Last updated: 02.04.2024

These security measures (" **Security Measures** ") are part of the agreement signed between NTICO and the Client which refers to this document. NTICO's performance of the Services must be in accordance with the Agreement and these Security Measures. Terms used herein, but not defined herein, are defined in the Agreement.

NTICO reserves the right to periodically change these Security Measures to reflect current security practices, and such change will automatically become effective.

NTICO will use commercially reasonable efforts to prevent the loss, theft, or damage of Customer Data from the Services. The Security Measures establish the requirements necessary to maintain a security program and ensure that sufficient physical, operational, and technical security measures are in place for the protection of Customer Data in the Services. These Security Measures apply when NTICO provides the Services and Support to the Customer.

1. Information Security Management

1.1 Information Security Management System. NTICO maintains and continually improves a documented information security management system in accordance with industry standard practices and accepted frameworks for the provision of OpCon services and support, of which its personnel must be informed and comply ("Information Security Management System").

1.2 Certification. During the term of the agreement, NTICO must maintain its AICPA SOC2 or equivalent report, as well as a legal transfer mechanism for the export of personal data out of the European Union.

1.3 Tests. NTICO conducts at least once a year third-party security testing on applications and infrastructure used to support the provision of services and support to identify security vulnerabilities.

2. Organizational Security

2.1 Information Security Responsibilities. NTICO has dedicated roles with clearly defined responsibilities for the administration of the information security management system.

2.2 Security policies. As part of the administration of the information security management system, NTICO has created information security policies that define the responsibility for the protection of its systems and customer data ("Information Security Policies"). Information security policies include requirements designed to monitor compliance with privacy and information security policies and procedures.

3. Asset classification

3.1 Asset management. NTICO maintains an asset management policy that is consistent with industry standard practices, including the classification of assets (*e.g.* , information, software, hardware) and an inventory of devices and systems that administer services and support to enable NTICO to protect customer data and assets.

3.2 Asset controls. NTICO has physical, organizational, and technical security controls in place to protect customer data from unauthorized access and disclosure.

4. Personal Safety

4.1 NTICO employees. NTICO employees must behave consistently with these Security Measures to ensure effective security. NTICO educates its employees on their responsibilities in maintaining effective security controls, particularly with respect to the use of passwords, information disposal, social engineering attacks, incident reporting, and the physical and technical security of users and company equipment through security awareness/onboarding training. NTICO publishes documented security policies, updates them as necessary, and provides monthly security training.

4.2 Background check. NTICO ensures that its employees involved in the provision of the Services and Support have successfully passed basic background checks designed to validate the completeness and accuracy of resumes, confirmation of professional qualifications, and identity verification where permitted by law.

5. Physical and environmental security

5.1 Physical access. When NTICO has a physical office, it ensures that only authorized users have physical access to the network, critical systems and applications, server rooms, communication rooms, and work environments. NTICO maintains controls to monitor unauthorized access attempts. Additional controls are maintained to prevent or detect the removal of such equipment.

5.2 Data Transfer. NTICO does not allow the transfer of customer data to external or removable storage media.

6. Communications and Operations Management

6.1 Vulnerability/patch management. NTICO has implemented a vulnerability/patch management process that ensures that all systems used to provide the Services and Support, including network devices, servers, and desktops/laptops, are patched against known security vulnerabilities within a reasonable time based on the criticality of the patch and the sensitivity of the Customer Data accessed through the systems.

6.2 Secure system configuration. NTICO has controls in place to ensure that all systems used to provide services and support are configured securely and repeatably. This involves changes to default settings to improve system security (*e.g.,* "hardening" the system), changes to default account passwords, and removal of software or useless services. In addition, employee devices used to interact with or manage the systems that provide Services and Support must also be configured in a repeatable manner. Specific additional requirements beyond what also exists in these Security Measures include:

6.2.1 Full/full disk encryption; and

6.2.2 Remote wipe and lock data in case the device is lost or stolen

6.3 Malware prevention. NTICO has implemented detection and prevention controls to protect against malware and appropriate user awareness procedures. NTICO maintains and updates technical controls and regularly assesses all systems for the existence of malware. NTICO performs real-time or regular scans of NTICO-owned devices for viruses, malware, and possible security incidents.

6.4 Logging and auditing. NTICO has implemented a comprehensive log management program that defines the scope, production, transmission, storage, analysis, and disposal of logs based on current industry practices. Systems and services provide logging capabilities in accordance with the following principles:

6.4.1 The scope of logging and retention policy is based on a risk-based approach, with a minimum retention of six (6) months;

6.4.2 Logs are collected to enable forensic analysis of information security incidents.

6.4.3 logs, record administrative changes to the Services;

6.4.4 the records are kept practically securely to prevent tampering;

6.4.5 Passwords and other sensitive data elements are not saved in any way;

6.4.6 Perform regular log analysis to assess security.

6.4.7 Configure all affected systems to provide real-time logging of any event that may indicate a system compromise, denial of service event, or other security breach, including notifying an administrator when predetermined event thresholds are exceeded. and

6.4.8 The logs are protected from unauthorized access or modification.

7. Disaster Recovery and Business Continuity Planning

7.1 Programs. NTICO has disaster recovery and business continuity programs in place and ensures that these plans ensure the confidentiality and integrity of customer data during recovery operations. NTICO ensures that programs do not allow for any reduction in security.

7.2 Backups. It is the customer's responsibility to back up their database(s) on a regular basis.

8. Security Incidents

8.1 Incident detection. NTICO has established and maintains a clearly documented operational incident detection capability and incident response program to respond to suspected or known security incidents or system breaches. Incident response plans include methods to protect evidence of activity from alteration or alteration, and to enable the establishment of a chain of custody of evidence.

8.2 Incident response. In the event of an incident affecting customer data, NTICO uses industry-standard efforts to respond to incidents and mitigate risk to the customer and customer data.

8.3 Incident notification. In the event of a confirmed incident that affects the Customer's data, NTICO will notify the Customer of the security incident within 48 (forty-eight) business hours of the confirmation.

9. Access Control

9.1 Authentication. NTICO supports single sign-on (SSO) mechanisms for the customer to interact with Solution Manager (*for example,* Okta).

9.2 Access to support. If NTICO allows its employees to access customer data through an application support interface, that interface, at a minimum, must (a) uniquely identify the NTICO employee who used it.

9.3 User passwords. NTICO provides employees with reasonably designed training to ensure that employees have sufficient complexity and expiration requirements or need an additional layer of security with multi-factor authentication.

9.3.1 Authentication and two-factor authentication. The term "two-factor authentication" refers to authentication by combining something that a person knows, such as a username and password, in combination with something that possesses, such as a disconnected authentication token, or a biometric factor, such as a fingerprint. NTICO uses multiple authentication factors when available, and NTICO uses at least one two-factor authentication to access accounts used to provide data hosting services. Any administrative access by NTICO employees must require two-factor authentication. If NTICO uses Google Apps to manage its accounts, two-factor verification must be enabled.

9.3.2 Inactivity. All NTICO-owned devices automatically lock after a reasonable period of inactivity.

9.3.3 Departure of an employee or consultant. Upon the departure of a third-party employee, contractor, or consultant, the individual's access to the networks, systems, and accounts used to provide the Services and Support, as well as access to all Customer Data, is terminated.

9.3.4 Authorization. Customer is solely responsible for controlling and providing access to Customer Data.

9.6.5 Network Access Controls. All networks used by NTICO to provide the Services and Support are protected by the use of controls capable of blocking unauthorized network traffic, both incoming (incoming) and outgoing (outgoing).

10. Data Security

10.3 Encryption.

10.3.1 Data in transit. NTICO ensures that HTTPS is enabled in any web interface related to the product or service. NTICO allows the customer to use TLS 1.2 or higher for web applications.

10.3.2 Data at rest. Customer data at rest for on-premises OpCon customers is the responsibility of the customer. For OpCon Cloud customers, it is encrypted at all times using industry-accepted cryptography standards. This includes, at a minimum:

10.3.2.1 Use of the Advanced Encryption Standard (AES) defined in FIPS 197.

10.3.2.2 When different algorithms are used, they have comparable strengths (*for example,* if an AES-256 key is to be encrypted, an AES-256 or higher, or RSA-3072 or higher key can be used to encrypt it).