Information Security Policy

Company	Document Date	Version Number
Nevin Consultant Group	November 05, 2025	v1.0

1. Introduction

a. Nevin Consultant Group ("we," "our," or "us") is committed to safeguarding the confidentiality, integrity, and availability of client data, research materials, and all interactions conducted through our website and digital platforms. This Information Security Policy outlines the technical, administrative, and procedural safeguards we implement to protect sensitive information from unauthorized access, disclosure, alteration, or destruction.

b. This policy supplements the Terms and Conditions and is subject to the terms of any applicable Master Service Agreement ("MSA") or Statement of Work ("SOW").

2. Data Protection Measures

a. We employ a layered security approach that includes:

i. Secure server infrastructure with firewalls and intrusion detection systems.

ii. Encrypted data transmission using HTTPS and TLS 1.2 or higher.

iii. Role-based access controls (RBAC) to limit data access to authorized personnel only.

iv. Multi-factor authentication (MFA) for administrative and sensitive systems.

v. Regular software updates and vulnerability patching to mitigate known threats.

vi. Endpoint protection and secure device management for all internal systems.

3. Data Encryption Standards

a. Data at Rest: Encrypted using industry-standard protocols such as AES-256.

b. Data in Transit: Protected using TLS 1.2 or higher to ensure secure communication.
c. Encryption Key Management: Keys are stored securely, access is restricted, and keys are rotated periodically to maintain data confidentiality and integrity.

4. Secure File Transfer Protocols

a. When transmitting confidential, proprietary, or sensitive information, we use:
    i. SFTP (Secure File Transfer Protocol).
    ii. Encrypted email attachments.
    iii. Client-approved secure portals.
b. We do not transmit sensitive data over unsecured channels such as unencrypted email or public file-sharing platforms.

5. Compliance with Cybersecurity Frameworks

a. Nevin Consultant Group aligns its security practices with recognized industry standards, including:
    i. ISO/IEC 27001 – Information Security Management Systems (ISMS).
    ii. NIST Cybersecurity Framework (CSF) – for risk assessment, mitigation, and continuous improvement.
b. These frameworks guide our approach to:
    i. Risk identification and mitigation.
    ii. Data governance and access control.
    iii. Incident response and recovery.
    iv. Ongoing security training and awareness.

6. Third-Party Service Providers

a. All third-party vendors used for hosting, analytics, communications, or project delivery are vetted for security compliance.
b. Vendors are contractually obligated to protect client data and may not use or disclose such data for any purpose other than service delivery.
c. Nevin Consultant Group does not authorize third-party providers to commercially exploit or sell client data without explicit written consent.

7. Monitoring & Incident Response

a. We monitor systems for suspicious activity and unauthorized access attempts.
b. A formal incident response protocol is in place to address potential data breaches or security events.

c. In the event of a confirmed breach, affected parties will be notified in accordance with:
    i. Applicable data protection laws (e.g., GDPR, CCPA).
    ii. Contractual obligations outlined in the MSA or DPA.

8. User Responsibility

a. Users are responsible for maintaining the confidentiality of any login credentials, access tokens, or secure links provided by Nevin Consultant Group.
b. If you suspect unauthorized access or misuse of your credentials, please notify us immediately via the contact method listed in the Contact Information section of our Terms and Conditions.

9. Security Audits & Continuous Improvement

a. We conduct periodic internal audits and may engage third-party security professionals to perform external reviews.
b. Audit findings are used to inform updates to our security posture and ensure compliance with evolving standards and threats.
c. We are committed to continuous improvement in all aspects of information security.

10. Client-Specific Security Commitments

a. For engagements involving sensitive or regulated data, Nevin Consultant Group offers the following client-specific security assurances:
    i. Custom Security Controls: Upon request, we will implement additional controls such as data residency restrictions, custom encryption protocols, or limitations on third-party tools, as documented in the applicable SOW or project brief.
    ii. Sub-Processor Transparency: A list of approved sub-processors is available upon request. All sub-processors are contractually bound to equivalent data protection obligations.
    iii. Data Retention & Return: Upon project completion or termination, we will return or securely delete all client data as directed. Written certification of deletion is available upon request.
    iv. Audit Rights: Clients may request a security review or documentation audit with reasonable notice. We will cooperate in good faith, subject to confidentiality and operational constraints.

11. Questions or Concerns?

a. If you have any questions, concerns, or requests regarding these policies, please contact us using one of the following methods:
   i. Email: support@nevinconsultant.com
   ii. Website Contact Form: https://nevinconsultant.com/contact-us/
   iii. Mailing Address:

   Nevin Consultant Group
   732 South 6th Street, STE 4893
   Las Vegas, Nevada 89101

b. We aim to respond to all inquiries within five (5) business days. For urgent compliance matters, please indicate the nature of your request in the subject line.