unlike typical virtualized cloud environments, where applications share processing and storage platforms, Sync247 operates on its own dedicated hardware. Nothing runs on the Sync247 platform except the Sync247 service.

Sync247 hardware is hosted in two independent data centers in the United States, physically distanced and isolated from each other, thus providing protection from higher level data center failures. Within each data center, redundant servers and file storage ensure that data center level failures can be isolated and resolved quickly.

The Sync247 associated data centers are certified against SAS 70 / SSAE 16 requirements for attestation and auditing.

Sync247 implements a variety of security strategies to continuously guard against, monitor and assess potential security risks. Mechanisms to ensure Access Security, Monitoring and Risk Assessment are further described below.

Access Security:

- All Sync247 application servers are protected with OS security modules that apply Discretionary Access Control and Mandatory Access Control policies to all server processes, thus ensuring that no software process can be gainfully subverted.
- All connection pathways are highly regulated as to the kinds of traffic that are allowed between various internal server endpoints. Any network traffic that does not meet the expected data flow patterns is immediately interrupted and reported to monitoring personnel through alerts.
- All known attack vectors are specifically prohibited.

Monitoring and Risk Assessment:

- Each Sync247 Data Center is monitored 24 hours per day, 365 days per year, by equipment service and operations staff who have immediate access to Sync247 engineering personnel in the event of an emergency.
- Dedicated software monitoring components are designed to track and evaluate the operation of servers, networking equipment, applications, and services within the Sync247 service infrastructure. This also includes monitoring of resources such as processor load, memory usage, and disk space usage.
- Alerts regarding performance or potential security issues are automatically distributed to several on-call staff members via SMS and email.
- Sync247 makes use of independent third-party penetration testing of Web, Agent, APIs and periodic SAS/SSAE audits.

Sync247 security policy settings have been established that adhere to HIPAA technical safeguards, as defined by 45 CFR 164.312. These security policy settings are based on industry leading practices and may satisfy the requirements of many businesses. If the

security policy settings detailed below are not sufficiently stringent to meet a client's unique needs, the client should not use Sync247.

You are solely responsible for ensuring that Sync247 meets your client's technical safeguard requirements for HIPAA compliance.

- **Passwords:** User passwords must not be the same as the username and must contain at least one number, one lower-case letter and one upper-case letter.
- **Session Timeout:** The Sync web interface, https://sync.itsupport247.net, is configured to induce a session timeout after 120 minutes of inactivity.
- **Log-in Page, no "Remember me" option:** Users are not provided with a *Remember Me* option on the web interface login page.
- **Mobile App Passcode:** The mobile apps have a passcode option that is user-configurable.

Public links for external sharing. By default, the Sync service allows user to create public links that allow external access to data stored in the Sync service. Admins may use the Public Links Policy to prevent users from creating public links.

Help Desk

RightAnswers is a cloud-based knowledge management system our Help Desk uses for issue tracking and troubleshooting. RightAnswers utilizes an SSL-encryption connection between a technician's browser and RightAnswers servers. User authentication is performed on NetTec NSI's servers. The username and group is then encrypted and passed to RightAnswers' servers. The encryption is accomplished through the use of GET requests with digested tokens. The digested tokens is passed from the application performing the authentication, to the RightAnswers portal, and is used to validate a single sign-on session request so that it will not be usurped by anyone. It is intended to validate that the intended authenticated user is the one generating the request. This validation is accomplished by passing an HTTP query string parameter value containing the digesting token. To avoid a man-in-the-middle or replay type of attack, the token is generated with a varying timestamp value added to it to make the final digested value unique for each use, and to produce a request that has a very limited lifespan.

Network Operations Center (NOC) Protocols

NOC Access Levels 0-4 are selected by you to designate how you would like proactive troubleshooting to be performed for your servers. For example, you might want the NOC Technician to login to the server, diagnose the problem but avoid fixing anything until they receive permission from you (Access Level 1).

Help Desk Protocols

As with the NOC, approval is a prerequisite for initial access to a client system directly contacting the Help Desk to perform specific tasks.

When calling in, the phone numbers are integrated into both CaPPS, our contact management application, and the Help Desk portal allowing the Help Desk to see the incoming phone number as well as the name (be it site or user) associated with the number.

Help Desk personnel are not authorized to change site-level administrator passwords or credentials filed in password vault. User passwords at contracted sites can only be changed with the authorization of the client administrator, unless personnel authorized approve security-related requests (such as password resets) are pre-documented by the client on the Portal. Calls will be made to the appropriate parties using phone numbers documented by the client when requesting authorization for security-related changes. If the user is not reached, a voicemail will be left and email sent.

Two-Factor authentication is available upon request of the client for client sites. For such sites a text message will be sent to the security-related change requestor. The client is responsible for supplying mobile numbers of personnel at the site prior to activating the two-factor option. When no mobile number is available the ticket will be escalated to an engineer for completion per our normal procedures.

Conclusion

NetTec NSI strives to provide clients with the highest level of security and protection of critical systems and sensitive information. We have implemented security policies, procedures and controls for our hardware and software, Network Operations Center (NOC), Help Desk personnel and for all Employees. Please contact your Account Management team if you have any questions.