Cyber Security Policy

Paradise Nutrients Pty Ltd Cyber Security Policy includes guidelines and provisions for security measures to help mitigate cyber security risk. It applies to all company employees, contractors, volunteers, and anyone who has permanent or temporary access to the company's systems and hardware.

1. CONFIDENTIAL DATA

Confidential data is valuable and is to be kept secret. Company confidential data includes:

- Unpublished financial information
- Data of customers/partners/vendors
- Patents, formulas or new technologies
- Customer lists (existing and prospective)

All employees are obliged to protect this data.

2. PROTECT PERSONAL AND COMPANY DEVICES

When employees use their digital devices to access company emails or accounts, they introduce security risk to company data. Employees are to keep both their personal and company-issued computer, tablet and mobile phones secure. To keep these devices secure:

- Keep all devices password protected
- Ensure the **Paradise Nutrients Pty Ltd** recommended antivirus is installed and up-to-date
- Do not leave 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

Employees must not access internal systems and accounts from other people's devices or lend their own devices to others.

3. SAFEKEEPING EMAILS

Emails can host scams and malicious software. To avoid virus infection or data theft, employees must:

- Avoid opening attachments and clicking on links when the content is not adequately explained (e.g. "Watch this video, it's amazing.")
- Be suspicious of clickbait 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 giveaways (e.g. grammar mistakes, capital letters, excessive number of exclamation marks).

If an employee isn't sure if an email they received is safe, they are to make contact with **Paradise Nutrients Pty Ltd** administration to be provided with further instruction.

4. MANAGING PASSWORDS

Password leaks are dangerous, since they can compromise the company's entire infrastructure. Not only should passwords be secure so they will not be easily hacked, but they should also remain secret. For this reason, employees are 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. If employees need to write their passwords, they are obliged to keep the paper or digital document confidential and destroy it when their work is done.
- 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 two months.

5. DATA TRANSFERS

Transferring data introduces security risk. Employees must:

- Avoid transferring sensitive data (e.g. customer information, employee records) to other devices or accounts unless absolutely necessary. When mass transfer of such data is needed, we request employees to ask the company's Security Specialists for help.
- Share confidential data over the company network/system and not over public wi-fi connections
- Ensure that the recipients of the data are properly authorised people or organisations who have adequate security policies.
- Report scams, privacy breaches and hacking attempts.

Paradise Nutrients Pty Ltd administration need to know about scams, breaches and malware as soon as an employee becomes aware of such, 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 admin@paradisenutrients.com.au, whom will investigate promptly, resolve the issue and send a companywide alert when necessary.

6. 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 [HR/IT Department].
- 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, email and internet usage policies.

7. REMOTE EMPLOYEES

Remote employees must follow the Cyber Security Policy. As remote employees will be accessing the company's accounts and systems from a distance, they are obliged to follow all data encryption, protection standards and settings and ensure their internet and devices used are secure.

8. DISCIPLINARY ACTION

All employees are to always follow the above-mentioned guidelines and those who cause security breaches may face disciplinary action:

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

Each incident will be examined on a case-by-case basis.

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