POLICY NO. CCPL-IMS-P-09

PRIVACY, CONFIDENTIALITY & INFORMATION TECHNOLOGY USER POLICY

Commplete recognises that the business has a moral and legal responsibility as well as a responsibility to its customers to keep personal information private, as well as our own, and our customers commercially sensitive information secure.

Commplete is required to collect personal information from employees, customers, suppliers, sub-contractors and consultants. The main purpose for collecting this information is to enable the alliance to effectively and efficiently conduct its business. Commplete is committed to adhering to the National Privacy Principles specified in the Privacy Act 1988 (Commonwealth) and shall respect personal privacy and sensitive information accordingly.

Commplete guarantees implementation and ongoing review of the below strategies as the basis of its privacy, confidentiality and information technology user policy;

- Identify and control risk and hazards associated with privacy and confidentiality within our business activities and implement risk management strategies to eliminate the potential for incident using the hierarchy of controls.
- Ensure compliance with privacy legislation during the undertaking of our operations.
- Ensure that personal information collected will be limited to that necessary for Commplete to effectively carry out its business activities.
- Collect information in a fair and lawful way and directly from the individual concerned where it is reasonable and practicable to do so.
- Take reasonable steps to ensure that all information it collects or uses is accurate, complete, up to date and stored in a secure environment and is only accessible by authorised personnel for permitted purposes.
- Provide suitable resources, training and supervision for employees and contractors to adhere to this policy.
- Pursue a culture where commercial and private correspondence is not left unattended and is secured when not in use.
- Ensure all Commplete owned IT equipment is maintained to the highest standard at all times with active virus protection.
- Provide a contact for any person wishing to:
    - Access or modify personal information which Commplete holds about them,

or make any complaint in relation to a breach of privacy.
    - Change the security access status of employees and contractors to read commercial and sensitive information.

Commplete uses various forms of information technology in order to carry out business activities effectively. It is essential to stay up to date with current market technologies and to keep connected with our field teams.

Both company and personal devices are used, including but not limited to; mobile phones, tablets, laptops, USB Flash drives, websites and applications. The systems used on these devices include but are not limited to; Telephone systems, email systems, WhatsApp, Google drive, Google photos and Skytrust.

Staff Responsibilities

- Ensure all devices used for Commplete information systems, personal or Commplete owned, are protected from unauthorised access by a password.
- Ensurse on company owned devices that anti-virus is active at all times, and do not open suspicious email.
- Ensure any misuse of the company's IT devices or systems are reported to management.
- In the event that a device containing company data is lost or stolen, this must be reported to Commplete management immediately.
- In the event that you upgrade a personal device containing company data, ensure that all data is deleted from the device. Management can assist.
- Do not send, encourage the receipt of, knowingly download, display, print or otherwise disseminate material that is sexually explicit, profane, obscene, harassing, fraudulent, racially offensive, defamatory or otherwise unlawful;
- Do not share company information or data including construction related photos with 3rd parties or on social media platforms unless prior written authorisation is obtained from management.
- Do not use or copy software in violation of license agreements or copyright;
- Do not use Company IT systems to interfere with the duties and functions of other persons or organisations.
- Do not load software on Company provided devices without prior written approval from Management.
- Do not use unauthorised codes or passwords and/or other unauthorised access to information.
- Do not share user profiles and passwords, except as authorised by the Network Administrator or as requested by Commplete Management.

Monitoring/Investigation

Commplete management reserves the right, for business and legal compliance purposes, to enter, search, and/or monitor the usage of Company provided communication and IT devices without advance notice and consistent with applicable state, federal and international legislation.

Abnormal usage may be investigated.

Company passwords and access codes must be made available to Commplete management upon request.

Disciplinary Action

Violation of this policy may result in the following disciplinary action including; Being placed on a warning, being instantly dismissed, or being made subject to Civil or Criminal Court action.

Director
Chris Mitchell

Director
Brenden Lavin