Information Technology (IT) Policy

Information Technology (IT) Policy

1. Introduction

This Information Technology (IT) Policy sets out the guidelines and best practices for the use of information technology resources at Concept Commissioning, located in Victoria, Australia. These policies are designed to ensure the security, efficiency, and ethical use of IT resources by employees, contractors, and any other parties with access to our IT systems.

2. Acceptable Use of IT Resources

2.1. Authorised Users: IT resources, including computers, networks, software, and data, should only be used by authorised employees or contractors. Unauthorised access is prohibited.

2.2. Data Security: All users must take responsibility for the security and confidentiality of data. Personal data, customer data, and company information should be protected from unauthorised access or disclosure.

2.3. Software Usage: Only licensed and approved software should be installed on company equipment. Unauthorised software is prohibited.

2.4. Email and Internet Usage: Email and internet access should be used for business purposes. Personal use should be limited and not interfere with work responsibilities.

2.5. Malware Protection: All devices connected to the company network must have up-to-date anti-malware software.

2.6. Password Security: Strong and unique passwords are required for all accounts. Passwords should be changed regularly, and they should not be shared.

3. Equipment and Data Handling

3.1. Equipment Care: All IT equipment should be used and maintained according to manufacturer recommendations. Any issues should be reported to the IT department.

3.2. Data Backup: Data should be regularly backed up and stored securely.

3.3. Data Retention: Data should be retained and disposed of in compliance with legal requirements.

4. Privacy and Confidentiality

4.1. Data Privacy: All users must respect the privacy of individuals and comply with relevant data protection laws.

4.2. Confidentiality: Confidential company information should not be shared with unauthorised individuals. Employees must sign a confidentiality agreement.

5. Reporting Security Incidents

Any security incidents or breaches should be reported immediately to the IT department. This includes lost or stolen equipment, data breaches, or suspected malware infections.

6. Compliance with Laws and Regulations

Users are expected to comply with all relevant laws, regulations, and industry standards applicable in Victoria, Australia, and internationally.

7. Consequences of Policy Violation

Violations of this IT policy may result in disciplinary actions, including but not limited to warnings, suspension, or termination of employment or contract.

8. Review and Updates

This IT policy will be reviewed annually and updated as necessary. Employees and contractors will be informed of any changes to the policy.

9. Contact Information

For questions, concerns, or reporting incidents related to this IT policy, please contact us at info@conceptcommissioning.com.au.

Ian Quaye | CPEng | MIEAust | NER | RPEQ | GSAP

Managing Director | Concept Commissioning

2023