Print Radio TASMANIA

Turning print into sound

Cyber Security Policy

Policy brief & purpose

This cyber security policy outlines our guidelines and provisions for preserving the security of our data and technology infrastructure. The more we rely on technology to collect, store, and manage information, the more vulnerable we become to severe security breaches. Human errors, hacker attacks and system malfunctions could cause great financial damage and may jeopardise the reputation and wellbeing of Print Radio Tasmania.

Scope

This policy applies to all our employees, contractors, volunteers, 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- Unpublished financial information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 of customers/partners/vendors
- Patents, formulas or new technologies
- Customer lists (existing and prospective).

All board members, employees and volunteers are obliged to protect this data. This policy includes instructions on how to avoid security breaches.

Protect personal and company devices

When board members, employees and volunteers use digital devices to access company emails or accounts, they introduce security risk to our data. We advise our committee members, employees and volunteers keep both their personal and company-issued computer, tablet and mobile phone secure.

They can do this if they:

- Keep all devices password protected.
- Choose and upgrade 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 board members, employees and volunteers to avoid accessing internal systems and accounts from other people's devices or lending their own devices to others.

When new committee members, employees and volunteers receive company-issued equipment they will receive instructions for:

- *Disk encryption setup*
- *Password management tool setup*
- *Installation of antivirus/ anti-malware software*

They should follow instructions to protect their devices and refer to the President or the Broadcast Manager if they have any questions.

Keep emails safe

Emails often host scams and malicious software (e.g., worms.) To avoid virus infection or data theft, we instruct committee members, employees, and volunteers to:

- 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 a committee member, employee, or volunteer isn't sure that an email they received is safe, they can refer to the President or the Broadcast Manager.

Manage passwords properly

Password leaks are dangerous since they can compromise our entire infrastructure. Not only should passwords be secure so they won't be easily hacked, but they should also remain secret. For this reason, we advise our committee members, employees, and volunteers 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 telephone instead of email, and only if they personally recognise the person they are talking to.
- Change their passwords every two months.

Committee members, employees and volunteers are obliged to create a secure password, following the above-mentioned advice.

Transfer data securely

Transferring data introduces security risk. Employees must:

- Avoid transferring sensitive data (e.g., customer information, employee records) to other devices or accounts unless 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.
- Report scams, privacy breaches and hacking attempts immediately to either the President or the Broadcast Manager.

Our organisation needs to know about scams, breaches and malware so that we can better protect our infrastructure. For this reason, we advise our committee members, employees, and volunteers to report perceived attacks, suspicious emails or phishing attempts as soon as possible to the President or the Broadcast Manager who must investigate promptly, resolve the issue and send a companywide alert when necessary.

The President and the Broadcast Manager are responsible for advising Committee members, employees, and volunteers on how to detect scam emails. We encourage all those associated with Print Radio Tasmania to reach out to them with any questions or concerns.

Additional measures

To reduce the likelihood of security breaches, we also instruct our committee members, employees, and volunteers to:

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

Committee members, employees and volunteers working remotely

Everyone associated with PRT working from a distance must follow this policy's instructions too. Since they will be accessing our organisation's accounts and IT systems from a distance, they are obliged to follow all data encryption, protection standards and settings, and ensure their private network is secure.

Disciplinary Action

We expect all our committee members, employees, and volunteers 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, committee members, employees and volunteers who are observed disregarding our security instructions will face progressive discipline, even if their behaviour has not resulted in a security breach.

Take security seriously

Everyone, from our volunteers and partners to our employees and sub- contractors, should believe 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.

Authorised by:
Nigel Green - Broadcast Manager

Endorsed by:
Management Committee
Print Radio Tasmania Inc.

Date: 16/03/2021