

WILSON JAMES POLICY STATEMENT



Policy Title	Information Security	Policy No.	G26
Owner	Chief Information Officer	Date Issued	Jan-19
Author	Information Security and Compliance Manager	Date Reviewed	Jan-19
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

A handwritten signature in black ink, appearing to be 'Mark Dobson', with a long horizontal flourish extending to the right.

Chief Executive Officer

WILSON JAMES POLICY STATEMENT



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 ISO 27001 Certification process.

The purpose of the policy is to ensure that:

- Information assets¹ 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 process²;
- The integrity of this information is maintained³;
- Confidentiality of information is assured⁴;
- Regulatory and legislative requirements are met⁵;
- A Business Continuity Framework is implemented and Business Continuity plans produced, maintained and tested in order to counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters⁶;
- Information security education, awareness and training is available to staff⁷;
- All breaches of information security, actual or suspected, are reported to, and investigated by the ISMF and the Incident Response team⁸; and
- Appropriate access control maintained and information is protected against unauthorised access.
- Effectiveness and monitoring is in place to ensure continuous improvement⁹

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 unauthorised 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.

WILSON JAMES POLICY STATEMENT



ISMS Objectives

- To maintain our third party UKAS approval to the latest revision of the ISO27001 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 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.

- **Acceptable Use:** 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. The WJ Management Team shall familiarise themselves with the following procedure and ensure that all team members comply with this procedure at all times **Acceptable Use: ISMS-SOP-No.1.**
- **Change Management:** Should a change in procedures, systems, or configuration be required it must be approved before implementation. The WJ Management Team shall familiarise themselves with the following procedure and ensure that all team members comply with this procedure at all times **Change Management: ISMS-SOP-No.2.**

WILSON JAMES POLICY STATEMENT



- **Data Handling:** Wilson James holds a wide variety of data both internal and external. It is expected that all data will be created, gathered, stored, backed-up, accessed, transmitted and deleted in a secure, auditable and transparent manner in compliance with the relevant legislation. The WJ Management Team shall familiarise themselves with the following procedure and ensure that all team members comply with this procedure at all times **Data Handling: ISMS-SOP-No.3.**
- **Incident Management:** When an incident that affects information systems occurs, it is vital that this is immediately reported to enable effective corrective action to be taken. Such incidents may vary widely in nature from physical damage, to accidental loss, to software attacks. The WJ Management Team shall familiarise themselves with the following procedure and ensure that all team members comply with this procedure at all times **Incident Management: ISMS-SOP-No.4.**
- **Physical Security:** 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 escorted at all times. The WJ Management Team shall familiarise themselves with the following procedure and ensure that all team members comply with this procedure at all times **Physical Security: ISMS-SOP-No.5.**
- **Portable IT Devices:** Wilson James provides its employees with a variety of portable IT devices to use in the execution of their duties. These devices are valuable both in themselves and for the data and potential network access they contain. The Company expects its employees to use and secure such devices in a professional and business orientated manner. The WJ Management Team shall familiarise themselves with the following procedure and ensure that all team members comply with this procedure at all times **Portable IT Devices: ISMS-SOP-No.6.**
- **Protective Marking.** The protective marking of documentation is an important foundation of information security. Unless documents are correctly marked it is all too easy for confidential information to be inadvertently released to inappropriate parties. Wilson James expects all its employees to ensure documents are correctly marked as to their confidentiality and to ensure that documents are handled according to their protective marking. The WJ Management Team shall familiarise themselves with the following procedure and ensure that all team members comply with this procedure at all times **Protective Marking: ISMS-SOP-No.7.**
- **Information Systems Acquisition, Development, Testing & Maintenance:** 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. The WJ Management Team shall familiarise themselves with the following procedure and ensure that all team members comply with this procedure at all times **Information Systems Acquisition, Development, Testing & Maintenance: ISMS-SOP-No.8.**
- **Remote Working:** Remote Workers must be authorised by Wilson James IT and their Line Managers. Remote workers must comply with all WJ-ISMS policies at all times whilst working remotely. The WJ Management Team shall familiarise themselves with the following procedure and ensure that all team members comply with this procedure at all times **Remote Working: ISMS-SOP-No.9.**

WILSON JAMES POLICY STATEMENT



- **User Access Control:** 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. The WJ Management Team shall familiarise themselves with the following procedure and ensure that all team members comply with this procedure at all times: **User Access Control: ISMS-SOP-No.10.**
- **Risk Assessment:** To carry out robust risk assessments and reduce information security risks to an acceptable level. The WJ Management Team shall familiarise themselves with the following procedure and ensure that all team members comply with this procedure at all times **Risk Assessment: ISMS-SOP-No.11.**
- **ISMS Manual:** The Information Security Management System Manual confirms how WJ meets all requirements of the ISO 27001:2013 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.
- **ISTS - Technical Standards:** All IT personnel must carry out work in accordance with the Information Security Technical Standards.