

Information Security Assurance Policy

Purpose

Surecall Recruitment has implemented an Information Security Management System (ISMS) and is committed to safeguarding the confidentiality, integrity, and availability of its information assets, in line with the ISO/IEC 27001:2022 standard. This policy provides a framework to ensure we assess risks within the business and protect information assets from threats, ensure compliance with legal and regulatory requirements, and foster a culture of information security.

Scope

This Information Security Policy applies to all employees, contractors, partners, and third parties with access to Surecall Recruitments' systems, networks, and information assets. It encompasses all business operations, processes, systems, and information in electronic, physical, or other forms. The scope includes all information stored on computers, transmitted across networks, printed out or written on paper, stored on portable media, or spoken in conversation or over the telephone.

Information Security Objectives

It is our policy to ensure that:

- we comply with UK Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country.
- we understand the needs and expectations of all interested parties and have determined those interested parties which are relevant to the information security management system.
- assigned relevant information security roles and responsibilities.
- all customer, client or Group held data is protected, handled, and shared where necessary in accordance with the requirements of UK Data Protection Laws and, to the extent applicable, the data protection or privacy laws of the country of the data owner.
- regular audits and reports are reviewed by the Executive Board.
- all breaches of Information Security, actual or suspected, are reported and investigated up to Board Level.
- confidentiality of information is assured.
- integrity of information is maintained.
- regulatory and legislative requirements, together with any contractual security obligations, are met.
- information is protected against unauthorised access.
- objectives and targets are set and monitored monthly in line with the Surecall Recruitments' Continual Improvement Procedure to achieve continual improvement in our Information Security Management System.
- information security training is provided, where required.
- procedures and instructions are implemented to support this Policy.
- continual improvement in our products and services and the effectiveness of our Information Security Management System.

Leadership Commitment

Top management is committed to:

- Supporting and providing the necessary resources to implement and maintain the ISMS.
- Establishing measurable information security objectives aligned with the organisation's strategy.
- Ensuring continual improvement of the ISMS to address emerging threats and changes to the business environment.
- Promoting a culture of information security awareness across all levels of the organisation.

Information Security Framework

The ISMS follows a risk-based approach and includes:

- Identification and assessment of information security risks, including external and internal interested parties.
- Implementation of appropriate controls to mitigate identified risks.
- Regular monitoring, auditing, and evaluation of the ISMS performance.
- Management of incidents and continual improvement of security measures.

Roles and Responsibilities

All personnel within Surecall Recruitment are responsible for adhering to this policy and supporting the ISMS. Specific responsibilities include:

- Top Management: Oversight, approval, and strategic direction of the ISMS.
- Compliance Manager: Implementation, monitoring, and continuous improvement of the ISMS.
- Managers: Responsible for implementing the Policy within their business areas, and for ensuring adherence by their staff.
- Employees and Contractors: Compliance with security policies, procedures, and reporting any security incidents.
- Third Parties: Adherence to contractual information security obligations.

Climate Change

Surecall Recruitment determines internal and external issues that are relevant to our purpose, strategic direction, and our ability to achieve the intended outcomes of our management system. As part of this evaluation, we also determine whether climate change is a relevant issue that may influence our risks, opportunities, operational performance, or strategic objectives.

Surecall recruitment has identified the interested parties that are relevant to our management system and the requirements of those parties. In doing so, we recognise that relevant interested parties may have requirements related to climate change, and we take these requirements into consideration when determining our obligations and when planning, implementing, and maintaining our management system.

Compliance and Review

Surecall Recruitment will ensure compliance with this policy by:

- Conducting regular internal audits and reviews of the ISMS.
- Ensuring any identified nonconformities are addressed and remediated.
- Reviewing and updating this policy at least annually or in response to significant changes.

Policy Awareness

This policy will be communicated to all relevant stakeholders, including employees, contractors, and third parties. Information security awareness training will be provided to ensure compliance and understanding.

This policy is regularly reviewed for continuing suitability.

A handwritten signature in black ink, appearing to read 'Tony Elia', with a stylized, cursive script.

Tony Elia

Company Director
Surecall Recruitment Ltd

January 2026