

Benoil Services Limited

Cyber Security Policy

1. INTRODUCTION

- 1.1 Benoil Services Limited ("the Company") is committed to protecting our information systems, data, and digital assets from cyber threats. This Cyber Security Policy outlines our approach to managing and mitigating cyber security risks to the Company.
- 1.2 This policy applies to all employees, directors, contractors, and third parties who access the Company's information systems, networks, and data. Adherence to this policy is essential to maintain the security and integrity of our digital infrastructure.
- 1.3 This policy is designed to safeguard our business operations, protect sensitive information, and ensure compliance with relevant legal and regulatory requirements.

2. CYBER SECURITY PRINCIPLES

- 2.1 All employees must:
 - a) Protect confidential and sensitive information from unauthorized access, disclosure, or theft,
 - b) Ensure that data and systems remain accurate, complete, and trustworthy, protecting against unauthorized modification,
 - c) Maintain reliable access to information systems and data for authorized users when needed, and
 - d) Comply with applicable laws, regulations, and industry standards relating to data protection and cyber security.

3. ACCEPTABLE USE OF IT SYSTEMS

- 3.1 Company IT systems, including computers, networks, email, and mobile devices, must only be used for legitimate business purposes.
- 3.2 Employees must not:
 - a) Access, download, or distribute illegal, offensive, or inappropriate content
 - b) Use Company systems for personal commercial gain
 - c) Attempt to bypass security controls or access unauthorized systems, or
 - d) Install unauthorized software or applications.
- 3.3 Limited personal use of Company IT systems is permitted provided it does not interfere with work responsibilities or violate this policy.

4. PASSWORD AND AUTHENTICATION

- 4.1 All employees must:
 - a) Create strong, unique passwords containing a minimum of 8 characters with a mix

Benoil Services Limited

Cyber Security Policy

of uppercase, lowercase, numbers, and special characters

- b) Change passwords regularly
 - c) Never share passwords with colleagues or third parties
 - d) Use different passwords for different systems
- 4.2 Where available, employees must enable multi-factor authentication for accessing Company systems and applications, particularly if they are required to access Company IT systems remotely.
- 4.3 Employees should lock computers and devices when unattended, and logout of systems and applications when not in use.
- 4.4 Employees must report any suspicious account activity immediately to the Managing Director, or Finance Director.

5. EMAIL AND COMMUNICATION SECURITY

- 5.1 Employees must
- a) Exercise caution when opening emails from unknown senders,
 - b) Avoid clicking on suspicious links or download unexpected attachments,
 - c) Verify the authenticity of requests for sensitive information or financial transactions by speaking with the counterparty by telephone or otherwise verifying the integrity of the request.
- 5.2 Employees must be vigilant against phishing attempts and report any suspicious emails to the Managing Director, or the Finance Director immediately.

6. DATA PROTECTION AND MANAGEMENT

- 6.1 All Company data must be stored on approved Company IT systems and regularly backed up. Documents containing sensitive information must be disposed of securely through shredding, secure deletion, or approved disposal methods.

7. MOBILE DEVICES AND REMOTE WORKING

- 7.1 All mobile devices containing Company data should be secured with passwords, PINs, or biometric authentication.
- 7.2 The Managing Director or Finance Director should immediately be informed of any lost or stolen Company device.
- 7.3 When working remotely, employees must:
- a) Use secure, password-protected Wi-Fi networks
 - b) Avoid using public Wi-Fi for accessing sensitive Company information

Benoil Services Limited

Cyber Security Policy

- c) Use Company-approved VPN services when accessing Company systems remotely

8. TRAINING AND AWARENESS

- 8.1 The Company will provide cyber security awareness training to all employees as and when appropriate to help mitigate cyber threats and risks.

9. COMPLIANCE

- 9.1 All employees are responsible for understanding and complying with this Cyber Security Policy. The Company reserves the right to monitor the use of its IT systems to ensure compliance with this policy and to detect security threats.

10. REVIEW AND UPDATES

- 10.1 This policy is part of our suite of Ethical Business Practices policies and has been approved by the Board. This policy will be reviewed annually to ensure its effectiveness and compliance with current cyber security threats and regulatory requirements.
- 10.2 The Company is committed to continuously improving our cyber security practices and adapting to emerging threats and technologies.

11. CONCLUSION

- 11.1 Benoil Services Limited is dedicated to maintaining robust cyber security practices to protect our business, employees, clients, and stakeholders. By adhering to this Cyber Security Policy, we can minimize risks and ensure a secure digital environment.

12. APPROVAL

This policy has been approved & authorised by:

Name: Matt Anstead
Position: Managing Director
Date: 5th February 2025
Signature:

A handwritten signature in dark ink, appearing to read 'MA Anstead', is written over the signature line.