INTERNET, EMAIL, COMPUTER & SOCIAL MEDIA POLICY

This Internet, Email, Computer and Social Media Policy applies to Miriklis Earthmoving Pty Ltd t/as XPower (ABN 31 106 521 304).

This policy applies to all XPower employees who use XPower's computer network by any means. The policy also applies to employees who contribute to external blogs and sites who identify themselves as associated with XPower.

This Policy explains in general terms how we respect XPower, employees, customers, competitors and the general public when using Internet, email, computers and social media. This policy sets out the standards of behaviour expected of employees using XPower's computer network (internet, email, online 'cloud' based software programs, and computer facilities), or when making reference to XPower on external sites, inside and outside working hours, in the workplace or at any other place whilst performing work for XPower. It includes, but is not limited to, desktop computers, laptop computers, iPhones, smart phones, smart watches and similar products.

WHAT IS THE WORKPLACE?

USE OF INTERNET, EMAIL AND COMPUTERS

Where use is allowed, employees are entitled to use the computer network only for legitimate business purposes. Employees are permitted to use XPower's computer network for limited and reasonable personal use. However, such personal use must not impact upon the employees work performance, other employees, or violate this policy or any other policy.

An employee must not use XPower's computer network for personal use if that use interferes with the efficient business operations of XPower or relates to a personal business of the employee. XPower gives no warranty or assurance about confidentiality or privacy of any personal information disclosed by any employee in the course of using XPower's computer network for his/her personal purposes.

SOCIAL MEDIA

Blogging and participation in social media has become one of the most popular means of communicating on the Internet. Recognising this phenomenon, XPower has implemented a policy that addresses the type of information employees are permitted to share on their personal blogs, on others' blogs, and in other online social media interactions.

What is Social Media?
Social media are primarily Internet and mobile-based tools for sharing and discussing information. The term is most often referred to as activities that integrate technology, telecommunications and social interaction, and the construction of words, pictures, videos and audio. Examples of social media applications are Google Groups, Facebook, YouTube, Twitter and Flickr.

What is Blogging?
A 'blog' refers to an Internet online personal journal established and frequently updated by an individual. Blogs are generally accessible to anyone with Internet access. A blog is fully searchable through Google or any other search engine, and other blogs can link to it, thereby carrying the blogger's message to millions of viewers. The nature of blogging encourages a freewheeling discussion of topics, the direction of which is often beyond a blogger's control. The millions of potential viewers of blogs may include an organisation's existing and potential customers, law enforcement personnel and employees.

Why Do We Need a Policy?
Social media can have a tremendous impact on a company's public and internal profile. Statements made in such unwieldy public forums can have serious legal, public relations and, ultimately, financial consequences, both for employees who participate in social media and for XPower.

Cyber Security - Data Breach
Any employee who suspects that a theft, breach or exposure of XPower's protected data or XPower's sensitive data has occurred must immediately provide a description of what occurred via email to libbi@xpower.com.au or by calling Libbi 0400 178 480.
This includes, but is not limited to, unauthorised access to XPower Server, sharing of information not intended for the recipient, suspicious emails and/or any of the prohibited conduct as listed on page 3.

Cyber Security Guide
- Refer to information available at the Australian Cyber Security Centre (ACSC) website www.cyber.gov.au
- Protect against Malware (malicious software)
    - Automatically update your operating system (Apple iOS & MacOS, Microsoft, Google Android OS etc.)
    - Automatically update your software applications (Google Chrome, Microsoft Word, Firefox etc.)
    - Backup data
- Scams (Phishing) – These are emails, SMS, social media etc., sent from individuals or organisations you 'think' you know. They mimic phrasing, branding, and logos to appear 'real' before conning you to click on a link or attachment, be aware of clicking on/opening these. Do not disclose or confirm personal information such as passwords, credit card or bank account details or changes, be cautious of requests for money and of requests to check or confirm login details.
- Use Multi-factor Authentication security if available
- Use Passphrases as passwords, a longer, more complex and easier to remember phrase. E.g., I like 0 pineapple on my pizza!
- Report recognised cyber security threats to the work group and interested parties if required

Basic Guidelines
XPower discourages all discussion of XPower business, employees and customers in employee blogs and other social media outlets.
General principles to follow: -

- Use common sense. Employees should refrain from posting items that could reflect negatively on XPower or otherwise embarrass XPower, including comments or other posts about drug or alcohol abuse, profanity, rude or sexual humour, and other inappropriate conduct. Don't use ethnic slurs, personal insults, obscenity, or engage in any conduct that would not otherwise be acceptable in XPower's workplace
- If an employee has identified themself as an XPower employee, either indirectly or directly as part of a user profile, they need to ensure their profile and related content is consistent with XPower policies and procedures
- All XPower policies and procedures will apply to all posts that may relate to and/or affect XPower
- Show proper respect for people's privacy and for topics that may be considered objectionable or inflammatory, like politics and religion
- Respect the law, including those laws governing defamation, discrimination, harassment, and copyright and fair use
- Do not reference XPower employees, customers etc. without their approval
- Assume that all topics discussed with XPower, employees and customers are confidential
- Make sure that your online activities do not interfere with your work commitments or job performance

Prohibited Conduct: -
The following violations will not be tolerated and may result in termination:

- Employees must not send (or cause to be sent), upload, download, use, retrieve, or access any email on XPower's network that is obscene, offensive, inappropriate, illegal, or unlawful. This includes text, images, sound or any other material, sent either in an email, text message, or any other electronic form or in an attachment to an email, or through a link to a site (URL) e.g. material of a sexual nature, indecent or pornographic material
- Disclosing XPower 'secrets'; confidential, classified or commercial-in-confidence information concerning the company
- Disclosing confidential information, which may include, but is not limited to XPower pricing information, customer contractual arrangements, financial information and data etc.
- Using XPower's computer network in a manner contrary to XPower's Privacy Policy
- Engaging in harmful conduct, such as workplace gossip, posting racially or sexually offensive language or graphics and belittling co-employees and customers
- Install software or run unknown or unapproved programs on XPower's computer network
- Send or cause to be sent chain or SPAM emails in any format
- Bringing the XPower brand or reputation into disrepute
- Breaching copyright and intellectual property conditions when using material
- Writing about a customer without their permission (including posting of client photos)
- Distributing third-party intellectual property without prior authorisation
- Disclosure of other companies' secrets

Employees must not use another employee's computer (including passwords and usernames/login codes) for any reason without the express permission of the employee or XPower.

XPower may use and disclose computer surveillance records (storage volumes, internet sites, volume downloads, suspected malicious code or viruses, emails (received, sent, deleted and stored) and computer hard drives) where that use or disclosure is:

- For a purpose related to the employment of any employee or related to XPower's business activities
- To a law enforcement agency in connection with an offence
- In connection with legal proceedings
- Deemed to be necessary to avert an imminent threat of serious violence to any person or substantial damage to property
- Illegal activity, including but not limited to, circumstance of assault, suspected assault, theft or suspected theft of XPower's property or damage to XPower's equipment or facilities

Trust is an essential ingredient in the positive and productive culture we are striving to achieve at XPower. We can't be there to guide every interaction, so we expect employees to follow these guidelines, advice and adopt the simple practice of stepping back, re-reading and thinking about what they are about to do before doing it.

Signed:_____
Director

Date: 27.04.23