# Cyber Security Policy Brief and Purpose

This cyber security policy outlines guidelines and provisions for preserving the security of data and technology infrastructure.

The more we rely on technology to collect, store and manage information, the more vulnerable we become to security breaches. Human errors, hacker attacks and system malfunctions could cause great financial and personal damage and may jeopardise our company's reputation.

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

## Scope

This policy applies to all our employees, contractors, and anyone who has permanent or temporary access to our systems and hardware.

## Policy elements

## Confidential Data

Confidential data is secret and valuable. Common examples are:

- Unpublished financial information;
- Data belonging to customers/associates/vendors;
- Intellectual property, and
- Customer lists (existing and prospective).

All employees are obliged to protect this data. In this policy, we will give our employees instructions on how to avoid 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 laptop computer, and mobile phone secure. They can do this if they:

- Keep all devices password protected;
- Ensure Norton Lifelock 360 is active;
- 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, and
- Log into company accounts and systems through only secure and private networks only.

Our employees are not permitted to access internal systems and accounts from other people's devices or lending their own devices to others.

When new staff receive company-issued equipment they will receive instructions for:

- Password management, and
- Management of Norton Lifelock 360.

They should follow instructions to protect their devices and refer to our IT support staff if they have any questions.

## Keep Emails Safe

Email often host scams and malicious software (e.g. worms.) 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 and / or the sender is not known;
- Be suspicious of clickbait titles (e.g. offering prizes);
- Check email and names of people they received a message from to ensure they are legitimate, and
- Look for inconsistencies or give-aways (e.g. grammar mistakes, capital letters, excessive number of exclamation marks.)

If an employee isn't sure that an email they received is safe, they are to delete it and empty the 'deleted items' and 'Junk Email' folders in Microsoft Outlook.

## 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);
- Remember passwords instead of writing them down;
- Exchange credentials only when absolutely 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, and
- Change their passwords no longer than every two months.

## Transfer Data Securely

Transferring data introduces security risk. Employees must:

- Avoid transferring sensitive data (e.g. customer information) to other devices or accounts unless absolutely necessary;
- 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 and a need to know, and

- Report scams, privacy breaches and hacking attempts.

Our IT support staff 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. Our IT support staff must investigate promptly, resolve the issue and send a company-wide alert when necessary.

Our IT support staff 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 our IT support staff;
- Change all account passwords at once when a device is stolen or misplaced;
- Report a perceived threat or possible security weakness in company systems;
- Refrain from downloading suspicious, unauthorized or illegal software on their company equipment, and
- Avoid accessing suspicious websites.

We also expect our employees to use their common sense when accessing and using social media and the internet.

Our IT support staff should:

- Install firewalls, anti-malware software and access authentication systems;
- Arrange for security training to all employees;
- Inform employees regularly about new scam emails or viruses and ways to combat them, and
- Investigate security breaches thoroughly.

## Remote Employees

Remote employees must adhere to this policy. 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 support staff.

## Cyber Detection and Prevention

Prevent Data Loss

BRG relies on employee trust, but that will not prevent data from leaving the company. BRG will regularly monitor access logs and footprints to its data stored in the cloud.

Back Up Data

BRG Back up data as a risk mitigation strategy against threats such as ransomware or emerging attacks. This is undertaken by:

a. Real time upload to the cloud as well as retention of local copies of files on BRG's network, and

b. External hard drive back up.

## Social Engineering

Social engineering tactics have been used successfully for decades to gain login information and access to encrypted files. Attempts may come from phone, email or other communications with staff. The best defence is to educate and train staff members and outline clear policies. Examples of these are false communications from banks which want your login and use the opportunity to gather your identification and passwords. Another example is the "Hi Mum" scam which requests money be sent urgently to criminals posing as children of the target.

For specific and contemporary social engineering tactics please refer to:

https://www.cyber.gov.au/acsc/view-all-content/publications/detecting-socially-engineered-messages

## Education

People are always your weakest link when it comes to information security. That does not mean you cannot limit the risk through regularly educating your users on cybersecurity best practices. Training should include how to: recognise a phishing email, create and maintain strong passwords, avoid dangerous applications, ensure valuable information is not removed from company drives in addition to other relevant user security risks.

## Update Software and Systems

With cyber-criminals constantly inventing new techniques and looking for new vulnerabilities, an optimised security network is only optimised for so long. BRG will keep its network protected and make sure software and hardware security is up to date with the latest releases.

## 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 will issue a verbal warning and train the employee on security, and
- 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 resulted in a security breach.

## BRG Takes 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.

For further information and contemporary scams refer to:

https://www.cyber.gov.au/learn/scams

This policy was last reviewed in February 2023.