NOVARTIS

Minimum Information Security Controls for Third Parties[1]

Version 4.0

April 2024

Information Security and Compliance

[1] The Minimum Information Security Controls for Third Parties can be found here: https://www.novartis.com/esg/reporting/codes-policies-and-guidelines

Minimum Information Security Controls for Third Parties[2]

1. Governance and Compliance

- Third Party shall implement and maintain an information security program, consistent with security industry practice and applicable laws and regulations, to protect the systems and network infrastructure, as well as the confidentiality, integrity, availability, and resiliency of data, at minimum, as set forth in this document and to ensure a level of security appropriate to the risk.
- Third Party shall ensure that it has nominated an appropriate individual to hold accountability on behalf of Third Party for ensuring technical and organizational compliance with information security controls.
- Third Party's information security program must include a governance framework with supporting risk management policies that will enable and support risk management.

2. Business Continuity

- Third Party shall have appropriate business continuity and disaster recovery plans to ensure timely recovery of its IT systems involved in any operation with data, in any form, supporting the services provided to Novartis, in the event of a disaster or other significant disruptive event.
- Third Party shall ensure that its disaster recovery plans are periodically tested and updated to ensure they are up-to-date and effective.
- Third Party shall ensure that technologies and processes used for data backup and recovery are regularly tested and have sufficient protection against any disruptive cyber-attacks.

3. Media Handling

- Procedures for the handling and storage of data shall be established by Third Party to protect data from unauthorized disclosure or misuse.
- Third Party shall ensure media is disposed of securely and safely when no longer required, using formal procedures with proper documentation.
- Third Party shall upon termination of the contractual relationship with Novartis or upon Novartis' request return to Novartis all media and other assets provided to Third Party by Novartis.
- Third Party shall ensure that system documentation is protected against unauthorized access.

4. Exchange of Data

- Third Party shall maintain the confidentiality, integrity, availability and resiliency of data and systems hosting or accessing such data within its organization and within any external entity; this includes exchange agreements, physical media in transit, electronic messaging and the protection of data associated with the interconnection of business information systems.

[2] Capitalized expressions used in this document have the same meaning as in the latest version of the Novartis Third Party Code (available at https://www.novartis.com/esg/reporting/codes-policies-and-guidelines) unless expressly defined in the attached glossary, stated otherwise or the context requires otherwise. In this document, reference to "Third Party" or "Third Parties" is limited only to such third parties that would be classified as falling under the definition of "Suppliers" in the Novartis Third Party Code.

5. Access Control

- Third Party must have an access control policy that ensures that only authorized users that have a business need that is approved will have access to Novartis data.
- Third Party shall review user access rights to ensure that the allocation and use of privileges are controlled and restricted where necessary and as applicable to Novartis data or any systems storing such data.

6. Cryptographic Control

- Considering relevant information security risks, state of the art, security industry practice and applicable laws and regulations, Third Party shall design, implement and maintain cryptographic controls, including encryption as appropriate of Novartis data.

7. Controlled Processing and Usage of Artificial Intelligence

- Third Party shall ensure separate processing of data collected for different purposes, e.g. multi-client capability, sandboxing, development/testing vs. production environment which is used by end-users.
- Third Party shall ensure that, only data which are necessary for each specific purpose of the processing are processed, by applying as appropriate data sanitization/minimization and data removal techniques.
- Third Party shall only use AI systems for processing Novartis´ data following prior agreement from Novartis. In such a case, Third Party shall maintain appropriate safeguards in accordance with the best industry practices (for example, prohibition of using Novartis data for training, anonymization of Novartis data, secure handling of Novartis data etc.) related to usage of such AI systems.

8. Communications and Network Security

- Third Party shall ensure that networks under Third Party's control are adequately managed, controlled and protected from threats and vulnerabilities, and shall maintain the confidentiality, integrity, and availability of data and prevent the unauthorized access to such systems and applications used to process data at rest or in transit.
- Third Party connecting to Novartis environment shall ensure it is capable of meeting the relevant Novartis technical standards applicable to such environment.

9. Security Training and Awareness

- Third Party shall ensure that all its Workers, contractors and agents are aware of information security threats and concerns, their responsibilities, and are equipped to support organizational security policy in the course of their work.
- Third Party will ensure that, all Workers, contractors and agents shall receive appropriate information security and data protection awareness training.
- Third Party shall ensure that its Workers use institutional e-mail addresses (as opposed to personal email or communication platform accounts) for any correspondence containing or relating to Novartis data.

10. Physical and Environmental Security

- Third Party shall ensure that appropriate information security perimeters and entry controls are in place to prevent unauthorized physical access, damage and interference to Third Party's premises and data including all end user devices.
- Third Party shall ensure that equipment is properly inventoried and maintained to ensure its continued information security.

11. Protection of Organizational Records

- Third Party shall ensure their information security program includes policies that cover data retention and data destruction consistent with security industry practice.
- Third Party shall ensure appropriate controls are implemented to prevent the loss, destruction, or falsification of records during their retention period, including determining whether and by whom data has been entered, accessed, modified or removed from data processing systems.
- Third Party agrees that upon the request of Novartis or as otherwise required by law, it shall dispose of (e.g. erase, destroy or render uninterpretable) all Novartis data that Third Party, its affiliates or subcontractors hold or manage (acknowledging that copies of the Novartis data may reside on Third Party's standard backup media that are subject to standard backup rotation scheme and are secured according to recognized and then-current data privacy practice and security industry practice). Third Party shall provide to Novartis report with appropriate level of detail on Novartis data stored on backup media upon Novartis request at no additional costs to Novartis. Novartis shall have the right to receive a copy of Novartis data in the form and within the timeframe specified by Novartis before its disposal.
- Where requested by Novartis, Third Party shall certify in writing that these actions have been completed.
- The following shall be considered as exceptions to this disposal requirement:
  - Third Party must keep Novartis data on file for legal or regulatory purposes; such Novartis data shall then be removed as soon as the legal retention periods have expired
  - Novartis data which Novartis has requested Third Party to keep archived for legal hold or other comparable purposes
  - Where Novartis has agreed in writing with Third Party specific return/destruction/retention requirements in respect of certain Novartis data, in which case, such specific requirements will apply.

12. Technical Vulnerability Management

- Third Party shall have a vulnerability management program that monitors and maintains the information security state of the Third Party environment.
- Third Party shall establish and maintain policies that demonstrate adequate application of updates and patch management of Third Party IT systems.
- Third Party shall create and maintain hardware and software inventories and conduct regular vulnerability scans.

13. Information Security Incident Management

- Third Party will ensure that management responsibilities and procedures are established to ensure a quick, effective and orderly response to security incidents and to report and manage information security incidents and weaknesses including appropriate reporting.
- Third Party will promptly inform Novartis in case of a security incident related to Novartis data.

14. Monitoring

- Third Party must monitor its environment to detect and respond to information security incidents or other unauthorized activities.
- Third Party shall ensure audit controls are implemented within the Third Party environment under Third Party's control to enable independent audits/testing of appropriate audit data on operational systems while minimizing the risk of disruption to processes.

15. Configuration and Change Management

- Third Party shall have a change management process that ensures that the impact of changes is understood prior to rollout, includes criteria for establishing the success or failure of a change, and ensures that any roll-back procedures for failed changes are approved before changes are made.

16. Harmful Code Prevention

- Third Party shall develop policies to manage the risks associated with the malicious use of harmful code and implement anti-malware defenses.