Information Security Management System (ISMS)

Position Statement

Introduction

yourtown is committed to providing innovative quality programs and services that support young people and their families, especially those who are marginalised and without voice.

We recognise the vital role information plays in maintaining efficient, effective and safe services and operations, and the importance of securing and protecting information in line with community expectations and legal requirements.

Our information management security system underpins our organisational repute and the trust held within our brands.

yourtown's Position

In protecting the interests of our clients, supporters and stakeholders, **yourtown** is committed to complying and satisfying any applicable requirements related to information security, including but not limited to legal, statutory, regulatory, contractual and industry requirements.

yourtown is also committed to the continuous improvement of the ISMS and maintaining currency of knowledge.

We recognise that there are both physical and electronic risks to information security. Accordingly, we undertake appropriate measures to ensure our personnel are aware and informed of their responsibilities, our systems and technologies are secure, and that information collected by **yourtown** is protected at all times.

This statement on Information Security Management Systems (ISMS) applies to all users of **yourtown** ICT resources – including (but not limited to) all personnel, third parties, partners, clients and visitors to **yourtown**. This applies to all **yourtown** ICT Assets and all devices connected to the **yourtown** network.

These measures include the following:

Human Resources Security

- Ensuring all personnel are subject to appropriate security frameworks and processes before, during and after ceasing their employment.
- Maintaining other policies, procedures, guidelines, and training to provide clear guidance to personnel on how they can manage and protect the information they handle.
- Ensuring the management and administration of our information systems and technologies are appropriately resourced and undertaken by competent personnel.

Web Application Security

- Ensuring that web applications be designed, built and tested (verified) to ensure security is applied at all layers of the application and technology.

Network Security

- Ensuring that **yourtown** network architecture be commensurate with current and future business requirements as well as with emerging security threats.

Data Security

- Implementing encryption techniques for protecting sensitive data during transmission and storage.

Cloud Security

- Ensuring that endorsed cloud based services follow a formalised risk assessment to identify the necessary security controls that must be established by the Cloud Service Provider and **yourtown** to manage security risks to an acceptable level.

Physical and Environmental Security

- Ensuring that facilities such as data centres and computer rooms etc. where critical information is stored or processed be constructed and arranged in a way that data is adequately protected from physical and environmental threats.

Security Incident Management

- Maintaining formalised security incident handling processes for responding quickly and effectively to information security breaches should they ever occur.
- Implementing incident detection mechanisms such as security event logging and antivirus programs on all IT systems.

Vulnerability Management

- Implementing security patch and vulnerability management processes to identify, prioritise and remediate security vulnerabilities.

Information Security Risk and Compliance Management

- Undertaking or arranging regular IT audits, reviews and testing of our information systems to assure integrity and to identify areas for improvement.
- Regularly reviewing our Privacy Policy to ensure it provides transparency and awareness in how we manage and protect personal information.
- Allowing for IT security to be identified, mitigated and monitored through **yourtown** risk management processes.
- Measuring and monitoring the compliance with **yourtown** ISMS to ensure that all **yourtown** Departments abide by ISMS's security controls.

User Access Management

- Ensuring all user access related requests (e.g. such as adding new users and revoking user access rights) are logged, assessed and approved in accordance with defined user access management process.
- Ensuring all personnel are authorised to manage the information they handle and systems maintain access authorisations dependent upon position.

Change Management

- Ensuring that any change to **yourtown** information systems must be logged and assessed for security, and risk impact as documented in the **yourtown** change management processes. The requirements, risk and impact of each request is evaluated and the proposed risk mitigation solution documented and approved.

Logging and Monitoring

- Maintaining logs for key security-related events such as user privilege changes and ensuring these logs are protected against unauthorised changes and analysed on a regular basis.

End User Protection

- Implementing measures that allow end user desktop computers, mobile computers (e.g., laptops, tablets) be protected with adequate security mechanisms to prevent the unauthorised disclosure and/or modification of **yourtown** data.

Data Backup

- Ensuring that data is backed up on a regular basis, protected from unauthorised access or modification during storage, and available to be recovered in a timely manner in the event of incident or disaster.

ICT Asset Management

- Ensuring that ICT asset owners implement appropriate ISMS and data handling controls to maintain Confidentiality, Integrity and Availability of **yourtown** Data.

ICT Recovery

- Ensuring that an ICT Recovery Plan and relative process is in place to enable the recovery of business critical **yourtown** services in a timely manner, to minimise the effect of IT disruptions and to maintain resilience before, during, and after a disruption.

ICT System Acquisition & Development

- Ensuring that ICT security requirements are addressed within the software development lifecycle, to reduce the risk of vulnerabilities being introduced during the acquisition or development of ICT systems.

Third Party Risk Management

- Ensuring that security risks arising from **yourtown** contracted third parties (i.e., suppliers, vendors etc.) who maintain direct or indirect access to **yourtown** IT systems and data must be operationally and contractually controlled.

Mobile Devices

- Ensuring that **yourtown** staff, contractors and users who are authorised to connect personally owned devices to the **yourtown** networks comply with secure practices to ensure the security of **yourtown** networks and **yourtown** data on their devices

ICT Acceptable Use

- Ensuring that all users who have access to **yourtown**'s ICT systems and services must adhere to specific rules regarding use of **yourtown** resources, their internet and email usage as well as when interacting with social media.