



# Information security policy

Document control	
Version number	2.0
Owner	Richard Newham
Reviewer	Paul Bird
Last review date	31/01/2024

## Contents

Terms and definitions .....	3
1. Executive statement .....	3
2. Introduction.....	4
3. Purpose.....	4
4. Scope .....	4
5. Information security policy .....	5
5.1. Organisation.....	5
5.2. Policy structure .....	5
5.3. Policy audience .....	5
5.4. Roles and responsibilities.....	5
5.5. Information security governance .....	6
5.6. Special interests and authorities .....	6
5.7. Asset management.....	7
5.8. Information risk management.....	7
5.9. Information security management.....	7
5.10. Security assurance programme management .....	8
5.11. Improvement coordination .....	8
6. Exceptions .....	8
7. Violations .....	9
8. References .....	9
Appendix A: Terms and definitions .....	10

## Terms and definitions

The terms used within this document are located and described in [Appendix A](#) of this document.

### 1. Executive statement

Tilbury Douglas is a leading UK building, infrastructure, engineering and fit-out business, delivering vital projects across a range of sectors including health, education, highways, justice, defence, aviation, water and environment.

It is the intention of Tilbury Douglas that the Group Information Security Policy is implemented throughout our sphere of operations.

The purpose of this Policy is to protect Tilbury Douglas' information assets (including those entrusted to us by third parties), across all operations and functions, from all identified risks, whether internal or external, deliberate, or accidental; it will be subject to periodic review to ensure that it continues to meet the company's requirements.

The principal intention is to handle information appropriately and always in accordance with the applicable requirements related to information security.

To achieve this, Tilbury Douglas' information security objectives and commitments are to ensure that we:

- Maintain the confidentiality, integrity, and availability of information under our control.
- Protect the name and reputation of the company and that of our customers.
- Identify and appropriately manage business risks.
- Maintain compliance with relevant legal and regulatory requirements related to information security.
- Provide information security training to all staff.
- Report and investigate all information security incidents, actual or suspected.
- Strive to continually improve our information security management system.

The Policy applies to all Tilbury Douglas employees, contractual third parties and agents of the company who use the facilities and equipment, or have access to, or custody of, Tilbury Douglas or Client information. All managers are directly responsible for ensuring adherence by their staff.

This policy shall be communicated within the organisation and be available to interested parties as deemed appropriate.



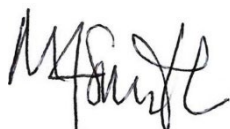
**Paul Gandy**  
Chief Executive Officer



**Craig Tatton**  
Chief Operating Officer



**Nick Pollard**  
Chair



**Martyn Smith**  
Commercial Director



**Matthew Gill**  
Chief Financial Officer

## 2. Introduction

The Head of Information Security under the direction of the Tilbury Douglas Senior Leadership Team (SLT) is responsible for the strategic and tactical deployment of a business wide information security management programme, and implementing the principles, frameworks and standards necessary for defending our organisation against all related threats.

## 3. Purpose

The purpose of this policy is to:

- Establish a business wide information security and data protection programme, which takes into account the internal and external issues relevant to its purpose and effectiveness and those that affect Tilbury Douglas' ability to achieve business outcomes.
- Establish, implement and maintain an ISMS to enable the delivery of the business' governance, risk and compliance controls. Controls will be administrative, physical and technological, the scope of which shall cover our facilities, people, processes and technology in the context of Tilbury Douglas' commercial, legal and regulatory environments.
- Establish authority, accountability and competence for managing information security and data protection at each 'business unit', including the management of operational risks. This includes implementing and maintaining the information risk management process and ensuring controls are adequate, effective, and efficient.
- Protect Tilbury Douglas 'assets' from risks associated with the theft, loss, misuse, damage or abuse whether intentional or unintentional.
- Preserve the following attributes of the organisations 'assets':
  - **Confidentiality** - Access to 'assets' shall be limited to those with appropriate authority.
  - **Integrity** – 'Information assets' shall be complete and accurate. 'Technology assets' shall operate correctly, according to specification.
  - **Availability** – 'Assets' shall be available to the right person, at the time when it is needed.
- Assess the output of controls to monitor their effectiveness, performance and for reporting, maturity, continual improvement and to inform management decisions.
- Ensure on-going commercial, legal and regulatory compliance.

## 4. Scope

The scope of this policy covers the facilities, people, processes and technology used by Tilbury Douglas and/or a 'business unit', in support of its operations and/or the provision of services. It also includes third party services that are provided to, for or on behalf of the 'Tilbury Douglas ' or a 'business unit'.

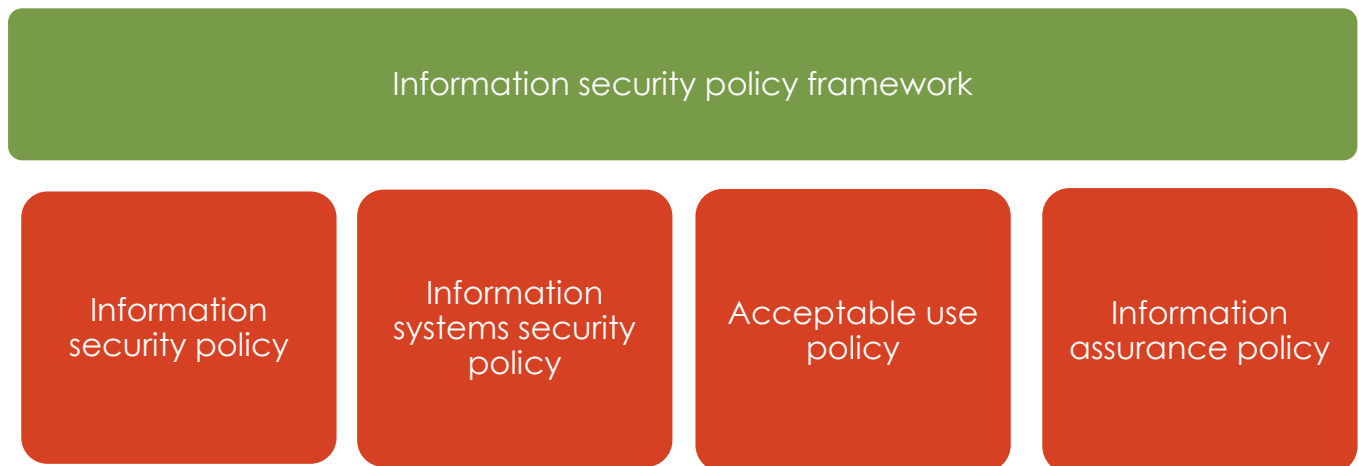
## 5. Information security policy

### 5.1. Organisation

- 5.1.1. Tilbury Douglas operates from multiple locations in the UK.
- 5.1.2. Tilbury Douglas or a 'business unit' may own or operate equipment that is located at other sites or supplier data centres. These sites and any equipment are considered in scope of this policy (see section 4).
- 5.1.3. High level organisation charts, describing operating and management structure.
- 5.1.4. Organisation charts, describing the functions, structure and reporting lines are maintained by each 'business unit'.

### 5.2. Policy structure

- 5.2.1. The information security policy is a key component of the ISMS as it establishes the framework for the effective management of information and privacy risks. This policy informs four sub-ordinate policies as defined below:



- 5.2.1. All technology is subject to the **information systems security policy**, which sets out the technical control requirements, frameworks and /or standards.
- 5.2.2. All 'users' are subject to the **acceptable use policy**, which sets out the requirements for using or interacting with the organisation's 'assets'. This can be accompanied by further guidance, for e.g. an employee handbook which describes the effective implementation of policy. There may also be other guidance documents referenced in, or in addition to, this for unique disciplines such as processing sensitive personal data or card holder data. All 'users' must read and comply with the requirements set out in this policy, associated guidelines and other referenced documents.
- 5.2.3. All business processes are subject to the **information assurance policy**, which sets out the control requirements for integrating information security and data protection.

### 5.3. Policy audience

- 5.3.1. Senior management, department managers, supervisors and team leaders across all 'business units' must read this information security policy.
- 5.3.2. Everyone must read the acceptable use policy.
- 5.3.3. Senior management, department managers, supervisors and team leaders across all 'business units' must read the information assurance policy.
- 5.3.4. All information technology staff must read the information systems security policy.

## 5.4. Roles and responsibilities

- 5.4.1. The information security team, its functions and responsibilities shall be set out and maintained in the operating model, which includes those across " " who are responsible, accountable, consulted and/or informed (RACI). The RACI shall be maintained and owned by the Head of Information Security.
- 5.4.2. The Head of Information Security shall maintain a RACI detailing the roles and responsibilities of the teams and team members of the Information Security Office in line with the ISMS controls and documentation.
- 5.4.3. Conflicting areas of responsibility must be segregated to reduce the risks of accidental or intentional misuse of the organisations 'assets'. Where segregation is not possible, increased audit and monitoring controls must be implemented; and,
- 5.4.4. SLT members who sign-off or accept an Information Security risk must not create a conflict of interest by signing-off or accepting a risk within their own area of responsibility; and,
- 5.4.5. Individuals, specifically those with elevated system and application privileges, must not have the capability to prevent, modify or erase audit log data.
- 5.4.6. The Head of Information Security will ensure the availability of necessary skills and competencies that person(s) must have, or must acquire, to effectively enable and support the ISMS.
- 5.4.7. Tilbury Douglas will support the development of any person(s) with accountability or responsibility for the ISMS through appropriate education, training and awareness, work experience, personal development and/or succession planning.
- 5.4.8. The Head of Information Security must ensure the continuity of information security operations by certifying that there is no reliance on a single person for critical functions within the ISMS.
- 5.4.9. Information security leads at each 'business unit' are responsible to ensure the continued and effective operation of the ISMS and for adhering to level reporting requirements.

## 5.5. Information security governance

- 5.5.1. The Board of Directors of 'Tilbury Douglas' bestow custodianship to information security.
- 5.5.2. The Head of Information Security is responsible for the Information Security Office, a strategic function with overall responsibility for the Tilbury Douglas information security operating model, and its governance, risk and compliance functions.
- 5.5.3. The Head of Information Security bestows custodianship for the tactical delivery and operational effectiveness of the ISMS to local 'business units' where practical to do so.
- 5.5.4. The ISMS shall be aligned with latest version of the ISO27001 standard, taking into account other controls as required through commercial, legal and regulatory interests and in response to incidents or emerging threats.
- 5.5.5. In support of 5.5.2, the Head of Information Security will issue policies and minimum standards to all 'business units'. The Head of Information Security is responsible for the effective delivery, enforcement and monitoring of these documents.
- 5.5.6. All planned information security expenditure must be approved by the Head of Information Security.
- 5.5.7. In support of 5.5.2, the IT Director will establish and chair a governing body known as the Solutions Committee. This body shall meet quarterly and the requirements for these meetings are defined in the Terms of Reference for that body.
- 5.5.8. The Head of Information security shall establish a governance body known as the Information Security Management Forum (ISMF), this will be attended by members of IT and the 'business' to provide tactical and operational oversight of the ISMS. The ISMF shall meet minimum of quarterly.
- 5.5.9. More frequent operational meetings can be scheduled if determined necessary by the Head of Information Security.

## 5.6. Special interests and authorities

- 5.6.1. The Head of Information Security shall maintain contact with special interest groups, professional forums and/or associations; and, shall subscribe to threat intelligence services and/or news bulletins to improve knowledge, stay current with best practice and to receive early warnings of attacks or vulnerabilities.
- 5.6.2. The Head of Information Security must maintain strict controls over external communications with external agencies including the authorities. This includes but is not limited to: regulators, press, media, news agencies, reporters, law enforcement, the courts, other legal or regulatory bodies). The Head of Information security must be informed of any communication relating to any misuse, abuse or breach of any ' ' security policy (see 5.2.1).

## 5.7. Asset management

- 5.7.1. All 'assets' must be identified, classified, labelled, recorded, owned (see 5.7.2) and controlled commensurate to the potential impact (see 5.8) resultant from attack, loss, theft, compromise or other damages arising from accidents, neglect or misuse.
- 5.7.2. A 'system owner', 'information risk owner', or for 'information assets', an 'information owner' must be defined for all 'assets' or logical assets as described in the Information Assurance Policy and the supporting information classification procedure.
- 5.7.3. All 'documented information' acquired, created, processed or stored for, or on behalf, 'Tilbury Douglas' or a 'business unit' must be controlled. Controls must include the identification, classification, review, approval, distribution and change control; and, must cover the life cycle of 'documented information' from acquisition or creation to retention and destruction.

## 5.8. Information risk management

- 5.8.1. The structure for Information Security Risk must be aligned to that of risk and the 'business unit' enterprise risk function, this includes but is not limited to, impact, likelihood, appetite, risk scoring, management and reporting requirements.
- 5.8.2. Information risk assessments must be performed in a structured manner to provide assurance that information risks are being consistently addressed. The process must include an assessment of the threats and vulnerabilities to 'assets' taking into account the impact of the risk and the likelihood of it occurring, the options for risk treatment and requirements for logging and reporting risk.
- 5.8.3. In accordance with the requirements above, the framework for Information Security Risk Management must be documented and aligned with Enterprise Risk.
- 5.8.4. Information risk assessments must be completed by all 'business units' following a common framework in order to consistently protect the 'assets', including the facilities and physical controls designed to protect them.
- 5.8.5. New and/or changes to existing 'assets' must be assessed. Owners must work with the Information Security Office to evaluate and treat risks to within acceptable limits.
- 5.8.6. Risks registers must be maintained and shall form part of management reporting. The Head of Information security shall provide reporting for information risks to the ISMF and/or risk committee in accordance with their Terms of Reference (ToR).
- 5.8.7. Where the 'information risk owner', 'data owner' and 'system owner' agree that a risk cannot be treated to within tolerable levels, or, requires risk acceptance, then a risk acceptance must be obtained, in writing, from the risk committee by completing a risk acceptance request form. Where the risk is associated with personal data then this also requires sign-off from the DPO.
- 5.8.8. **Important:** Only a member of the Risk Committee can sign off or accept an Information Security risk (see 5.4.4). All risk acceptance must be reported to the Head of Information Security and shall form part of ISMF reporting.

## 5.9. Information security management

- 5.9.1. Information security and data protection activities must be embedded into the business unit's functions, processes and technological controls to ensure that required security controls are maintained, with respect to risk (see 5.8) and that commercial, legal and regulatory requirements remain in a state of compliance.
- 5.9.2. The requirements for security in business processes shall be set out in the Information Assurance Policy and shall include but is not limited to: awareness & training; asset management, information security risk management, project management; change management; incident management; supply chain management; procurement; contractual management and business continuity management.
- 5.9.3. The requirements for the management of technology shall be set out in the Information Systems Security Policy and shall include but are not limited to: security architecture; cyber defence; identity and access management; end-point, application, network and systems management; electronic communications; cryptography; physical and environmental security; software development and acquisition; patch management; threat and vulnerability management; log management, alerting and reporting.

## 5.10. Security assurance programme management

- 5.10.1. The Head of Information security shall establish and maintain an information security assurance program to provide the senior management with an accurate, comprehensive and coherent assessment of the information security condition and maturity as a mechanism for confirming control(s) effectiveness, ISMS performance and the general health condition of each 'business unit'.
- 5.10.2. The security assurance program must comprise of information security controls derived from commercial, regulatory and legal drivers to ensure information security controls are consistently prioritised and addressed according to information security obligations associated with legislation, regulations, contracts, industry standards and organisational policies.
- 5.10.3. The security assurance program shall deliver the systematic; monitoring, measurement, analysis and evaluation of the ISMS, taking into account the person(s), business processes (see 5.9.2) and technology controls (see 5.9.3), throughout the organisation and its supply chain.
- 5.10.4. The Head of Information Security is responsible for determining the monitoring requirements, the methods utilised, the performance measurements and metrics including the identification of the person(s) or department(s) required to provide key metrics or data, including the reporting frequency, and; shall maintain a documented record of these activities as evidence of compliance. This shall be provided to the Head of information security based on level reporting requirements.
- 5.10.5. The Head of Information security working in conjunction with Internal Audit shall perform information assurance and control maturity assessments to determine the security condition of each 'business unit' and specific areas of the ISMS and related controls.

## 5.11. Improvement coordination

- 5.11.1. The results of the information security assurance program and independent reviews such as any external audits shall be reviewed by senior management to ensure continuing suitability, adequacy and effectiveness, and/or to drive continual improvement activities.
- 5.11.2. Improvements or non-conformities shall be prioritised by the and the Head of Information security based on the severity and/or impact to the business (see 5.8).
- 5.11.3. A full list of business as usual (BAU) or 'run' activities, including but not limited to the monitoring, measurement, analysis and evaluation of the information security condition of the organisation are included in the ISMF (see 5.5.7) Terms of Reference and the meeting template.
- 5.11.4. A full list of all information security management activities, including but not limited to the evaluation, review, decision making, unbudgeted expenditure, risk acceptance, non-conformities and improvement of the ISMS are included in the ITLT.



- 5.11.5. Records of actions and decisions arising from the ISMF including but not limited to: performance reviews, improvement activities; risk or policy exceptions; non-conformities; audit results; and/or organisational or threat assessments, must be retained as evidence and for onward reporting or compliance checks.
- 5.11.6. Records of Security Improvement Plans (SIP) and related activities performed at each 'business unit' must be maintained. These plans and activities must be ratified by the Head of Information security to ensure alignment across the organisation for reporting purposes.

## 6. Exceptions

Any applications for exceptions to this policy must be made in writing to the Head of Information Security at [it.security@tilburydouglas.co.uk](mailto:it.security@tilburydouglas.co.uk) with a completed exception form (available on the intranet for from the information security team). All requests will be considered by the Head of Information Security at the time of making and after completion of a risk assessment. Requests shall be reviewed thereafter on an agreed basis, but shall not exceed 12 months. Evidence must be retained of the exception granted and the authorisation for annual review.

## 7. Violations

Compliance with this policy and/or any subordinate policy is mandatory. The Head of Information Security will regularly assess compliance against this policy and sub-ordinate policies.

## 8. References

This document has the following references:

- Information Security Asset Management Standard
- Information Security Business Application Standard
- Information Security Third Party Access Standard
- Information Security Access Management Standard
- Information Security Network Management Standard
- Threat and Vulnerability Management Standard
- Information Security Incident Management Standard
- Information Security Electronic Communications Standard
- Information System Development Management Standard
- Information Security Risk Standard
- Information Security Mobile Standard

## Appendix A: Terms and definitions

<u>'Applications':</u>	collectively includes all 'end-point applications' and 'enterprise applications'.
<u>'Asset'</u>	collectively includes all 'information assets' and 'technology assets'.
<u>'Availability':</u>	is that information is accessible when it's needed.
<u>'Business unit'</u>	refers to a single business entity, namely, 'The Business units within the organisation, This includes all associated subsidiaries, trading or brand names relating to that business unit.
<u>'Confidentiality':</u>	is that information is not disclosed to individuals or systems that are not authorised to receive it.
<u>'Documented information':</u>	is the collective term used to describe the organisations documents and records (e.g. policies, procedures and printed materials) and the medium upon which they are stored (e.g. paper or electronic).
<u>'Employee' or 'Staff':</u>	is anyone employed by the organisation and operating under an employment contract, including but not limited to: full-time or part-time, contractors, sub-contractors, temporary or agency staff.
<u>'End user' or 'User':</u>	is anyone (excluding customers) who consumes services provided by, or behalf of, the " and has been issued access to any of the Business' 'networks', 'information systems', 'devices' or 'applications'.
<u>'The organisation' or 'Tilbury Douglas':</u>	Any Tilbury Douglas company including but not limited to Tilbury Douglas and Paragon.
<u>'Information owner':</u>	is the person with overall accountability for any 'information' which is generated or received by that business unit / department and its 'employees'. It is the SLT member with authority for that 'business unit' and its processes. Responsibility may be pushed to other tiers of management by the executive lead. The information owner is responsible for ensuring that 'information' generated or received by that department is appropriately classified and the appropriate level of information security safeguards are available and are applied. They are also responsible for ensuring that 'information' is shared and disseminated in accordance with policy and/or regulations
<u>'Information risk owner':</u>	is the senior most person (within the BU), outside of the Information Security Office) with the authority to assess the risk to an 'asset'. It may be the same person as the 'information owner' and/or the 'system owner'. The information risk owner is responsible for ensuring that risks are reported, assessed and controlled in accordance with the requirements set out in the information security risk and enterprise risk management frameworks.
<u>'Information system':</u>	is a logical grouping of hardware (e.g. 'information assets', 'networks', 'devices') and software components (for e.g. 'operating systems', 'applications', 'API's' or other 'software' components which are used for the purposes of storing, processing or transmitting the organisations 'information'. Examples of information systems includes the: finance system, remedy.
<u>'Information':</u>	is data that is (1) accurate and timely, (2) specific and organised for a purpose, (3) presented within a context that gives it meaning and relevance, and (4) can lead to an increase in understanding and decrease in uncertainty, and (5) has meaning to the organisation, customers, employees, end users or supply chain.

<u>'Integrity':</u>	is that information cannot be modified in an unauthorised manner.
<u>'Network' or 'Infrastructure':</u>	collectively includes all networking and telecommunications equipment providing enterprise-wide connectivity and enabling voice, data or integrated communications supporting one or more 'information systems' or inter-connected 'devices'.
<u>'Run':</u>	otherwise known as Business As Usual (BAU), refers to the performance and completion of routine operational activities in line with the organisations policies procedures and work instructions in order to achieve desired business outcomes is the SLT member with overall accountability for the 'information system' and the 'information' which it contains.
<u>'System owner'</u>	custodianship may be pushed to other tiers of management by the executive lead. The System Owner (also referred to as Information System Owner) is responsible for the overall procurement, development, integration, modification, operation, maintenance, and retirement of an information system. They are also responsible for controlling access to the system and its 'information' and for ensuring that appropriate safeguards are implemented in accordance with policy and the law, and controls remain effective throughout the systems life cycle.
<u>'Technology asset'</u>	Is any hardware or software in physical or electronic form that can be accessed, processed, stored or transmitted. Furthermore can be used for accessing, processing, storing or transmitting the organisations 'information assets'. This includes but is not limited to: 'physical ID', 'User ID', 'authentication token', 'devices', 'removable media', 'information assets', 'documented information', 'networks', 'servers', 'operating systems' or 'applications' including those operated for and/or on behalf of a 'business unit' or the Organisation".

## Version control

Author	Date Issued	Version No	Authorised
Scott Davies	27/02/2023	1.4	Paul Bird
Scott Davies	23/11/2023	2.0	Paul Bird