

# Information Security Management System Policy

V2.0 102025

## 1. Introduction

- 1.1 Tecknuovo are committed to Information Security and the confidentiality, integrity, and availability of physical and information assets to provide clients and employees with confidence that their information is handled securely. Tecknuovo are actively maintaining the ISO 27001:2022 certification for the provision of technology consultancy services to custom build enduring in-house capabilities and deliver bespoke technology solutions. Tecknuovo are currently seeking ISO 20000:2018 certification.

## 2. Scope

- 2.1 This policy covers all individuals working at all levels and grades, including senior managers, officers, directors, employees, consultants, trainees, homeworkers, part-time and fixed-term employees, volunteers, interns and casual workers.
- 2.2 This policy also covers our sub-contractors and associates whom we contract with to deliver consultancy and project management services alongside us in support of our delivery of services to our clients.

## 3. Responsibility

- 3.1 The Chief Legal Officer has overall responsibility for implementing this policy. They have a key role in ensuring the systems and controls we have in place are effective.
- 3.2 All employees have a role to play in complying with our information security performance objectives and are encouraged to make further suggestions in relation to initiatives we could undertake. If anyone has a suggestion, they should contact the Chief Legal Officer.
- 3.3 In line with that commitment, in accordance with our Whistleblowing Policy, we actively encourage all staff members who have serious concerns about any real or perceived departure from the high ethical standard that we set, to voice those concerns openly. Our Whistleblowing Policy can be found on our online HR system.
- 3.4 We are committed to ensuring our policy remains effective. As part of our ongoing commitment, this policy is reviewed at least annually to verify its effective operation. Records of the reviews are maintained, and any necessary amendments are made to the policy, as appropriate.

## 4. Communication

- 4.1 We communicate this policy to our employees by means of our HR System and/or SharePoint. It is available externally upon request.

## 5. Our Conduct

- 5.1 Whilst identifying and understanding that we operate in an information rich business, where information may be at risk, the ISMS has been established to minimise potential breaches. Below is framework that has been determined

for setting objectives to ensure Information Security is at the heart of everything we do and that we continually aim to enhance our ISMS:

- Information will be protected from unauthorised access.
- All service assets are identified, classified and managed in accordance with documented asset management procedures
- Confidentiality of information will be assured.
- Integrity of information will be maintained.
- Availability of information for business processes will be maintained.
- Legislative and regulatory requirements will be met.
- Business Continuity plans and service continuity plans (in alignment with service delivery under ISO20000-1) will be developed, maintained, and tested.
- Information Security training will be provided to all employees upon employment and throughout the duration.
- All actual or suspected information security breaches will be reported to the IT Manager and will be thoroughly investigated.
- Continually improve the ISMS.

The Information Security Management System Policy is available internally and externally. In support of the objectives set by Senior Management, they are also committed to:

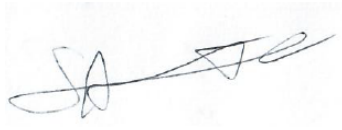
- Performing Management Reviews and periodically assessing the ISMS Policy and ISMS objectives to ensure their continuing suitability.
- Assessing all informational assets, risks, and opportunities against all internal, external, deliberate, or accidental threats, including interested parties. The information security risks inclusive of those associated to the SMS shall be reviewed at least annually as a minimum.
- Ensuring that information security is addressed, monitored, and reviewed as part of our ongoing supplier management process.
- Ensuring that information security controls are embedded within all service management processes, including incident, change, asset and supplier management, to ensure the confidentiality, integrity, and availability of services delivered to clients.
- Providing resources for the implementation and continued provision of physical controls that enforce and aid in driving policies.

## 6. Responsibility

An annual review of the policy is delegated to the Chief Legal Officer who will:

- Ensure that it remains up to date, compliant and relevant to the needs of the organisation and its clients.
- Verify it is in effective operation across the practice.

INTERNAL

A handwritten signature in black ink, appearing to read 'Gus Sargent', is written over a light blue rectangular background.

Gus Sargent

Director

Date: 14/10/2025

Reviewed: 14/10/2025

Next Review: 14/09/2026