CYBER SECURITY POLICY

AS AT SEPTEMBER 2023

1. INTRODUCTION

a) Commitment

The Board has adopted this Cyber Security Policy (Policy) to safeguard the digital assets of Bannerman Energy Ltd ("**Bannerman**" or "**the Company**").

b) Scope

The policy covers all IT systems, networks, digital communications, and data stored digitally or physically at our sites.

c) Purpose of this Policy

The purpose of this Policy is to :

i) protect company information from unauthorised access, disclosure, alteration, destruction, or theft;

ii) ensure business continuity and minimise business damage;

iii) comply with regulatory requirements and international cyber security standards.

d) Who is covered by this Policy?

This Policy applies to the Company's current or former, Directors and employees, the Company's contractors (including subcontractors) and employees of the Company's contractors, joint venture partners (who have agreed to be bound by the Policy) and suppliers (each a **Company Person**).

This policy is available to officers and employees of the Company at www.bmnenergy.com and can also be obtained from an Authorised Officer.

2. POLICY ELEMENTS

a) User Access Control

i) Implement strict access controls with different levels of permissions.

ii) Regularly review and update access rights.

b) Data Protection and Privacy

i) Encrypt sensitive data both in transit and at rest.

ii) Adhere to local and international data protection laws.

c) Network Security

i) Use firewalls, intrusion detection systems, and anti-virus software.

ii) Regularly update and patch network systems.

d) Incident Response and Management

i) Establish an incident response team.

ii) Regularly conduct drills and training for incident response.

e) Employee Training and Awareness

i) Conduct regular cyber security awareness programs.

ii) Include cyber security in employee induction programs.

f) Physical Security

i) Secure physical access to IT infrastructure.

ii) Implement surveillance and access logs at critical sites.

g) Compliance and Legal Requirements

i) Comply with Australian Cyber Security regulations.

ii) Adhere to international standards and regulations relevant to our global offices.

h) Remote Work and Mobile Device Management

i) Secure and monitor remote connections.

ii) Implement policies for BYOD (Bring Your Own Device) and company-issued devices.

i) AI-Enhanced Security Measures

i) **AI-Driven Threat Detection**: Deploy AI-based systems to continuously monitor and analyse network traffic and user behaviour for unusual or malicious activity signs.

ii) **Automated Incident Response**: Utilise AI algorithms to respond to detected threats automatically, reducing the time between threat detection and response.

iii) **Predictive Analytics**: Implement AI tools for predictive analytics to anticipate potential vulnerabilities and attacks by analysing trends and patterns.

iv) **AI for Identity Verification**: Use AI-powered identity verification tools for enhanced access control, ensuring that only authorised personnel access sensitive systems and data.

j) Vendor and Third-Party Management

i) Ensure third-party vendors comply with our cyber security standards.

ii) Conduct regular audits of third-party access and services.

k) Cloud Security

i) Implement security measures for cloud-hosted data and applications.
ii) Develop strategies for securing multi-cloud and hybrid cloud environments.

l) Cybersecurity Risk Assessment

i) Conduct regular risk assessments to identify and mitigate cyber threats.
ii) Update security strategies based on risk assessment outcomes.

m) End-Point Security

i) Secure end-point devices with regular updates and patches.
ii) Enforce endpoint protection policies.

n) Disaster Recovery and Business Continuity Planning

i) Maintain a disaster recovery plan for business continuity.
ii) Regularly test and update the disaster recovery plan.

o) Supply Chain Security

i) Secure the supply chain against cyber threats.
ii) Assess and manage risks from suppliers and partners.

p) Multi-Factor Authentication (MFA)

i) Implement MFA for accessing sensitive systems and data.

q) Information Security Management System (ISMS)

i) Establish and maintain an ISMS in accordance with ISO/IEC 27001 standards.
ii) Continuously monitor and improve the ISMS.

r) Security for Emerging Technologies

i) Include security measures for emerging technologies like IoT devices.
ii) Securely integrate new technologies into the IT environment.

s) Whistleblower Protection

i) Provide protections for employees reporting vulnerabilities or breaches.
ii) Ensure confidentiality and protect against retaliation.

t) Social Media Security

i) Develop guidelines for the secure use of social media.
ii) Train employees on social engineering threats via social media.

u) Legal and Regulatory Updates

i) Stay updated on new cyber security laws and regulations.

ii) Regularly revise the policy to comply with legal changes.

3. RESPONSIBILITIES OF PERSONS USING COMPANY ASSETS

i) **Individual Accountability**: All employees and contractors are personally responsible for securely using Bannerman Energy Ltd's digital and physical assets.

ii) **Proper Usage**: Company assets, including computers, mobile devices, and network resources, must be used solely for business purposes and in accordance with company policies.

iii) **Securing Devices**: Users must ensure that all devices are secured with strong passwords and that these passwords are kept confidential.

iv) **Reporting Security Incidents**: Any suspected or actual security incidents or threats involving company assets must be immediately reported to the IT security team.

v) **Software and Application Management**: Only authorised software may be installed on company devices. Unauthorised software installation is strictly prohibited.

vi) **Data Handling**: Sensitive data must be handled in accordance with data protection policies, ensuring its confidentiality and integrity.

vii) **Remote Work Security**: Employees must follow the guidelines for securing their internet connection and safeguarding company data against unauthorised access.

4. REPORTING SECURITY INCIDENTS AND POTENTIAL THREATS

i) If a Company Person suspects or identifies a potential cybersecurity threat to the Company or its assets, or a suspected or actual security incident involving company assets occurs, this must be immediately reported to the IT Security Team.

ii) The Company Person should escalate the report to the Company Secretary / Authorised Officer (refer to pg. 7) if a satisfactory response is not received and/or the Company Person has reason to suspect an actual or perceived threat remains.

5. POLICY ENFORCEMENT

i) Violating this policy will result in disciplinary action, which may include termination of employment.

6. POLICY REVIEW AND UPDATE

ii) This policy will be reviewed annually or as required by changes in technology or business practices.

7. GLOSSARY

1. **Access Control**: Methods and protocols used to restrict access to sensitive data and systems, ensuring that only authorised individuals can view or manipulate them.

2. **AI (Artificial Intelligence)**: A branch of computer science dealing with creating machines or software capable of performing tasks that typically require human intelligence. In cybersecurity, AI involves using advanced algorithms and machine learning techniques to detect, analyse, and respond to cyber threats more efficiently, often in real-time. This includes predictive analytics, automated incident response, and AI-driven threat detection and identity verification.

3. **Anti-Virus Software**: Software designed to detect, prevent, and take action to disarm or remove malicious software programs, such as viruses and worms.

4. **BYOD (Bring Your Own Device)**: A policy that allows employees to use their personal devices, such as smartphones or laptops, for work-related activities.

5. **Cloud Security**: Security measures and protocols are used to protect data and applications hosted in cloud environments, including multi-cloud and hybrid cloud setups.

6. **Company Person**: Refers to individuals who are either directly employed by, or are working in association with, Bannerman Energy Ltd. This includes current and former Directors and employees, contractors and their employees, joint venture partners (who have agreed to be bound by the policy), and suppliers. A Company Person is subject to the guidelines and responsibilities outlined in the Cyber Security Policy and is expected to adhere to its terms to ensure the security and integrity of the company's digital and physical assets.

7. **Compliance**: Adherence to laws, regulations, guidelines, and specifications relevant to the business.

8. **Cybersecurity Risk Assessment**: The process of identifying, analysing, and evaluating cybersecurity risks, followed by implementing strategies to manage and mitigate those risks.

9. **Data Encryption**: The process of converting data into a code to prevent unauthorised access. It includes data at rest (stored data) and in transit (data being transferred).

10. **Data Protection Laws**: Legal frameworks established to govern the handling of personal data to protect the privacy of individuals.

11. **Disaster Recovery Plan**: A documented, structured approach with instructions for responding to unplanned incidents to restore systems and data after a cyber-attack or other disruption.

12. **End-Point Security**: Security measures focused on protecting end-point devices like computers, smartphones, and tablets from cyber threats, including managing software updates and security patches.

13. **Firewall**: A network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules.

14. **Incident Response**: A plan or process activated in response to a cyber security breach or attack.

15. **Information Security Management System (ISMS)**: A systematic approach to managing sensitive company information, ensuring it remains secure, often implemented following international standards such as ISO/IEC 27001.

16. **Internet**: A global network connecting millions of private, public, academic, business, and government networks of local to global scope, linked by a broad array of electronic, wireless, and

optical networking technologies. It facilitates the exchange of information and data, including email, video, and other forms of communication.

17. **Internet of Things (IoT)**: The network of physical objects—devices, vehicles, buildings, and other items—embedded with electronics, software, sensors, and network connectivity that enables these objects to collect and exchange data.

18. **Intrusion Detection System (IDS)**: A software application or device that monitors a network or systems for malicious activity or policy violations.

19. **IT Infrastructure**: The physical and virtual components, such as hardware, software, networks, and facilities, that are required to operate and manage the IT environment of an organisation.

20. **Legal and Regulatory Updates**: The process of regularly updating company policies and procedures to comply with new and changing legal and regulatory requirements related to cybersecurity.

21. **Multi-Factor Authentication (MFA)**: A security system that requires multiple authentication methods from independent categories of credentials to verify the user's identity for a login or other transaction.

22. **Network Security**: Measures taken to protect the integrity, confidentiality, and accessibility of computer networks and data.

23. **Patch Management**: The process of managing patches or updates for software and technologies, including the acquisition, testing, and installation of patches to correct vulnerabilities and improve usability or performance.

24. **Physical Security**: Security measures that are designed to deny unauthorised access to facilities, equipment, and resources and to protect personnel and property from damage or harm.

25. **Remote Work**: Working from a location outside the conventional office environment, often from home or a location with internet connectivity.

26. **Social Media Security**: Security measures and guidelines related to the use of social media platforms to prevent leakage of sensitive information and protect against social engineering attacks.

27. **Supply Chain Security**: Security practices aimed at protecting the supply chain from cyber threats, including risk assessments and management of cybersecurity risks posed by suppliers and partners.

28. **Surveillance and Access Logs**: Tools and records used to monitor and record activity in a physical or virtual environment, often for security purposes.

29. **Third-Party Vendor**: An external organization that provides services or products to an enterprise but is not part of that organization.

30. **User Access Permissions**: The rights or privileges assigned to an individual user, group, or role that define what actions they can perform and what resources they can access within a system or network.

31. **VPN (Virtual Private Network)**: A technology that creates a safe and encrypted connection over a less secure network, such as the internet, to provide remote access to an organization's

Schedule 1- Authorised Officers

Name	Position	Contact Details
Ronnie Beevor	Chairman	rhbeevor@gmail.com +61 8 9381 1436
Steve Herlihy	Company Secretary	sherlihy@bmnenergy.com +61 8 9381 1436