WILSON JAMES POLICY STATEMENT

Policy Title	Information Security	**Policy No.**	G26
Owner	Information Security Management Forum	**Date Issued**	Jan-19
Author	Information Security Manager	**Date Reviewed**	Dec-23
Scope	This Policy applies to all persons who carry out work on behalf of Wilson James and including employees, consultants, contractors, agency, and temporary staff.		
Responsibility	The Policy owner is responsible for ensuring that this policy remains current and up to date and shall formally review the policy on an annual basis		

Statement by CEO

Wilson James recognises that Information Technology / Information Systems play a major role in our business activities. Like any other asset, the data in our possession and the infrastructure that handles it, must be kept secure. A breakdown in security could have serious effects on our business. Any breach could result in a direct financial loss, a loss of confidence, or a breach of legal and/or regulatory requirements. For these reasons the Board of Directors have approved the production and companywide implementation of an Information Security Management System ("ISMS") and programme.

The ISMS establishes standards that represent the minimum-security requirements that apply to all our information systems, and the processes that support them. It also gives important responsibilities to managers who must ensure compliance within their areas of control. This will ensure that there is a correct balance between the objectives of creating and maintaining an open, trusting environment in which information, with limited exceptions, is made freely available to all employees, while protecting our data from accidental or deliberate loss, alteration, or disclosure.

It is essential that this Policy is fully implemented and that all employees are aware of their responsibilities regarding the protection of data and systems against unauthorised access or disclosure. I would therefore ask that you read this document and direct any questions to your manager.

Mark Dobson
Chief Executive Officer

Focus

The principal focus of Information Security is to provide the following:

- Confidentiality: the restriction of access to information to authorised persons, entities, and processes at authorised times and in an authorised manner.
- Integrity: safeguarding the accuracy and completeness of information and information processing systems.
- Availability: ensuring that authorised users have access to information and associated assets when required.

Purpose

Wilson James aims to maintain the security of all the information it holds, whether that be internal information, or any external information held for clients or other organisations. Accordingly, an Information Security Management System (ISMS) is implemented to guide staff in how such security is to be maintained which will enable the business to satisfy legislative and customer requirements.

This policy is communicated to employees through the Company Induction and regular communication. It is available to all interested parties through the WJ website. Specific excerpts will be published on Wilson James's website (www.wilsonjames.co.uk) and as part of the 27001 Certification process.

The purpose of the policy is to ensure that:

- Information assets[1] are protected from threats, whether internal or external, deliberate, or accidental.
- Information is made available with minimal disruption to staff and clients as required by the business process[2];
- The integrity of this information is maintained[3];
- Confidentiality of information is assured[4];
- Regulatory and legislative requirements are met[5];
- A Business Continuity Framework is implemented, and Business Continuity plans produced, maintained, and tested to counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters[6];
- Information security education, awareness and training is available to staff[7];
- All breaches of information security, actual or suspected, are reported to, and investigated by the ISMF and the Incident Response team[8]; and
- Appropriate access control maintained, and information is protected against unauthorised access.
- Effectiveness and monitoring are in place to ensure continuous improvement[9]

[1] Information takes many forms and includes data stored on computers, transmitted across networks, printed out or written on paper, stored on tapes, USB, or spoken in conversation and over the telephone.

[2] This will ensure that information and vital services are available to users when and where they need them.

[3] Safeguarding the accuracy and completeness of information by protecting against unauthorised modification.

[4] The protection of valuable or sensitive information from unauthorized disclosure or unavoidable interruptions.

[5] This will ensure that Wilson James remains compliant to relevant business, national and international laws and it include meeting the requirements stated in legislations such as the Companies Act and the Data Protection Act.

[6] Business Continuity Management should be implemented effectively to ensure continuity of business operations in the event of a crisis or disaster.

[7] Ensure that relevant and effective training is provided to staff.

[8] Ensure that the staff understand their roles and responsibilities in handling incidents and have a comprehensive and well-tested incident response plan ready.

[9] Effectiveness of the policies and controls as well as monitoring will be co-ordinated and reported to the ISMF and escalated to the Directors as appropriate to ensure continual improvement.

ISMS Objectives

- To maintain our third-party UKAS approval to the latest revision of the 27001 standard.
- Maintain the integrity of the WJ ISMS.
- Maximum availability of critical systems.
- Regular awareness Information Security training/communication for all employees.
- Achieve all regulatory, legal, and other requirements.
- Achieve a robust patch management system.
- Achievement of process effectiveness KPIs.
- Maintain and continually improve our ISMS.

ISMS Framework

- Policies, Procedures and Guidelines are available on the WJ IMS (intranet) to support this ISMS Policy.
- The Company has direct accountability for maintaining the ISMS Policy and has appointed the Information Security Management Forum ("ISMF") to write, develop, manage, and approve the relevant policies, procedures, and guidelines to support the ISMS policy.
- The Directors are directly responsible for implementing the ISMS Policy within the organisation, and for adherence by their staff.
- It is the responsibility of each member of staff to adhere to the ISMS Policy and relevant procedures. Failure to do so may result in disciplinary action.
- Information security is managed through Wilson James's ISMS framework.
- The availability of information and Information Systems will be met as required by the core and supporting business operations.
- Internal audits shall assess compliance with this ISMS policy and the Information System.
- The ISMS includes a Third-Party Security Policy.
- The ISMF will monitor and implement continuous improvement.

ISMS Management System – All persons carrying out work on behalf of WJ.

The ISMS is structured to enable continual improvement of the ISMS through regular review that includes audit, management review and results analysis. The following ISMS Policies and Procedures confirm the process to be complied with by all employees, consultants, contractors, agency, and temporary staff to enable Wilson James to achieve this ISMS Policy and understand their contribution to the effectiveness of the information security management system, including the benefits of improved information security performance.

- **ISMS Manual:** The Information Security Management System Manual confirms how WJ meets all requirements of the ISO 27001 International Standard. All personnel who have a management role in the Information Security Management System must ensure that the Wilson James Information Security Management System is maintained in accordance with the requirements of this manual.

- **Acceptable Usage Policy:** Wilson James expects all its employees to use its information systems in a professional, courteous, sensible, and legal manner following appropriate Company procedures outlined in the ISMS. Employees are expected to comply with this policy irrespective of what system they are using to conduct company business.

- **Access Control Policy:** This policy defines controls against threats of unauthorized access, theft of information and disruption to information communication and technology services of Wilson James Ltd and establishes responsibilities when managing access to systems and applications.

- **Asset Management and Information Classification Policy:** This policy defines rules to maintain appropriate level of protection for Information Communication and Technology assets owned and managed by Wilson James Ltd.

- **IT Operations and Network Security Management Policy:** This policy establishes rules for a secure Information Communication and Technology operation within Wilson James Ltd with the responsibilities to ensure the network environment is sufficiently secured.

- **Information Security and Privacy Risk Assessment and Treatment Policy:** The policy establishes rules that need to be followed when identifying, assessing, and treating risks related to information security and privacy.

- **ISMS-SOP-No.1 ISMS Management Review and Compliance Procedure:** This procedure refers to the process and guidelines followed by the company to ensure the effective management and review of Information Security Management System (ISMS). The procedure involves regular reviews of the ISMS to assess its performance, identify areas for improvement, and ensure its alignment with the organization's objectives and goals.

- **ISMS-SOP-No.2 Change Management Procedure:** Should a change in procedures, systems, or configuration be required it must be approved before implementation. The procedure ensures that changes are effectively managed to minimize disruption and maximize the benefits for the company and its employees.

- **ISMS-SOP-No.3 Incident Management and Awareness Procedure:** When an incident that affects information systems occurs, it is vital that this is immediately reported to enable effective corrective action to be taken. Further, regular training and exercises are conducted to familiarize personnel with the procedure, enabling them to respond effectively to incidents and mitigate their potential impact.

- **ISMS-SOP-No.4 Asset Management and Disposal Procedure:** Effective management and disposal of Information Technology (IT) assets is important to ensure that the IT assets are identified, recorded, managed effectively to prevent unauthorised access or misuse and they are disposed securely.

- **ISMS-SOP-No.5 Vulnerability and Patch Management Procedure:** It is important to identify, assess, and address vulnerabilities in systems and software. It involves regularly scanning for potential weaknesses and applying necessary patches and updates to mitigate any potential security threats. This procedure ensures that the IT infrastructure and systems remains secure and protected against emerging vulnerabilities.

- **ISMS-SOP-No.6 Third Party Security Management Procedure:** This procedure involves assessing and managing potential risks associated with third-party relationships and implementing appropriate security measures. By following this procedure, Wilson James aims to safeguard sensitive information, protect against security breaches, and maintain a secure environment.

- **ISMS-SOP-No.7 User Access Management Procedure:** To ensure that registration and de-registration of IT user accounts for access to IT networks and systems is conducted in a secure and timely manner and includes the requirements for allocating user account privileges on a need-to-know basis, including when a user changes their job role.

- **ISMS-SOP-No.8 Availability and Capacity Management Procedure:** This procedure includes resource capacity monitoring and the implementation of necessary measures to maintain system reliability and meet operational demands. This process helps us minimize downtime, enhance system scalability, and provide a seamless experience for system users.

- **ISMS-SOP-No.9 Cryptography and Electronic Key Management Procedure:** This procedure outlines the principles and practices of securing sensitive information through encryption and proper key management. This procedure ensures confidentiality, integrity, and authenticity of data in electronic communications and in rest.

- **ISMS-SOP-No.10 Malware Protection Procedure:** The measures taken to safeguard systems and IT network from malicious software, known as malware. This includes real-time monitoring, malware scanning, and management of anti-malware software within Wilson James Ltd.

- **ISMS-SOP-No.11 Network Security Management Procedure:** This procedure outlines the steps and measures that are in place to protect IT infrastructure from unauthorized access, data breaches, and other potential security threats to ensure integrity, confidentiality, and availability of data and systems.

- **ISMS-SOP-No.12 Remote Working Procedure:** Ensures safety and protection of employees and sensitive information while working remotely. This involves the use of virtual private networks (VPNs), secure authentication mechanisms, and encryption technologies to safeguard sensitive information and prevent unauthorized access.

- **ISMS-SOP-No.13 Physical Security Management Procedure:** All employees have a part to play in the physical security of Wilson James offices and staff working areas, including individual offices, conference rooms and desks, and shall; maintain a clear desk; ensure that sensitive business information is secured and protected from unauthorised access or removal; lock their screen when away from the desk; and confirm that all visitors are booked in and always escorted.

- **ISMS-SOP-No.14 Information Systems Acquisition, Development, Testing & Maintenance Procedure:** To produce dependable information systems that meet business requirements and adequately protect information confidentiality, integrity and availability requires a sound approach for their acquisition, development, testing and maintenance.