PROJECT INDEPENDENCE

Cyber Security Policy

Introduction

Project Independence (PI) wishes to foster a culture of openness, trust, and integrity, and this can only be achieved if external threats to the integrity of the organisation's systems are controlled, and the organisation is protected against the damaging actions of others.

The Australian Charities and Not-For-Profit Commission (ACNC) states that:

- Cyber security applies to all electronic information, but if a charity handles personal or sensitive information it must be particularly careful about how it is handled.
- Some cyber security risks are:
  - An employee or volunteer having unauthorised access to files they should not have access to.
  - Keeping a written register of passwords on a desk.
  - An employee clicking on a link in an email from an unfamiliar source.
  - Individuals having weak passwords on their work devices.
  - An organisation not prioritising the protection of information that could be valuable to an attacker.

Purpose

- This policy sets out guidelines for generating, implementing, and maintaining practices that protect PI's cyber media- its computer equipment, software, operating systems, storage media, electronic data and network accounts- from exploitation or misuse.

- This policy applies to employees, contractors, consultants and volunteers at PI, including all personnel affiliated with third parties, to all equipment owned or leased by PI, and to all equipment authorised by PI for the conduct of the organisation's business.

Policy

- Data created on PI's systems remains the property of PI.
- Employees and volunteers will take all necessary measures to maintain the necessary cyber security procedures, including protecting passwords, securing access to computers, and maintaining protective software.
- PI will educate employees on cyber security awareness, including recognition of phishing attempts, malware, and other risks that may threaten the security of the company network and data.

- Breach of this policy by any employee may result in disciplinary action, up to and including dismissal. PI reserves the right to audit networks and systems periodically to ensure compliance with this policy.
- PI will implement security measures to mitigate any identified risks, such as password protecting sensitive information.
- PI will activate an Incident Response Plan to respond to any identified data breach, which will result in an update to cyber security processes.

Related Documents

Privacy, Dignity and Confidentiality Policy