Information Security and Data Protection Statement

This statement sets out the approach NOV8 Consulting has taken to date throughout the current and future financial years, with the aim of ensuring all business is conducted with confidentiality. All information handled by NOV8 Consulting, including client data, internal information, project documentation and personal data will be in line with UK GDPR, obligations and best practice.

Business Activities

All our consultants rely upon this statement to conduct business with confidentiality and integrity. This statement applies to all our staff, directors, contractors, consultants, and other third parties (collectively referred to as Personnel) acting on behalf of NOV8 Consulting, regardless of their workplace location. Its scope covers all systems and media (devices, cloud platforms, client systems, removable media and printed records) in compliance with Cyber Essentials Certification.

Legislation

NOV8 Consulting is committed to ensuring compliance with applicable standards:

- The UK General Data Protection Regulation (UK GDPR)
- The Data Protection Act 2018
- The Network and Information Systems (NIS) Regulations 2018, where applicable
- The Computer Misuse Act 1990
- The Privacy and Electronic Communications Regulations 2003 (PECR)
- Cyber Essentials Certification requirements
- ISO/IEC 27001 – Information Security Management, as a guiding framework

Core Principles

NOV8 Consulting's approach to information security and data protection is built on the following principles that apply to all information held and processed by the firm:

Confidentiality: Information is accessible only to those who are authorised to access it.

Integrity: The accuracy and completeness of information and processing methods is always safeguarded.

Availability: Authorised users can access the information and systems they need, when they need them.

Lawfulness: All personal data is collected and processed on a valid lawful basis in accordance with UK GDPR.

Transparency: Individuals are informed about how their personal data is used, through clear and accessible privacy notices.

N.O.V8 Consulting Ltd

Accountability: NOV8 Consulting can demonstrate compliance with its data protection obligations and takes responsibility for the personal data it holds.

Roles and Responsibilities

Board of Directors: The Board has overall accountability for information security and data protection at NOV8 Consulting. The Board approves this policy and ensures that sufficient resources are allocated to maintain effective controls.

Managing Director: The Managing Director is responsible for overseeing the implementation of this policy, for responding to significant security incidents, and for ensuring that data protection and information security considerations are embedded in business operations.

All Personnel: All Personnel are responsible for reading and complying with this policy, completing required training, and promptly reporting any security incidents, suspected data breaches, or concerns to the admin team or Managing Director.

Access Control

NOV8 Consulting systems and data are controlled and granted strictly on the principle of least privilege, allowing Personnel access to information to perform their role:

- All Personnel must have unique, individual login credentials; account sharing is strictly prohibited
- Access rights must be reviewed regularly and revoked promptly upon departure or change of role
- Strong passwords of at least 12 characters must be used
- Multi-factor authentication (MFA) must be enabled on all systems where available, and is mandatory for remote access and email
- Privileged administrative access must be restricted to those with a legitimate and documented operational need

Device Security

All devices used to access NOV8 Consulting systems and data are to meet the following standards:

- Operating systems, applications, and security software must be kept up to date with the latest patches and updates
- Approved and up-to-date anti-malware software must be installed and active on all devices
- Full-disk encryption must be enabled on all laptops and mobile devices
- Devices must be locked when unattended and must require authentication to unlock
- Lost or stolen devices must be reported to the Managing Director and IT Lead immediately so that access revocation can be actioned

Remote Working Network Security

All devices used to access NOV8 Consulting systems and data must meet the following controls when working outside company premises:

- A Virtual Private Network (VPN) is used when accessing firm systems from any external network
- Public or unsecured Wi-Fi must not be used to access sensitive client or firm data without an active VPN connection
- Home network routers should be secured with a strong, unique password and kept up to date with the latest firmware

- Personnel must ensure that sensitive on-screen information cannot be viewed by others when working in public spaces

Email and Phishing

All NOV8 Consulting Personnel undergo Cyber Security training including the following:

- Be vigilant about phishing emails and verify the identity of senders before opening attachments or clicking links
- Never provide credentials, personal data, or financial information in response to an unsolicited or unexpected request
- Report suspicious emails to the IT Lead or Managing Director immediately, without clicking any embedded links or opening attachments
- Not use personal email accounts to send, receive, or store NOV8 Consulting business information

Data Protection and Personal Data

Lawful Processing: NOV8 Consulting will only collect and process personal data where it has a valid lawful basis for doing so under UK GDPR. The firm will document the lawful basis for each category of personal data it processes and will not use personal data for purposes incompatible with those for which it was originally collected.

Data Minimisation: NOV8 Consulting will only collect and hold the personal data that is necessary for the specific purpose for which it is being processed. Personnel must not collect personal data "just in case" it may be useful in the future.

Data Handling

All data held by NOV8 Consulting must be handled in accordance with the following:

- Client and personal data must not be stored on unencrypted or unauthorised devices or platforms
- Sensitive or special category personal data must be identified, handled with additional care, and access restricted to those with a specific need
- Data must be shared only via approved, secure channels and never via unencrypted email where avoidable
- The firm's Privacy Policy and Data Retention Schedule must be followed at all times

Data Retention and Disposal: Personal data must not be retained for longer than is necessary for the purpose for which it was collected. When data reaches the end of its retention period we securely delete or destroy it in a manner appropriate to its sensitivity.

Data Subject Rights: Individuals have rights in relation to their personal data under UK GDPR, including the right to access, rectify, erase, and restrict processing of their data. NOV8 Consulting will respond within the statutory timeframe of one calendar month.

Privacy: NOV8 Consulting will provide clear, transparent, and accessible privacy notices to individuals whose personal data it collects, explaining what data is collected, how it is used, with whom it is shared, and how long it is retained.

Third Party and Cloud Security

NOV8 Consulting uses Cloud-based services and relies on third-party technology vendors. Where those vendors process personal data on behalf of the firm, they act as data processors and are subject to the requirements of UK GDPR. We will:

- Assess the security standards and data protection credentials of all key technology providers
- Ensure appropriate Data Processing Agreements (DPAs) are in place with all suppliers who process personal data on behalf of the firm
- Limit the sharing of personal and sensitive data with third parties to what is strictly necessary
- Regularly review third-party access rights and revoke access when it is no longer required
- Not transfer personal data outside the UK without ensuring that appropriate safeguards are in place, in accordance with UK GDPR transfer rules

Use of Artificial Intelligence Tools

AI tools may be used only where approved by the Managing Director and necessary for NOV8 Consulting business activities. They must be used securely, with human review of outputs and in line with the below:

- Use only approved AI tools or AI-enabled services
- Do not enter client confidential information, personal data, credentials or sensitive business information into public or unauthorised AI tools
- Apply data minimisation and review AI-generated outputs before use
- Report any suspected AI-related security incident, data breach or misuse immediately

IT Disaster Recovery

NOV8 Consulting maintains IT disaster recovery arrangements to support business continuity and protect confidentiality, integrity and availability of information. Core controls include Cyber Essentials certification, cloud-first working, MFA, encrypted devices, secure backups and documented recovery steps.

The firm will prioritise restoration of communications, client files and critical administrative systems, with clear responsibility for incident escalation, containment, recovery and external communications.

- Maintain secure backups, cloud versioning and recovery routes for business and client information
- Isolate affected devices or accounts, preserve evidence and notify the Managing Director or appointed IT provider immediately
- Review recovery arrangements annually to confirm access, backups, contact details and restore processes remain effective

Reporting Incidents

All Personnel must report suspected or confirmed security incidents: data breaches, ransomware attacks, device loss, unauthorised access, and accidental disclosure immediately. All Personnel must:

- Not attempt to resolve the incident independently without guidance from the IT Lead or Managing Director
- Preserve evidence by not deleting files, emails, or system logs without explicit instruction
- Document what happened, when, and what data or systems may be affected
- Where a personal data breach meets the threshold for the reporting, the Managing Director must notify the Information Commissioner's Office within 72 hours of becoming aware of the breach, in accordance with UK GDPR Article 33

Training and Awareness

Cyber security and data protection are the responsibility of every member of Personnel. NOV8 Consulting will:

- Provide mandatory information security and data protection training to all Personnel
- Refresh training at least annually and following any significant incident or regulatory change
- Issue periodic security awareness communications to keep Personnel informed of emerging threats, phishing campaigns, and best practice

Acceptable Use of IT Systems

NOV8 Consulting's information systems must be used primarily for legitimate business purposes. Personnel must not:

- Install unauthorised software on firm-owned devices
- Use firm systems to access, store, or transmit illegal, offensive, or inappropriate content
- Attempt to access systems or data for which they are not authorised
- Circumvent, disable, or attempt to bypass any security control

Consequences of Non-Compliance

Failure to comply with this policy is a serious matter. Depending on the nature and severity of the breach, non-compliance may result in:

- Formal disciplinary action up to and including summary dismissal
- Personal criminal liability under the Computer Misuse Act 1990 or the Data Protection Act 2018
- Regulatory investigation and enforcement, including substantial financial penalties under UK GDPR
- Civil liability to individuals whose personal data has been affected

Quality Commitment Statement

We are committed to protecting information assets, delivering high-quality services and maintaining legal, regulatory and client compliance. We preserve confidentiality, integrity and availability; promote security awareness; and continually improve through monitoring, audits, training and feedback.

This statement will be reviewed at least annually by the Board of Directors and updated to reflect changes in legislation and regulatory guidance.

For and on behalf of the NOV8 Consulting Executive Board

Neil Porter
Managing Director
April 2026