1 Scope

1.1 This policy applies to all third parties that provide software, services, or other deliverables to the Top Energy Group, whether on-premises or as a cloud-based solution (further referred to as services).

1.2 There are three sections to this policy:

a) All third parties must comply with section I of this policy.

b) Third parties with formal attestation or certification against internationally accepted information security standards may elect to comply with section II.

c) Any third parties that do not comply with section II must comply with section III.

1.3 This policy applies in addition to any agreement (agreement) between you and a member of the Top Energy group. If there is a conflict between the terms of an agreement and the terms of this policy, then, to the extent of the conflict, priority will be given to the terms of the agreement.

1.4 Top Energy may change this policy at any time by providing written notice to you. Any updated policy will also be posted on Top Energy's website.

1.5 In this policy:

Good practice means the skill, diligence, care and foresight expected of a highly skilled and experienced person in the same or similar circumstances.

Malicious code means any virus, bomb, trojan horse or other malicious software or computer programming code that could impair, deny or otherwise adversely affect any Top Energy data, services or systems.

Related company has the same meaning as specified in section 2(3) of the Companies Act 1993 as if "company" includes a company or other corporate body incorporated or constituted in New Zealand or any other jurisdiction.

Security incident means the unauthorised access, use, alteration, or destruction of any Top Energy data or systems or any other compromise or breach of your or our electronic or physical security.

Security vulnerability means a weakness at the network, operating system, database or application software level or within associated functions (such as a physical vulnerability at the location where Top Energy data is stored) that could allow a security incident to occur.

Top Energy means Top Energy Limited or, in relation to an agreement, the member of the Top Energy Group that is a party to that agreement.

Top Energy data means all data, information, text, drawings and other materials in any form that a Top Energy Group member provides to you or that you generate, collect, process, hold, store or transmit in connection with an agreement, excluding your materials.

Top Energy Group means Top Energy Limited and each of its related companies.

Top Energy systems means the electronic information systems including hardware, equipment, software, peripherals and communications networks owned, controlled, operated or used by the Top Energy group.

We, us and our means Top Energy.

Your materials means all software, documents, and other materials created or owned by you or a third party independent of an agreement and provided to Top Energy by you or on your behalf.

Section I - policy requirements applicable to all third parties

2 Security Incidents

2.1 If you become aware of a security incident that has or may significantly impact the delivery of any service or the confidentiality of Top Energy data, or the integrity of Top Energy systems, you must:

a) Notify us within 24 hours of becoming aware of the incident.

b) Promptly, within 48 hours after the first notification, provide any additional information we reasonably request in relation to the incident, its manner of introduction and the impact that the incident had/is likely to have.

c) Provide regular status updates for the incident until it is resolved.

d) Provide as soon as practicable, but in any event within 7 days following resolution of the incident, a written report including;

i. The date the incident occurred.

ii. The length of any outage.

iii. A summary of the incident.

iv. Details such as how/when the incident was detected, what was impacted, and any containment strategies.

v. The incident's root cause.

vi. What corrective action was taken to prevent reoccurrence.

2.2 If we determine that other measures are required to contain, respond to or remediate a security incident (such as notice, credit monitoring services, fraud insurance or establishing a call centre to respond to customer inquiries), you will undertake those remedial actions. You will bear the cost of doing so if the incident was caused by your negligence, failure to follow your processes, failure to comply with this policy or an agreement, or any other act or omission by you (intentional or not).

2.3 You must treat the occurrence and impact of any security incident as confidential. If you are required by law to disclose any details of a security incident, you must, unless prohibited from doing so by applicable law, immediately notify us, and unless you have our prior written consent, you must only disclose the minimum required by law.

3 Protection Of Top Energy Data

3.1 Top Energy data is confidential to Top Energy. You must not access, store or use Top Energy data except as required to perform your obligations under an agreement. Top Energy data may not be incorporated into a generative AI tool without our prior written consent.

3.2 Where Top Energy data includes personal information (as defined in the Privacy Act 2020 or any successor legislation), you must hold and process that personal information following our obligations under the Privacy Act 2020 or any successor legislation and our privacy statement, available at https://topenergy.co.nz/tell-me-about/top-energy-group/publications-and-disclosures/privacy-policy.

If you supply software or provide software development services to the Top Energy group, you must also comply with clauses 4 and 5.

4 Malicious Code and Security Vulnerabilities

4.1 As a provider of software or software development services, you must take all precautions following good practices necessary to prevent the introduction of malicious code and security vulnerabilities that impact Top Energy data or Top Energy systems, including:

a) Using best endeavours to ensure that, when you provide us with software, it does not contain any malicious code or security vulnerabilities and that you do not otherwise introduce malicious code or security vulnerabilities into any Top Energy systems; and

b) Taking appropriate action when a security incident occurs, or malicious code or security vulnerabilities are discovered, such as quarantining the affected file, code, or hardware or software component (where applicable).

4.2 If you become aware of any security incident that involves the discovery or introduction of malicious code or security vulnerabilities, you must:

a) Identify the malicious code or security vulnerabilities and the corrective actions required to contain and resolve the incident.

b) Provide us with a software patch to fix, remedy, or remove the malicious code or security vulnerability as soon as reasonably practicable and, in any case, within one month or such other timeframe as we agree.

c) If requested by us, take all necessary and reasonable corrective action to eliminate the malicious code or security vulnerabilities and prevent reoccurrence (including implementing appropriate processes to prevent further occurrences) and rectify any consequence capable of rectification; and

d) If the malicious code or security vulnerabilities cause a loss of operational efficiency or loss of data, provide all necessary assistance that we request to mitigate the losses and restore the efficiency and/or data as quickly as practicable.

5 Testing

5.1 Before providing any software to us, you must run your own tests using the most recent version of a reputable, commercially available software program to ensure, to the extent possible, that the software:

a) Meets the requirements of the applicable agreement.

b) Does not contain any malicious code or security vulnerabilities.

c) Will pass any acceptance testing conducted under that agreement.

5.2 If you fail to run such tests without limiting our other rights or remedies, you must cooperate fully with us and reimburse all reasonable costs incurred by Top Energy in relation to that failure, including eliminating or reversing any adverse effects of any destructive element.

Section II – policy requirements applicable to third parties with formal attestation or certification

6 Third Parties with Formal Attestation or Certification

6.1 You do not need to comply with section III if you hold any of the following attestation or certification and comply with section II:

a) ISO/IEC 27001:2022 certification.

b) ISO/IEC 27001:2013 certification, provided you are transferring from ISO/IEC 27001:2013 to ISO/IEC 27001:2022.

c) Current SOC2 type 2.

6.2 To satisfy Top Energy's cyber security requirements, the services you provide to Top Energy must be within the scope of the attestation or certification you are relying on, and you must provide us with the following documentation as evidence.

a) ISO/IEC 27001 certification:

i. The current ISO/IEC 27001 certificate that is not older than 12 months

ii. The statement of applicability that is referenced on the certificate

b) SOC2 type 2:

i. The latest SOC2 type 2 report that is not older than 12 months

ii. Evaluate how you have designed and implemented your protective controls as defined in the AICPA trust service criteria

c) We may reasonably request any additional information from you to provide evidence of your implementation of the protective controls referred to in such statement of applicability or SOC2 type 2 report.

6.3 You must:

a) Maintain the formal attestation or certification that you have provided us evidence of in compliance with this section II; and

b) On an annual basis, provide the respective documentation listed in clause 6.3.

6.4 Section III applies if the attestation or certification you have submitted to us pursuant to this section II lapses.

Section III - policy requirements applicable to all third parties who do not comply with section II

7 Security Requirements

7.1 As a supplier of services to Top Energy, you must apply good practice to:

a) Continually assess your cyber risk.

b) Apply effective security controls and formal cyber risk governance processes to protect you and us from cyber threats.

c) Implement appropriate security controls that consider your and our cyber risk and, without limitation, ensure that bypassing a single control or protection does not result in a security incident.

d) Ensure your employees have the appropriate cyber security awareness to fulfil their roles and responsibilities.

e) Use appropriate technologies, processes, and procedures to address current and emerging cyber threats and maintain a consistent baseline of controls to detect, prevent, and respond to them.

f) Apply any learnings from a security incident to improve cyber defences.

7.2 You must use reasonable, appropriate and adequate administrative, technical, procedural and physical safeguards following good practice to detect and prevent unauthorised use of, or access to, the services, Top Energy data and Top Energy systems.

7.3 Without limiting your obligations under clause 7.2, you must apply good practice to:

a) Use and regularly monitor logical access controls with appropriate levels of identification, authorisation, authentication, and traceability to restrict access to the services and Top Energy data to only those individuals who require access to meet your obligations under an agreement and ensure that those controls are updated when individuals change roles or leave.

b) Enforce a password policy that meets or exceeds good practice concerning password management.

c) It prohibits your users who access the services, Top Energy data, and Top Energy systems from using generic user IDs and shared passwords.

d) Implement multi-factor authentication for all remote access and privileged or administrative accounts.

e) Implement appropriate controls to detect and prevent malicious code or other security vulnerabilities on your own systems and ensure that any third-party systems you use to provide the services and communicate with Top Energy data or Top Energy systems do so.

f) Promptly apply security measures and patches designed to address security vulnerabilities following the recommendation of the hardware or software supplier you use to provide services to us.

g) Detect, prevent, and monitor actual or suspected security breaches on any network, infrastructure, or systems you use to provide services to us. Document and regularly test a formal response process for recovering from such events.

h) Ensure that your staff are trained in and understand.

i) Your information security policies, procedures and responsibilities, including those specifically related to providing services to us.

j) The importance of maintaining the confidentiality of Top Energy data.

k) Regularly monitor the security of any network, infrastructure and systems you use to provide services to us and promptly report any events impacting Top Energy, as described in clause 2.

l) Implement secure coding policies, standards and practices and ensure that all employees and contractors you use to provide our coding services follow them. We may require you to provide evidence of the effective implementation of these standards, including the results of any quality assurance, testing and change and release management.

m) Ensure that any remote connection to Top Energy systems is secure and complies with any specific security requirements we notify you of for third-party connections, including when you connect using an interface or specification we provide.

8 Information Security Assurance

8.1 If you generate, collect, process, hold, store or transmit Top Energy data or have access to any Top Energy systems:

a) We may require you to provide a written report summarising the result of any technical security assessment, for example, penetration testing, which is relevant to the services and any risks identified during the security assessment, including:

i. A description of identified vulnerabilities.

ii. Any applicable compensating controls.

iii. The corrective action proposed.

iv. The expected timeframe for you to correct the security vulnerability.

b) You must complete our third-party information security assessment questionnaire and promptly respond to all consequential questions we may have.

8.2 If we consider any report or answers provided in paragraph 5.1 unsatisfactory, we may, acting reasonably and at our cost, carry out ourselves or appoint a third party to conduct an independent security assessment of your security processes. This could include (and is not limited to) vulnerability assessments, penetration testing or controls testing of the services, and the protective controls securing Top Energy data and Top Energy systems under this policy and any agreement. Any such assessment will be subject to appropriate confidentiality obligations. You will provide all assistance and access to personnel and systems that we reasonably request.

8.3 If a security assessment reveals that your processes do not meet the minimum standards required by this policy or reveals significant deficiencies that result in a level of risk in relation to the services that we consider unacceptable (acting reasonably), then you must promptly meet with us to discuss and agree appropriate corrective steps and apply those steps without delay.

9 Policy Implementation

		Competence and interface
Implementation of the policy	**G**	Board of Directors
	A	Chief Executive Officer
	R	General Manager Finance
	R	General Manager Generation
	R	General Manager Network
	R	General Manager Contracting
	R	Chief Information Officer

Legend: **g** - governance; **a** - accountability; **r** - responsibility; **c** - co-operation.

10 References

The following references should be considered in support of this policy:

Ref. Number	Name
D5.3	Information Systems Security Policy
Protocol Policy System	Information Systems Security Standards
Nintex Risks	Information Security Risks Portfolio
D5.2	Data and Information Sharing Policy
E4.2	Procurement of Good and Services

The following procedural arrangements are implemented in support of this policy:

Ref. Number	Name
SS03-08	Vendor Management (Whole Process)
SS06-05-017S	Vendor Information Security Assessment
SSxx-xx	Security Vendor Assessment - Lite
SSxx-xx	Vendor Information Security Compliance Request