Cyber Security Procedures

Responsibilities

It is the responsibility of the Project Independence (PI) CEO to ensure that staff are aware of the cyber security policy and processes, and that any policy breaches are dealt with appropriately. They must monitor changes in cyber security requirements and ensure policy and procedures reflect those changes.

All PI employees and volunteers have the responsibility to familiarise themselves with the policy and procedures and ensure that they conform to them.

Processes

a. Monitoring

The CEO may authorise at any time, an appropriate individual to monitor the organisation's equipment, systems and network traffic for security and network maintenance purposes.

b. Confidentiality

PI shall classify the information it controls in the organisation's computer system files, website, and databases as either non-confidential (open to public access) or confidential (in one or many categories). The CEO will review and approve the classification of the information and determine the appropriate level of security that will best protect it.

c. Controlling Access

Staff shall only be permitted to access those resources that they have clearance for (from the CEO), with access control being exercised by username and password controls.

d. Security Processes

- **Password Security** PI staff must use strong passwords, never reveal their passwords to others, not reuse old passwords, not attempt to use an account other than their own and not share their user account information with others. Passwords must be kept secure and

should not be accessible in the vicinity of the computer or mobile device concerned. Employee log-on IDs and passwords must be deactivated as soon as possible if the employee leaves PI.

- **Emails** PI staff must use extreme caution when opening email attachments received from unknown senders and must not send PI information through unauthorised messaging applications or social media platforms. They must not send emails containing passwords in clear text, or account information such as Log-On ID and password combinations. Corporate email addresses must not be used for any other purpose than for PI business.

- **Data/ Information Sharing** PI staff must not provide information about, or lists of, PI residents to parties outside the organisation or parties within the organisation who do not have the authority to access this. All data must be shared in the appropriate shared location as provided by PI. PI retains the right to delete any personal media files stored in shared locations. Use of removable media (USB Drives, external Hard Drives, CDs/DVDs) to store sensitive information is not permitted unless specifically authorised by the CEO. No PI information or data can be stored on any personal device, even if only temporarily.
- **Downloading Data or Software** Staff must not access data, a server, or an account for any other purpose other than for PI business. The exceptions to this are the 'additional freedoms' PI extend to the Live-In Resident Coordinators (LIRCs) regarding the use of PI provided IT and communications equipment, namely permission in non-work hours to:

  - Store music and other personal media such as photos and videos as long as they are obtained legally and otherwise do not breach PI policy.

  - Download and watch movies and TV shows where they are downloaded lawfully and do not otherwise breach PI policy.

  - Use Facebook and other social media applications after hours as long as they do not breach PI policy.

  - Conduct lawful private activity without exceeding monthly budgets allocated for usage as long as this activity does not breach PI policy.

- **Social Media Use** PI information must only be shared over official, authorised communication channels. Staff are not to place comments representing or giving the

impression of representing PI on social media unless explicitly authorised to do so, nor send PI data and information on personal devices.

When accessing social media sites on PI computers or devices:

- End users may be subject to logging and monitoring checks;
- Access may be restricted to specific social media sites; and
- Inappropriate social media websites will be blocked.

- **Security of Devices** Staff must not leave PI devices in places that are readily accessible by individuals who are not employed by PI and must always lock the screen or log off when a PI device is unattended. They must not allow any other individual to use their PI devices unless they are also a PI staff member, or they are a casual staff member authorised to use the equipment for PI business. In the event of a device being lost or stolen, staff must report it immediately to their supervisor.

e. Incident Response Processes

- Security incidents can originate from intentional or unintentional actions. Staff who believe their computer systems or mobile devices have been subjected to a security incident, intentional or unintentional, or has otherwise been improperly accessed or used, should report the situation to their supervisor immediately, who will in turn notify the CEO. The PI Cyber Security Incident Response Process follows the steps recommended by the ACNC for responding to a security breach:

  - **Identify** Report the actual or suspected data breach immediately to the supervisor who will escalate it to the CEO. The CEO will identify whether a breach has occurred or not using the Office of the Australian Information Commission (OAIC) Guide. If a data breach has occurred, the CEO will appoint a Response Coordinator.

  - **Investigate** The Response Coordinator will investigate the breach and assess: the time and date of the data breach; the type of information involved; the cause of the breach; the extent of the breach, people who have been or may be affected; the extent of the harm; the need to notify the people affected, and what information they need to know.

  - **Assess** The assessment will consider: what is the extent of the loss, misuse or disclosure of information; what is the risk of harm to the organisation; is there a risk of harm to individuals because of the breach (for example, has it revealed personal or sensitive data); what action needs to be taken to reduce the risk of harm (to individuals, to the organisation); and is there a need to notify affected people or regulators.

  - **Notify** The CEO will notify affected people, associated businesses and regulators.

  - **Review** The Response Coordinator and CEO will review the data breach and response. Findings will be recorded and recommendations for improvements made. The review will include: an understanding of how the breach occurred, updates to policy and

procedures required to prevent another breach occurring, and if employee training for dealing with private and confidential information is required.

Related Documents

Privacy, Dignity and Confidentiality Policy

Privacy, Dignity and Confidentiality Procedures