Information Security and Data Protection Policy

1.0 Purpose

The purpose of this policy is to set out a framework by which Elemental Infrastructure Holdco Pty Ltd and its related bodies corporate ("Zenith Energy") will:

- protect information and related assets from a range of threats;
- maintain the confidentiality, integrity and availability of Zenith Energy, client, customer and business partner information and resources; and
- minimise business risks and maximise business opportunities related to information.

"Information Security" refers to the processes and methodologies that Zenith Energy has designed and implemented to protect print, electronic, or any other form of confidential, private and sensitive information or data ("information") from unauthorised access, acquisition, modification, misuse, disclosure, disruption or destruction.

This policy applies to information assets owned or leased by Zenith Energy, and to devices that connect to the Zenith Energy network or reside at Zenith Energy sites. This policy applies to all staff, directors, contractors, temporary staff, consultants, and authorised agents of Zenith Energy.

For the purpose of this policy, the term 'end user' includes all groups who have access to Zenith Energy electronic resources.

2.0 Tier 1 Controls

2.1 Governance Requirements

- Cyber security discussions must occur at the executive level regularly. The nature of these discussions should focus on the effectiveness of cyber security protections and additional requirements based on risks faced, security incidents experienced and/or compliance obligations.
- An end-user security policy must be developed and communicated to staff to outline expectations and responsibilities in upholding the security of Zenith Energy's information and IT systems.
- Key third party contracts must include requirements to keep Zenith Energy's information secure.

2.2 Application, device operating system and network controls

- Applications and operating systems in use at Zenith Energy must be updated promptly when vulnerabilities are rated as critical.
- Automatic updates on all applications on devices that connect to the network must be enabled. Where this is not possible, manual update processes must be in place.
- Applications and operating systems that are no longer supported by the vendor must not be used.
- User devices provided by Zenith Energy must have antivirus software installed with appropriate configurations such as scheduled scans and scanning files when these are accessed by users.
- End users must not have permissions to modify the security settings of software (e.g., anti-virus) running on computing equipment (except for approved devices and end-users).
- When end users use their own devices (BYOD), the security requirements of Zenith Energy must be followed.
- Devices that access sensitive information must have only approved software installed.
- A firewall must be deployed at the network level to protect Zenith Energy's network from internet-based threats.
- An email filtering solution must be implemented to reduce spam and malware received via email.

2.3 Restrict administrative or privileged user access

- End users must not maintain administrative privileges over devices that Zenith Energy has supplied for work purposes. While administrative privileges are sometimes required to perform actions on a device, these should only be provided to a very limited number of personnel (1 or 2). If an end user requests access to administrative privileges on a device the following process for providing this access should be used:
- Confirmation of the certain task the end user needs to perform using administrative privileges.
- A complex password must be set on the account, as this account now carries greater risk if it were to be compromised.
- The use of administrative privileges should be time bound and regularly validated. For example, a user should only hold elevated privileges for the time they require them, post that, these should be removed.
- Privileged users at Zenith Energy are also those end users who have access to information considered sensitive (for example, client personal information). User access reviews of IT systems holding sensitive information must be conducted on a regular basis (e.g., monthly, quarterly) to identify user accounts that must be deprovisioned or have access levels adjusted.

2.4 Password management

- Passwords must comply with the following requirements:
  - Minimum length and complexity requirements as determined by Zenith Energy.
  - The use of a passphrase, which is a string of four or more random, unrelated words strung together is recommended. When coupled with complexity requirements, this increases password strength.
  - The use of shared user accounts must be minimised. If shared accounts are used, passwords to these accounts must be shared securely and changed when staff with knowledge of the password leave Zenith Energy.
  - When end users receive passwords to user accounts the passwords must be shared securely.
  - IT systems in use at Zenith Energy, must allow for end users to select their own password or change their password at first login.
  - Default administrative passwords on devices must be changed.
  - When an account compromise has occurred or is suspected, passwords on these end user accounts must be changed.
  - To minimise password incrementation, passwords should be more complex and changed when required. Both examples below are secure passwords:
    - Random characters: Hn8$lp&A
    - Memorable passphrase, with altered characters: No1-CanGuessMe!

2.5 Multi factor authentication

- Multi-Factor authentication (MFA) must be used for IT systems/applications in use at Zenith Energy that are internet-facing and hold sensitive information.

2.6 Awareness and training

- All end users must develop an understanding of the following points:
  - Password usage and management - Creation, frequency of changes, secure storage, multi-factor authentication (MFA).
  - Policy - Implications of non-compliance.
  - Emails - Attachments, links, phishing, spam, email list etiquette.
  - Web usage - Appropriate usage (e.g., work-related internet browsing, file and content sharing via organisation approved platforms).
  - Social engineering - Shoulder surfing, phishing, unusual activity, password resets
  - Incident response - Roles, responsibilities and procedures (who to contact, what to do).
  - Personal use - Use of systems at work and at home.
  - Patching - Regular updates (e.g., timely update of patches when they are released by IT).
  - Access control concepts - Principle of least privilege, privileged access, separation of duties.

- Desktop - Screensavers, locking unattended screens.
- Existing staff must receive appropriate refresher training on an annual or more frequent basis.

2.7 Regular backups

- Regular backups of central information stores that are considered high value (i.e. if lost or unrecoverable for an extended period of time, would impact on the operations of the organisation) must be performed.
- The backup must be stored in a different location to the original data that is backed up.
- Backups must be scheduled according to the availability and integrity requirements of the information that is being backed up. A backup schedule must be documented and maintained for Zenith Energy's critical information systems.
- A simple data recovery test for important IT systems must be performed annually.

2.8 Incident response awareness

- End users at Zenith Energy must be aware of the contact point at Zenith Energy in the event of a security incident.
- Zenith Energy must know who to contact externally to seek assistance, if required.
- For example:
  - IT Support provider
  - The Australian Cyber Security Centre (ACSC) should be contacted to provide advice and assistance.

3.0 Tier 2 Controls

3.1 Identification controls

3.1.1 Information asset management

- Zenith Energy's assets and systems (hardware, software and electronic data/information) must be recorded in an inventory or asset register with explicit asset owner and data ownership identified.
- The asset inventory or register must be regularly updated in accordance with any change that may affect an asset (e.g., addition or decommission of an infrastructure component, break fix involving the replacement of an IT component etc).
- Access to the asset inventory must be limited to authorised staff only.

3.1.2 Information asset classification and handling

- Assets must be classified by assigning an impact level in accordance with the worst - case consequence of loss or disclosure of asset information.
- Information assets must be labelled with one of the following four (4) Classification Levels comprising Zenith Energy's Information Classification Scheme:
  - Public - Information intended for public use where public use and disclosure would not negatively impact Zenith Energy (e.g., Marketing brochures and promotional material, online website content, job advertisements).
  - Internal - Proprietary information intended for internal use or authorised external use where unauthorised disclosure may cause embarrassment or minor damage to Zenith Energy, such as general emails (which are often shared outside the organisation, but not publicly).
  - Confidential - Information subject to a need-to-know basis for certain individuals or groups where unauthorised access may cause major damage to Zenith Energy. For example, limited access within the organisation such as day-to-day emails, organisational performance information, certain customer data (such as name, contact details) etc.
  - Sensitive - Information subject to a need-to-know basis for certain individuals or groups. Access is typically approved by Zenith Energy senior management. Unauthorised disclosure may cause severe financial or reputational damage to Zenith Energy. For example, sensitive information about or belonging to customers or staff (e.g., date of birth, credit card details or client health information).
- Information systems must be reassessed on a periodic basis, or at least annually, and declassified when there is no need to retain the initial classification level.
- In handling information, Zenith Energy staff members must cautiously make decisions and take actions that are commensurate with the classification of the information asset throughout its lifecycle (i.e. creation, access, storage, transmission, retention and destruction).

3.1.3 Information security risk management

- Information security risks are identified, mitigated and monitored through formalised security risk management procedures.
- Information security risk handling must align to Zenith Energy Enterprise Risk Management model following risk analysis, likelihood and consequence classification, and residual risk assessment.
- Exemption requests must be documented, reviewed by IT/Security or other appropriate staff and risk accepted by the accountable manager.
- Compliance with Information security risk management must be assured via internal reviews/auditing and/or external auditing.

3.1.4 Third party management

- Third parties must contractually and operationally commit to meeting Zenith Energy's commercial, security and regulatory compliance obligations. The following requirements must be included in third party agreements:
  - External parties are covered by a confidentiality agreement that explicitly states that persons with access to Zenith Energy's facilities or proprietary information are not to disseminate any information about Zenith Energy, its capabilities or activities without written authorisation.
  - The obligation of the third party to notify Zenith Energy in cases of security incidents which may affect Zenith Energy (e.g., third party virus outbreak, successful third party network compromise etc).
  - The obligation of the third party to maintain confidentiality, integrity and availability of Zenith Energy's information.
- All outsourcing contracts must include an agreement on minimum required security control obligations of the third party (e.g., penetration testing and vulnerability management processes for key IT systems or applications).
- Controls must be in place to ensure the security of remote connections between the parties. The third party must utilise the existing Zenith Energy security infrastructure and take responsibility for the maintenance of the respective security controls that have been established by Zenith Energy.
- The business continuity and disaster recovery arrangements for the resumption of the third party services in case of service interruption or data loss/destruction.

3.2 Protective controls

3.2.1 Identity and access management

A standardised process and procedures for access provisioning and deprovisioning, account management and authentication of users at Zenith Energy must be followed.

- User account ID and password are authenticated as a whole (i.e. at the same time) during the logon process.
- User access reviews should be conducted at least annually to verify that only legitimate, authorised users have access to networks and IT systems, and a process should be established to remediate or remove incorrect or excessive access.
- A process must be established to manage the provisioning and deprovisioning of access across the end user lifecycle.
- User access requests for high risk applications, applications containing sensitive data, administrative level access, or access outside of role scope should be approved by the IT Manager at Zenith Energy, prior to provisioning of access rights.
- A Role Based Access Control (RBAC) framework should be used to determine user access and permissions based on roles, and to establish a predefined set of access rights for users to inherit based on their role.
- User accounts must follow segregation of duties to separate authorisation, approval responsibilities and prevent abuse of unauthorised privileges.

- User accounts must only be used for their approved and intended purpose and for no other reason.
- User accounts must have defined characteristics such as lockout duration for 15 minutes of idle time, inactivity lockout in case of 3 months of inactivity and account lockout threshold if there are 5 consecutive invalid password attempts.
- The use of personal email accounts or non-approved information technology resources for work-related activities must be prevented. If these are to be used, they must be approved by the IT Manager.

3.2.2 Physical Security

Assets must be physically protected to mitigate the following accidental or malicious risks:

- Physical damage.
  - Natural, accidental or malicious causes.
  - Destruction of media, documents, or equipment.
  - Damage that can result in the need to repair or replace a device.
- Theft or unauthorised access.
  - Inappropriate or lack of controls in place to protect physical assets (such as equipment, removable media) and physical access to buildings.
  - Inadequate formal processes for asset and information destruction.
  - That can result in unauthorised disclosure of sensitive information, loss of control over a system or malicious damage to systems and assets.
- All lost keys must be reported immediately to the appropriate team and access revoked immediately.
- Visitor access must be restricted, monitored and escorted.
- Regular (annual) physical asset inventories are reviewed and signed off.
- Visitor access to organisation premises or information processing facilities is formally logged and maintained.
- Keep a record of all asset destructions and destruction certificates.

3.2.3 Remote access and WiFi

- All remote access requests must be securely provisioned through Zenith Energy's standard enterprise remote access solution. Zenith Energy's remote access solutions must inspect the content transmitted via remote connections in accordance with the criticality of the content.
- All remote access to Zenith Energy's information assets must be securely established and managed. User remote access must be authenticated, authorised, terminated, logged, monitored and reviewed periodically.
- Remote user access into the internal Zenith Energy's network requires MFA, at intervals determined by Zenith Energy. The authorised standard site-to-site remote connections are to be as per Zenith Energy's network provider's and must be

authenticated via secure and approved authentication mechanisms (e.g., digital certificates).

- Staff should never connect to any public WiFi networks on their work devices when accessing information of a sensitive nature. Only the Zenith Energy's WiFi network, or the trusted personal mobile data can be used when accessing information of a sensitive nature.
- If working from home, personnel must follow the requirements specified by Zenith Energy in any remote working or information technology policies or procedures.

3.2.4 Configure Microsoft Office macro settings

- Only specific Microsoft Office applications for which there is a demonstrated business requirement for macro use should be allowed to execute approved macros from trusted locations or macros that are digitally signed by trusted publishers. All other Microsoft Office applications should have support for macros disabled

3.3 Detective controls

3.3.1 Security logging

- Security event logs should be collected from Zenith Energy's critical information systems. The type of events recorded must be defined based on the capability of the system producing log data and the classification of information stored within the system.
- Key security - related events, at least successful and unsuccessful logins and changes to the audit policy, must be recorded in logs.
- Security event logs must be protected against unauthorised modification and deletion.
- Where possible, security events must be logged using an industry-standard non-binary format that is human readable. This reduces the possibility of these logs being inaccessible in the future and increases Zenith Energy's capability to integrate, centralise, and correlate information security events.
- Security logs must be retained for at least one (1) year or as specified by Zenith Energy and external regulatory requirements.

3.3.2 Monitoring and review of security event logs

- Logs must be analysed on a regular basis to identify potential unauthorised activities and facilitate appropriate follow-up action.
- Where possible, log monitoring must be automatic and rule-based to immediately alert of a suspected security incident.

- Automated event monitoring and alerting systems must be assessed on a regular basis to ascertain that they have been configured according to their design and are functioning correctly.
- Where no automated mechanism exists to alert on potential security incidents, key security event logs must be checked on a more frequent basis for evidence of actual or potential security incidents.

3.3.3 Threat intelligence

- External threat intelligence can be obtained from a number of organisations, for example ASIO, ASD, AusCERT and global sources from open-source threat intelligence. Intelligence must be considered in the context of Zenith Energy's IT environment and should be used in assessing the adequacy and effectiveness of the security controls in operation and in identifying new information security control requirements.

3.3.4 IDS/IPS (Intrusion Detection and Prevention Software)

- An intrusion detection capability or any other advanced protection mechanisms (e.g., web filtering), if provided by anti-malware software installed on endpoints and servers, or provided by routers or other network devices, must be enabled.

3.3.5 Firewalls

- Zenith Energy must have network edge, and device-based firewalls enabled.
- Network firewalls must be managed by Zenith Energy's IT department or Zenith Energy's contracted IT service provider. Management tasks include appropriate configuration and firewall rule management to provide protection from potential internal and external attacks.

3.3.6 Vulnerability scanning and security testing

- Security testing activities must be conducted on a regular basis to identify vulnerabilities in Zenith Energy's information systems. These include:
  - Vulnerability Assessments – Assess Zenith Energy's information systems for known vulnerabilities. This includes internal and external vulnerability scans.
  - Configuration Reviews – Monitor the configuration of information systems to ascertain that the configuration remains in line with the system's baseline configuration. In addition, the approved Request for Changes (RFCs) and security patches have been applied and are up to date.
  - Penetration Tests – Periodic security reviews to test the effectiveness of the security controls implemented to address identified vulnerabilities. The following criteria must be considered when establishing the need for a penetration test:
    - Regulatory requirements.

- Type of system (e.g., Internet or internal facing).
- Scope of penetration test.
- Contractual agreement (if an external service provider performs the penetration test).

3.4 Response and Recovery Controls

3.4.1 Incident response planning

- An Incident Response ("IR") plan must be developed by Zenith Energy to allow for quick and effective handling to minimise damage.

3.4.2 Disaster recovery planning

- A Disaster Recovery Plan ("DRP") must be developed by Zenith Energy to document the recovery processes and procedures that must be adhered to in the event of a disruption or a disaster relating to critical applications and systems.

3.4.3 Business continuity planning

- A Business Continuity Plan ("BCP") must be developed by Zenith Energy to minimise loss through operational downtime

3.4.4 Cyber insurance

- Zenith Energy must assess insurance options on an annual basis for appropriateness of cyber insurance cover that may be required based upon organisational requirements.

This Policy will be reviewed regularly and updated as required.

Signature: Date:

Hamish Moffat
Managing Director and CEO