Cyber Security Policy

OBJECTIVE

The objective of this policy is to ensure that all employees are aware of their responsibilities in relation to Cyber Security in preserving the security of our data and technology infrastructure.

SCOPE

As the Group continues to incorporate technology into its day-to-day operations, the more data we collect, store, and manage, the larger the risk of personal and business data being a target for potential security breaches. Human errors, hacker attacks and system malfunctions that could cause great financial damage and may threaten our company's reputation.

For this reason, we have implemented several security measures. We have also prepared instructions that may help mitigate security risks. We have outlined both provisions in this policy.

POLICY RESOURCES & CONRIBUTORS

Australian Cyber Security Centre	https://www.cyber.gov.au/ Cyber Security Guide
Cessnock Hospitality Group	Cyber Security Procedures Data Breach Reporting Procedure Data Breach Recovery Plan
IT Team	John Harwood (General Manager CHG) Diamond IT (IT Provider) 02 4944 2444 support@diamondit.com.au

POLICY

Confidential data

Confidential data is secret and valuable. Common examples are:

- Unpublished financial information
- Data of Members, Employee or Third-Party Suppliers

All employees are obliged to protect this data. In this policy, we will give our employees instructions on how to avoid data/security breaches.

Protect personal and company devices

When employees use their digital devices to access company emails or accounts, they introduce security risk to our data. We advise our employees to keep both their personal and company-issued computer, tablet and cell phone secure. They can do this if they:

- Keep all devices password protected and where possible use 2 form Authentication
- Choose and keep updated a complete antivirus software.
- Ensure they do not leave their devices exposed or unattended.
- Install security updates of browsers and systems monthly or as soon as updates are available.
- Log into company accounts and systems through secure and private networks only.

We also advise our employees to avoid accessing internal systems and accounts from other people's devices or lending their own devices to others.

Keep emails safe

Emails often host scams and malicious software known as "Phishing", to avoid virus infection or data theft, we instruct employees to:

- Avoid opening attachments and clicking on links when the content is not adequately explained.
- Be suspicious of clickbait (Phishing) titles (e.g. offering prizes, advice.)
- Check email and names of people they received a message from to ensure they are legitimate.
- Look for inconsistencies or give-aways (e.g. grammar mistakes, capital letters, excessive number of exclamation marks.)

If an employee is not sure that an email, they received is safe, they can refer to our IT Provider

Manage passwords properly
Password leaks are dangerous since they can compromise our entire infrastructure. Not only should passwords be secure so they will not be easily hacked, but they should also remain secret. For this reason, we advise our employees to:

- Choose passwords with at least eight characters (including capital and lower-case letters, numbers, and symbols) and avoid information that can be easily guessed (e.g. birthdays.)
- Exchange credentials only when necessary. When exchanging them in-person is not possible, employees should prefer the phone instead of email, and only if they personally recognise the person they are talking to.
- Change their passwords every three months.

Transfer data securely
Transferring data introduces security risk. Employees must:

- Avoid transferring sensitive data (e.g. member information, employee records) to other devices or accounts unless necessary. When mass transfer of such data is needed, we request employees to request permission from the CEO
- Share confidential data over the company network/system and not over public Wi-Fi or private connection.
- Ensure that the recipients of the data are properly authorised people or organisations and have adequate security policies.
- Report scams, privacy breaches and hacking attempts

Our IT Team need to know about scams, breaches, and malware so they can better protect our infrastructure. For this reason, we advise our employees to report perceived attacks, suspicious emails or phishing attempts as soon as possible to our specialists. Our IT Team will investigate promptly, resolve the issue, and send a companywide alert when necessary.

Our IT Team are responsible for advising employees on how to detect scam emails. We encourage our employees to reach out to them with any questions or concerns.

Additional measures
To reduce the likelihood of security breaches, we also instruct our employees to:

- Turn off their screens and lock their devices when leaving their desks.
- Report stolen or damaged equipment as soon as possible to IT Team.
- Change all account passwords at once when a device is stolen.
- Report a perceived threat or possible security weakness in company systems.
- Refrain from downloading suspicious, unauthorised, or illegal software on their company equipment.
- Avoid accessing suspicious websites.

We also expect our employees to comply with our social media and internet usage policy.

Our IT Team should:

- Install firewalls, anti-malware software and access authentication systems.
- Inform employees regularly about new scam emails or viruses and ways to combat them.
- Investigate security breaches thoroughly.
- Follow this policy provisions as other employees do.

Our company will have all physical and digital shields to protect information.

Remote Connection's

Remote Connection's must follow this policy's instructions too. Since they will be accessing our company's accounts and systems from a distance, they are obliged to follow all data encryption, protection standards and settings, and ensure their private network is secure.

We encourage them to seek advice from our IT Team

Disciplinary Action

We expect all our employees to always follow this policy and those who cause security breaches may face disciplinary action:

- First-time, unintentional, small-scale security breach: We may issue a verbal warning and train the employee on security.
- Intentional, repeated, or large-scale breaches (which cause severe financial or other damage): We will invoke more severe disciplinary action up to and including termination. We will examine each incident on a case-by-case basis.

Additionally, employees who are observed to disregard our security instructions will face progressive discipline, even if their behaviour has not resulted in a security breach.

Take security seriously

Everyone, from our customers and partners to our employees and contractors, should feel that their data is safe. The only way to gain their trust is to proactively protect our systems and databases. We can all contribute to this by being vigilant and keeping cyber security top of mind.

Adopted: 27 June 2023
Last updated: 27 June 2023