NOVARTIS

Minimum Information Security Controls[1]

Information Security and Risk Management

[1] The document to be found here: https://www.novartis.com/about-us/corporate-responsibility/resources/codes-policies-guidelines/

Minimum Information Security Controls[2]

1. Governance and Compliance

- Supplier shall implement organizational security policies and standards aligned to security industry standards and ensure compliance with those.
- Supplier shall ensure that it has nominated an appropriate individual to hold accountability for ensuring technical and organizational compliance with security and privacy controls as defined in this contract and in the Supplier's own policies.

2. Continuity

- The Supplier shall have appropriate business continuity plans, including IT disaster recovery, in place to counteract and / or ensure timely recovery of its IT systems storing or processing Novartis data or IT systems otherwise supporting the services provided to Novartis, in case of a disaster.
- The Supplier shall ensure that its disaster recovery plans are tested and updated regularly to ensure they are up-to-date and effective.
- Supplier shall maintain the integrity and availability of information and information processing facilities through back up-copies of information and software, which shall be taken and tested regularly in accordance with the agreed backup policy.

3. Media Handling

- Procedures for handling and storage of information shall be established by the Supplier to protect information from unauthorized disclosure or misuse.
- Supplier shall ensure media is disposed of securely and safely when no longer required, using formal procedures.
- Supplier shall ensure that system documentation is protected against unauthorized access.

4. Exchange of Information

- Supplier shall maintain the security of information and software exchanged within its organization and within any external entity; this includes exchange agreements, physical media in transit, electronic messaging and the protection of information associated with the interconnection of business information systems.

5. Access Control

- Supplier shall establish and implement an access control policy to ensure authorized access to users and to prevent unauthorized access, in particular, to sensitive personal data.
- Supplier shall review user access rights to ensure that the allocation and use of privileges are controlled and restricted where necessary.

6. Cryptographic Control

- In higher risk situations the Supplier shall supplement existing access controls with encryption solutions both for data at rest as in transit. Higher risk may relate to:

[2] Capitalized expressions used in this document have the same meaning as in the Novartis Supplier Code (https://www.novartis.com/about-us/corporate-responsibility/resources/codes-policies-guidelines) unless expressly defined in the attached glossary, stated otherwise or the context requires otherwise.

  - the type of data (e.g. sensitive personal information or information can materially impact Novartis requires better protection than data that is not personal information or otherwise confidential)
  - the related vulnerabilities (e.g. data stored in internet facing system is more vulnerable then data stored inside the private network)
  - the related threats (e.g. data in transit over an open network is more threat sensitive).
- The Supplier shall have a policy on the use of cryptographic controls for protection of information that is implemented and followed.

7. Network Control

- Supplier shall ensure that networks are adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit.

8. Security Training and Awareness

- Supplier shall ensure that all employees, contractors and third party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organizational security policy in the course of their work.
- Supplier shall ensure that its employees, contractors and third party that handle personal information (including coded) are aware of the definition of personal data and sensitive personal data as stated by the European Commission and such other relevant authorities.
- Supplier will ensure that where relevant, all employees, contractors and third party users shall receive appropriate awareness training.
- Supplier shall ensure that its employees use institutional e-mail addresses when communicating or transferring data and/or personal data.

9. Physical and Environmental Security

- Supplier shall ensure that the appropriate security perimeters and entry controls are in place to prevent unauthorized physical access, damage and interference to the Supplier's premises and information including all end user devices.
- Supplier shall ensure that equipment is correctly maintained to ensure its continued availability and integrity.

10. Protection of Organizational Records

- Supplier shall ensure their security policy includes data retention and data destruction policies and security standards.
- Supplier shall ensure appropriate controls are implemented to prevent records from loss, destruction or falsification during their retention period.
- Supplier agrees that upon the request of Novartis or upon termination of the Agreement, it shall dispose (e.g. erase, destroy or render unreadable) all Novartis data that Supplier, its Affiliates or subcontractors hold, (excluding any and all copies of the Novartis data residing on the Supplier's standard backup media, providing that such backup media are secured according recognized and then-current data privacy and data security best practices). Supplier 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.
- Where requested by Novartis, Supplier shall certify in writing that these actions have been completed.

- The following shall be considered exceptions to this disposal requirement:
  - Supplier 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 Supplier to keep archived for legal hold purposes

11. Technical Vulnerability Management

- Supplier shall endeavor to reduce risks resulting from exploitation of published technical vulnerabilities.
- Supplier shall implement applicable industry best practices which are defined for example in Center for Internet Security (CIS) standards (https://www.cisecurity.org/)

12. Information Security Incident Management

- Supplier 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.

13. Monitoring

- Supplier will use appropriate systems and controls to detect unauthorized information processing activities.

14. Configuration Management

- Supplier shall establish and maintain policies that demonstrate adequate application of updates and patch systems.
- Supplier shall create and maintain hardware and software inventories and conduct regular vulnerability scans.
- Supplier shall ensure audit controls are implemented to enable independent audits/testing of appropriate audit data on operational systems while minimizing the risk of disruption to business processes.

15. Harmful Code Prevention

- Supplier shall develop policies that manage the risks to the business processes from harmful code and include anti-malware defenses.

16. Information Risk Management

- Supplier shall establish a governance framework with supporting risk management policies that will enable and support risk management.

Glossary

"**Agreement**" means any formal written contract signed between Supplier and/or its Affiliates and Novartis and/or its Affiliates which incorporates by reference or otherwise the Novartis Supplier Code (version 3) (excluding for this purpose a confidentiality/non-disclosure agreement under which no products/goods or services are provided).

"**Affiliate**" means, unless defined otherwise in the context of a specific Agreement (in which case the expression Affiliate shall be defined, for the purposes only of such specific Agreement, in accordance with the definition contained therein) any person, firm or corporation that directly or indirectly controls or is controlled by or is under common control with Novartis (in this case a "Novartis Affiliate") or Supplier (in this case a "Supplier Affiliate"). For purposes of this definition, "control," "controls" or "controlled" means ownership directly or through one or more Affiliates, of fifty percent (50%) or more of the shares of stock entitled to vote for the election of directors, in the case of a corporation, or fifty percent (50%) or more of the equity interests in the case of any other type of legal entity, status as a general partner in any partnership, or any other arrangement whereby a party controls or has the right to control the board of directors or equivalent governing body of a corporation or other entity, or the ability to cause the direction of the management or policies of a corporation or other entity.