NTT DATA BUSINESS SOLUTIONS INC. INFORMATION SECURITY

NTT DATA Business Solutions Inc. (NTT DATA) Security Programs are designed to protect both NTT DATA and customer data in areas such as:

- The systems that customers rely upon for cloud services, technical support and other services;
- NTT DATA source code and other sensitive data against theft and malicious alteration; and
- Personal and other sensitive information that NTT DATA collects in the course of its business, including customer, partner, supplier and employee data residing in NTT DATA's internal IT systems

NTT DATA's information security policies cover the management of security for both NTT DATA's internal operations and the services NTT DATA provides to its customers, and apply to all NTT DATA personnel, such as employees and third-party contractors. These policies are generally aligned with industry standards and guide all areas of security within NTT DATA. Reflecting the recommended practices in security standards issued by the United States National Institute of Standards and Technology (NIST), and other industry sources. NTT DATA implements a wide variety of preventive, detective and corrective security controls with the objective of protecting information assets.

TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES

NTT DATA maintains the following security standards for the data protection and system integrity. These standards are subject to enhancements and change as determined by NTT DATA's local and global Chief Information Security Officer in alignment with our information security policy.

Encryption and Pseudonymization

Encryption is intended to prevent access to Personal Data by unauthorized persons or provide warning of the same (e.g. hacker attacks or espionage). Encryption refers to the process of converting data into a form known as ciphertext, which is difficult for unauthorized persons to understand.

Measures pertaining to the Encryption :

- Selection of a suitable method for encryption using the latest technology
- Regular checking of encryption methods for security loopholes and updating of relevant software as required
- Email encryption
- Deletion concept for sent encrypted files
- Use an encryption method corresponding to the data protection concept
- Encryption on directory and file level

Pseudonymization is the processing of Personal Data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, provided that this additional information is kept separately and is subject to corresponding technical and organizational measures.

Measures pertaining to the pseudonymization :

- Selection of a suitable method for pseudonymization using the latest technology
- Pseudonymization of data in accordance with a risk-based approach and the different protection requirements applicable to different categories of data
- The pseudonymization requirement is a central component of the data protection concept
- Use of software that allows management of pseudonymized data

- Secure storage of the cryptographic keys and checklists used for pseudonymization (encrypted storage of checklists, if necessary)
- Authorization concept for access to cryptographic keys or control lists allowing personalization.

Physical Access Control.

Unauthorized persons are prevented from gaining physical access to premises, buildings or rooms where data processing systems that process and/or use Personal Data are located.

Measures:

- Protecting assets and facilities by using security classification which are periodically assessed by an internal security department.
- Securing buildings through access control systems (e.g., mantrap or smart card access system).
- As a minimum requirement, the outermost entrance points of the building are fitted with a certified key system including modern, active key management.
- Depending on the security classification, buildings, individual areas and surrounding premises may be further protected by specific access profiles, video surveillance, intruder alarm systems and biometric access control systems.
- Access rights are granted to authorized persons on an individual basis according to the System and Data Access Control measures. This also applies to visitor access. Guests and visitors to NTT DATA buildings must register their names at reception and must be accompanied by authorized NTT DATA personnel.
- NTT DATA employees and external personnel must wear their ID cards at all NTT DATA locations.

Additional measures for physical access at Data Centers:

- All Data Centers adhere to strict security procedures enforced by surveillance cameras, motion detectors, access control mechanisms and other measures to prevent equipment and Data Center facilities from being compromised.
- Only authorized representatives have access to systems and infrastructure within the Data Center facilities.
- To provide proper functionality, physical security equipment (e.g., motion sensors, cameras, etc.) undergo maintenance on a regular basis.
- NTT DATA and all third-party Data Center providers log the names and times of persons entering NTT DATA private areas within the Data Centers.

System Access Control.

Data processing systems used to provide the NTT DATA Services are designed to prevent use without authorization.

Measures:

- Multiple authorization levels are used when granting access to sensitive systems, including those storing and processing Personal Data. Processes are in place so to that authorized users have the appropriate authorization to add, delete, or modify users.
- Users access NTT DATA systems with a unique identifier (user ID).
- Procedures in place to confirm that requested authorization changes are implemented only in accordance with the guidelines (for example, no rights are granted without authorization). If a user leaves the company, his or her access rights are revoked.
- Password policy that prohibits the sharing of passwords, governs responses to password disclosure, and requires passwords to be changed on a regular basis and default passwords to be altered. Personalized user IDs are assigned for authentication. All passwords must fulfil defined minimum requirements and are stored in encrypted form. In the case of domain passwords, the system forces a password changes regularly in compliance with the requirements for complex passwords. Each computer has a password-protected screensaver.

- Firewalls to protect the NTT DATA network from the public .
- Up–to-date antivirus software at access points to the company network (for e-mail accounts), as well as on all file servers and all workstations.
- Security patch management to provide regular and periodic deployment of relevant security updates based on customer availability and approval.
- Two factor authentication for remote access to NTT DATA corporate network and infrastructure.

Data Access Control.

Persons entitled to use data processing systems gain access only to the Personal Data that they have a right to access, and Personal Data must not be read, copied, modified or removed without authorization in the course of processing, use and storage.

Measures:

- Personal Data requires at least the same protection level as "confidential" information.
- Access to personal, confidential or sensitive information is granted on a need-to-know basis.
- Authorization concepts that document how authorizations are assigned and which authorizations are assigned to whom.
- Personal, confidential, or otherwise sensitive data is protected in accordance with the NTT DATA security policies and standards. Confidential information must be processed confidentially.
- Production servers are operated in the Data Centers or in secure server rooms. Security measures that protect applications processing personal, confidential or other sensitive information are regularly checked.
- Internal and external security checks and penetration tests on its IT systems.
- Security standard governing how data is deleted or destroyed once they are no longer required.
- Equipment (laptops/servers) utilizing full disk encryption to protect data at rest.

Data Transmission Control.

Except as necessary for the provision of the Services in accordance with a client's relevant agreement, Personal Data must not be read, copied, modified or removed without authorization during transfer. Where data carriers are physically transported, measures are implemented at NTT DATA to comply with the agreed-upon service levels (for example, encryption and lead-lined containers).

Measures:

- Personal Data transfer over NTT DATA internal networks are protected in the same manner as any other confidential data according to NTT DATA Security Policy.
- When data is transferred between NTT DATA and its clients, the protection measures for the transferred Personal Data are set forth in a Data Processing Agreement. This applies to both physical and network-based data transfer.
- Client assumes responsibility for any data transfer once it is outside of NTT DATA-controlled systems (e.g. data being transmitted outside the firewall of the Data Center).

Data Input Control.

NTT DATA is able to retrospectively examine and establish whether and by whom Personal Data have been entered, modified or removed from NTT DATA's data processing systems.

Measures:

- Only authorized persons are allowed to access Personal Data as required in the course of their work.
- In Client's SAP system, Client controls the input, modification and deletion, or blocking of Personal Data by NTT DATA or its subprocessors.
- SAP standards are applied s to inserting, deleting, or modifying SAP records.

Job Control.

Personal Data being processed on a client's behalf is processed solely in accordance with the relevant agreement and related instructions of the client.

Measures :

- Controls and processes aligned with industry standards when working with clients, subprocessors or other service providers.
- Employees and contractual subprocessors or other service providers are contractually bound to respect the confidentiality of all sensitive information including trade secrets of NTT DATA clients and partners.
- For remote administration of on-premise systems, NTT DATA uses a secure VPN connection for connectivity in which the client owns security management of the managed systems.

Availability Control.

Personal Data is protected against accidental or unauthorized destruction or loss.

Measures:

- Backup processes and other measures that rapidly restore business critical systems as and when necessary.
- Uninterrupted power supplies (for example: UPS, batteries, generators, etc.) to provide power availability to the Data Centers.
- Defined contingency plans as well as business and disaster recovery strategies for the provided services.
- Emergency processes and systems are regularly tested.

Data Separation Control.

Personal Data collected for different purposes are processed separately.

Measures:

- NTT DATA uses the technical capabilities of the deployed software (for example: multi-tenancy, or separate system landscapes) to achieve data separation among Personal Data originating from multiple clients.
- Clients have access only to their own data.
- If Personal Data is required to handle a support incident from a specific client, the data is assigned to that particular message and used only to process that message; it is not accessed to process any other messages. This data is stored in dedicated support systems.

Data Integrity Control.

Personal Data will remain intact, complete and current during processing activities.

Measures:

- A multi-layered defence strategy as a protection against unauthorized modifications.
- NTT DATA uses the following to implement the control and measure described above:
  - Firewalls;
  - Security Monitoring Center;
  - Antivirus software;
  - Backup and recovery;
  - External and internal penetration testing;
  - Regular external audits (SSAE 18 SOC 1 Type 2/ ISAE 3402 and SOC 2 Type 2) to prove security measures.

Controls for compliance with security and privacy requirements.

- Employees are required to go through annual security/privacy training.
- Client specific security and privacy concerns are addressed with employees and third-party service providers prior to client engagements.

- Employees and third-party service providers understand that they are prohibited from accessing client systems or data unless required for the performance of client services or through direct instructions from the client.
- Employees and third-party service providers that engage in prohibited conduct will be removed from client engagement.