Information Security Policy

Purpose

This policy defines how EMPHN protects its information, and information systems from threats. It aims to safeguard the integrity, confidentiality, and availability of data while maintaining compliance with legal and regulatory requirements.

Scope

This policy applies to EMPHN staff, contractors, vendors, university students involved in research projects and stakeholders who access, manage or support EMPHN's Information, data and IT infrastructure.

EMPHN's information security objectives

Effective information management: Ensure the confidentiality, integrity, and availability of all organisational data.

Prevent unauthorised access: Implement measures to restrict unauthorised access to information systems.

Maintain compliance: Adhere to relevant laws, regulations, and industry standards related to IT security.

Promote security awareness: Foster a culture of security awareness and responsibility among employees.

ISO27001 certification: Ensure EMPHN uses the certification process to maximise information protection and cyber security; and to ensure effective response mechanisms are in place and regularly tested.

Roles and Responsibilities

IT Security Team

The IT Security Team is responsible for the development, implementation, and maintenance of the security policies and procedures. They monitor security threats, respond to incidents, and ensure compliance with security standards. The IT Security Team consists of EMPHN's IT Team and the Managed Services Provider (MSP).

EMPHN has Technological Controls in place to manage

- *Endpoint devices via MS Intune*
- *Privileged access rights*
- *Information access restrictions*
- *Secure authentication utilising MFA, SSO, VPN*
- *Capacity – Storage, Licenses*
- *Technical vulnerabilities*
- *Information backup and recovery*
- *Redundancy of information processing facilities*
- *Software licensing and installation*
- *Information security awareness campaigns*

Employees

All EMPHN staff must complete mandatory and recurring security training, report security incidents, and protect their login credentials and devices. Assigned system owners have additional responsibilities as outlined within this policy.

Security Practices

Access Control

Access to information systems, facilities, services and materials is restricted based on the principle of least privilege. Employees are granted access only to the data and systems necessary for their job functions. Multi-factor authentication (MFA) or Single Sign On (SSO) is required for accessing sensitive systems.

Access to information systems, facilities, services and materials by third parties is provided according to the Third-Party Information Security Policy. The Executive Director, Corporate Services may rescind user access at any time.

Establishing the identity of employees is part of identity management and identity is provided and established by issuing access credentials to the employee on the MS Platform. This process is initiated once HR completes their recruitment process and assigns tasks within Employment Hero to IT. This informs IT with the necessary information to raise an onboarding ticket (form with identity details of the employee) with the MSP. Once the identity is established the MSP will return details to IT to pass onto the new employee at induction time (along with a laptop etc) to setup authentication methods to access the EMPHN systems.

Application system owners are identified in the IT Access Management Master List, maintained by the Executive Director, Corporate Services. A record of all users must be maintained by the system's owner. Owners must review all delegated authority quarterly to ensure access levels are appropriate and deactivation of accounts no longer needed has occurred. User accounts that have been inactive for 90 days must be removed or disabled. System owners are responsible for this.

For example, Employment Hero is managed by the HR Team and is web hosted. This means HR is responsible for ensuring those who are onboarded to the EH system have the correct access level within that system. Another example is Access Financials (which is also web hosted) and includes an accounting system, an expense module and an invoice payment system. Most senior employees have limited capability to approve invoices and/or expenses within Access. This system is administered by the Finance Manager.

MS Teams are workspaces formed to provide a collaboration environment for a group of staff who work on a topic together. Each workspace, known as a Team and Channel(s) environment includes space for file storage, project planning, hosting of meetings and group chat functionality. Teams can be configured as Public, Private or Shared and each type has different levels of access controls. Private Microsoft Teams membership and access is managed by the MS Team's owner. Public Microsoft Teams can be accessed by any EMPHN user, however external guests can be added only by the team owner. In these environments the Team's owner is accountable for ensuring third parties have access to EMPHN's Third Party Information Security Policy and understand their obligations. There is no record kept in the IT Access Management Master List for MS Teams or Channels as they are not deemed individual applications.

The Executive Director, Corporate Services or their nominee monitors and audits IT user activity on EMPHN's network, in accordance with the Acceptable Use of Information Systems and Technology Procedure.

Network security

The organisation employs firewalls, intrusion detection systems (IDS), and encryption to protect its network from unauthorised access and attacks. Regular network security assessments and vulnerability scans are conducted to identify and mitigate potential threats.

The IT Manager maintains a documented overview of the IT facilities.

The EMPHN domain (the Microsoft Platform) is protected by Geo Location blocking meaning access into the domain from outside of Australia is not possible unless specific user exemption is granted.

Regular penetration (PEN) testing is performed on EMPHN's firewalls and external websites to identify weaknesses and vulnerabilities which are mitigated and retested for certainty.

Data protection

All sensitive data is encrypted both in transit and at rest. Data access is monitored and logged, and regular backups are performed to ensure data recovery in case of a breach or disaster.

The IT Manager is responsible for ensuring all backups of business-critical data is tested periodically to ensure they support full system recovery. Restore procedures are documented and tested annually.

Device security

All devices including laptops, BYOD used to access organisational systems must be secured with strong passwords and up-to-date antivirus software. Employees are required to report lost or stolen devices immediately. EMPHN hard drives (laptops) are encrypted using Microsoft BitLocker.

Patch management

Software and systems must be regularly updated with the latest security patches to protect against vulnerabilities. The IT Team is responsible for managing the patching process and ensuring timely updates. Patching is performed automatically via Windows update, Defender and MS Intune.

Incident response

The organisation has a defined incident response plan to address security breaches and incidents. The plan includes procedures for detection, containment, eradication, and recovery. All incidents must be reported to the IT Security Team immediately.

Security training

Regular security training and awareness programs are conducted for all employees. The training covers topics such as phishing, social engineering, password management, and safe browsing practices. Phishing awareness campaigns are initiated every 3 months via the Knowbe4 platform and awareness training is performed every 6 months via Employment Hero.

Compliance

EMPHN is preparing for ISO27001 certification in December 2025. As part of ongoing compliance with the ISO27001 Standard, an internal audit program of the organisation's information security is conducted each year. This program is reviewed and tested during each certification and surveillance audit by the certifying external auditor (at the time of writing, the certifying audit is Intertek).

Policy review

This Information Security Policy is reviewed and updated every 3 years or whenever significant changes occur in the organisation's infrastructure or threat landscape.

Breaches

Violations of this policy may result in disciplinary actions, including termination of employment or contracts.

Where to get help?

- For enquires about this policy, contact: the **Executive Director, Corporate Services**
- You can provide feedback on this policy, or EMPHN's handling of a security incident, via the feedback button on EMPHN's website or intranet