



Privacy Policy

1. Purpose

The purpose of this Privacy Policy is to ensure that NevadaNano complies with SOC 2 requirements for the protection of personal and sensitive information. This policy outlines how we collect, use, store, and disclose personal information to ensure the privacy and security of individuals' data.

2. Scope

This policy applies to all personal information collected, processed, stored, and shared by NevadaNano. It covers all employees, contractors, and third-party service providers who have access to this data.

3. Policy Statement

NevadaNano is committed to protecting the privacy of personal information. We adhere to the principles of transparency, security, and user control in our data handling practices. This policy establishes the guidelines for collecting, using, storing, and sharing personal information.

4. Definitions

- **Personal Information:** Any information relating to an identified or identifiable individual, including but not limited to name, address, email, phone number, financial information, and identification numbers.
- **Sensitive Information:** A subset of personal information that includes data such as social security numbers, health records, and financial information.
- **Data Subject:** Any individual whose personal information is collected, stored, or processed by NevadaNano.

5. Collection of Personal Information

- **Lawful Basis:** Personal information will be collected only for legitimate business purposes, with the consent of the data subject, or as required by law.
- **Data Minimization:** Only the minimum amount of personal information necessary for the specified purpose will be collected.
- **Transparency:** Data subjects will be informed about the purpose of data collection, how their information will be used, and their rights regarding their data.

6. Use of Personal Information

- **Purpose Limitation:** Personal information will be used only for the purposes for which it was collected, unless consent is obtained from the data subject for other uses.
- **Data Accuracy:** Efforts will be made to ensure that personal information is accurate, complete, and up to date.
- **Access Control:** Access to personal information will be restricted to authorized personnel who need it to perform job duties.

7. Storage and Protection of Personal Information

- **Data Security:** Personal information will be stored securely using appropriate technical and organizational measures to protect against unauthorized access, alteration, disclosure, or destruction.
- **Encryption:** Sensitive personal information will be encrypted both in transit and at rest.
- **Data Retention:** Personal information will be retained only as long as necessary to fulfill the purposes for which it was collected or as required by law.
- **Disposal:** Personal information will be disposed of securely to prevent unauthorized access and use.

8. Sharing of Personal Information

- **Third-Party Disclosure:** Personal information will be shared with third parties only for legitimate business purposes, with the consent of the data subject, or as required by law.
- **Third-Party Agreements:** Third parties receiving personal information must agree to comply with privacy and security standards consistent with this policy.
- **International Transfers:** Personal information transferred outside of the country will be protected in accordance with applicable data protection laws.

9. Data Subject Rights

- **Access:** Data subjects have the right to request access to their personal information.
- **Correction:** Data subjects have the right to request corrections to inaccurate or incomplete personal information.
- **Deletion:** Data subjects have the right to request the deletion of their personal information, subject to certain conditions.
- **Objection:** Data subjects have the right to object to the processing of their personal information for certain purposes.
- **Portability:** Data subjects have the right to request a copy of their personal information in a portable format.

10. Incident Response and Breach Notification

- **Incident Management:** Procedures will be in place to detect, respond to, and recover from data breaches and security incidents.
- **Breach Notification:** Data subjects and relevant authorities will be notified of data breaches in accordance with applicable laws and regulations.

11. Training and Awareness

- **Employee Training:** Regular training will be provided to employees on privacy policies, data protection practices, and their responsibilities.
- **Awareness Programs:** Awareness programs will be conducted to reinforce the importance of privacy and data protection.

12. Compliance and Review

- **Compliance Audits:** Regular audits will be conducted to ensure compliance with this privacy policy and SOC 2 requirements.
- **Policy Review:** This policy will be reviewed annually or as required due to changes in laws, regulations, or business practices.
- **Enforcement:** Non-compliance with this policy may result in disciplinary actions, including termination of employment or contract.

13. Enforcement

Violations of this policy may result in disciplinary action, up to and including termination of employment. Legal action may also be taken where applicable.

14. Revision History

DATE OF CHANGE	RESPONSIBLE	SUMMARY OF CHANGE
JUNE 2024		DRAFT.
JULY 9, 2024		REVISION 1
MAY 16, 2025	JEFFREY SNYDER	APPROVED