CYBER SECURITY POLICY

This cyber security policy is for our employees, suppliers, and customers to refer to when they need advice and guidelines related to cyber law and cybercrime. Having this cyber security policy, we are trying to protect Blackwood Plant Hire Ltd.'s (BPH) data and technology infrastructure.

This policy applies to all of BPH employees, suppliers, and anyone else who may have any type of access to BPH systems, software and hardware.

Examples of Confidential Data

Some of the common examples of confidential data include:

- Classified financial information.
- Customer data.
- Data about suppliers.
- Technology and technical data.

Device Security- Using personal devices.

Logging in to any of company's accounts from personal devices such as mobile phones, tablets or laptops, can put our company's data at risk. BPH prohibits accessing any restricted company's data from personal devices unless authorised by BPH Managing Director. If authorised, staff are obligated to keep their devices in a safe place, not exposed to anyone else.

All employees must follow best practices as below:

- Keep all electronic devices' password secured and protected .
- Logging into company's accounts should be done only through safe networks.
- Install security updates on a regular basis.
- Upgrade antivirus software on a regular basis.
- Do not leave your devices unprotected and exposed.
- Lock your computers when leaving the desk.

Email Security

Emails can carry scams or malevolent software. In order to avoid virus infection or data theft, all employees must:

- Abstain from opening attachments or clicking any links in the situations when its content is not well explained.
- Make sure to always check email addresses and names of senders.
- Search for inconsistencies
- Be careful with clickbait titles (for example offering prizes, advice, etc.)

In case that an employee is not sure if the email received, or any type of data is safe, they can always contact our IT specialist.

Managing Passwords

To ensure avoiding that your company account password gets hacked, use these best practices for setting up passwords:

- At least 8 characters (must contain capital and lower-case letters, numbers and symbols)
- Do not write down password and leave it unprotected
- Do not exchange credentials when not requested or approved by supervisor
- Change passwords every [x] month

Transferring Data

Data transfer is one of the most common ways cybercrimes happen. Follow these best practices when transferring data:

- Avoid transferring personal data such as customer and employee confidential data
- Adhere to personal data protection law
- Data can only be shared over company's network

Working Remotely

Even when working remotely, all the cybersecurity policies and procedures must be followed.

Disciplinary Action

When best practices and company's policy are not followed, disciplinary actions may take place.

Some of the examples of disciplinary actions include:

- In case of breaches that are intentional or repeated, and are harmful to the Company, or its clients. BPH will take serious action which could result in termination of employment.
- Depending on how serious the breach is, verbal/formal written warnings will be issued in line with current HR policies.
- Each case and incidence will be assessed on a case-by-case basis.

Signed:

Paul McCormack
Managing Director

Dated: 01 March 2022