POLYGON INFORMATION SECURITY POLICY

Document Control

Document Storage

Document Title Information Security Policy
Document Location Intranet

Version History

Version No	Version Date	Author	Summary of Changes
1.0	10/01/2011	Andy Clark	First Issue
1.1	14/01/2013	Andy Clark	Updates for change of email system
1.2	01/04/2015	Andy Clark	Updates for off-site working
1.3	04/01/2016	Andy Clark	Annual review
1.4	07/02/2017	Andy Clark	Annual review
1.5	07/11/2017	Andy Clark	GDPR Review
1.6	24/12/2018	Andy Clark	Annual review
1.7	16/12/2019	Andy Clark	Annual review
1.8	11/01/2021	Andy Clark	Annual review
1.9	06/01/2022	Andy Clark	Annual review
2.0	09/01/2023	Andy Clark	Annual review
2.1	09/01/2024	Andy Clark	Annual review
2.2	09/01/2025	Andy Clark	Annual review

Approvals

Name	Title	Date of Approval	Version No
Andy Clark	IT Service Delivery Manager	09/01/2025	2.2

Distribution

Name	Title	Date of Issue	Version No
Everyone	Intranet	09/01/2025	2.2

Contents

1. Introduction

1.1. Information is an asset that the organisation has a duty and responsibility to protect. The availability of complete and accurate information is essential to the organisation functioning in an efficient manner and to providing products and services to customers.

1.2. The organisation holds and processes confidential and personal information on private individuals, employees, partners and suppliers and information relating to its own operations. In processing information, the organisation has a responsibility to safeguard information and prevent its misuse.

1.3. The purpose of this Information Security Policy is to set out a framework for the protection of the organisation's information assets:

- to protect the organisation's information from all threats, whether internal or external, deliberate or accidental,
- to enable secure information sharing,
- to encourage consistent and professional use of information,
- to ensure that everyone is clear about their roles in using and protecting information,
- to ensure business continuity and minimise business damage,
- to protect the organisation from legal liability and the inappropriate use of information.
- describing the principals of security and explaining how they shall be implemented in the organisation.
- introducing a consistent approach to security, ensuring that all members of staff fully understand their own responsibilities.
- creating and maintaining within the organisation a level of awareness of the need for Information Security as an integral part of the day-to-day business.

2. Scope

2.1. This Information Security Policy outlines the framework for management of Information Security within the organisation. For the avoidance of doubt, this policy includes all the Polygon companies and subsidiaries bought into the group from mergers and acquisitions.

2.2. The Information Security Policy, standards, processes and procedures apply to all staff and employees of the organisation, contractual third parties and agents of the organisation who have access to the organisation's information systems or information.

2.3. The Information Security Policy applies to all forms of information including but not limited to:

- speech, spoken face to face, or communicated by phone or radio,
- hard copy data printed or written on paper,
- information stored in manual filing systems,
- communications sent by post / courier, fax, electronic mail,
- stored and processed via servers, PC's, laptops, mobile phones, PDA's,
- stored on any type of removable media, CD's, DVD's, tape, USB memory sticks, digital cameras.
- Stored or processed by so called cloud providers.

3. Responsibilities for Information Security

2.4. Ultimate responsibility for information security rests with the Country President of Polygon, but on a day-to-day basis the Data Protection Officer shall be responsible for managing and implementing this policy and any related procedures.

2.5. Line Managers are responsible for ensuring that their permanent and temporary staff and contractors are aware of:

- The information security policies applicable in their work areas
- Their personal responsibilities for information security
- How to access advice on information security matters

2.6. All staff shall comply with information security procedures including the maintenance of data confidentiality and data integrity. Failure to do so may result in disciplinary action.

2.7. The Information Security Policy shall be maintained, reviewed and updated by the Data Protection Officer. This review shall take place at least annually and also if processes within the organization change in such a way that data may be compromised.

2.8. Line managers shall be individually responsible for the security of their physical environments where information is processed or stored.

2.9. Each member of staff shall be responsible for the operational security of the information systems they use.

2.10. Each system user shall comply with the security requirements that are currently in force, and shall also ensure that the confidentiality, integrity and availability of the information they use is maintained to the highest standard.

2.11. Contracts with external agents that allow access to the organisation's information systems shall be in operation before access is allowed. These contracts shall ensure that the staff or sub-contractors of the external organisation shall comply with all appropriate Polygon security policies.

3. Risks

3.1. Data and information which is collected, analysed, stored, communicated and reported upon may be subject to theft, misuse, loss and corruption.

3.2. Data and information may be put at risk by poor education and training, misuse, and the breach of security controls.

3.3. Information security incidents can give rise to embarrassment, financial loss, non-compliance with standards and legislation as well as possible judgements being made against the organisation.

3.4. The organisation will undertake risk assessments to identify, quantify, and prioritise risks. Controls will be selected and implemented to mitigate the risks identified.

3.5. Risk assessments will be undertaken using a systematic approach to identify and estimate the magnitude of the risks.

4. Organisation of Information Security

4.1. Statement of Management intent

4.1.1. It is the policy of the Organisation to ensure that Information will be protected from a loss of:

- Confidentiality: so that information is accessible only to authorised individuals.
- Integrity: safeguarding the accuracy and completeness of information and processing methods.
- Availability: that authorised users have access to relevant information when required.

4.1.2. The Data Protection Officer will review and make recommendations on the security policy, policy standards, directives, procedures, incident management and security awareness education.

4.1.3. Regulatory, legislative and contractual requirements will be incorporated into the Information Security Policy, processes and procedures.

4.1.4. The requirements of the Information Security Policy, processes, and procedures will be incorporated into the organisation's operational procedures and contractual arrangements.

4.1.5. The organisation will align to ISO27000 standards as its basis for information security.

4.1.6. Guidance will be provided on what constitutes an Information Security Incident.

4.1.7. All breaches of information security, actual or suspected, must be reported to line management and the IT Department, and will be investigated.

4.1.8. Business continuity plans will be produced, maintained and tested.

4.1.9. Information stored by the organisation will be appropriate to the business requirements.

5. Legislation

5.1. Polygon is obliged to abide by all relevant local legislation. The requirement to comply with this legislation shall be devolved to employees and agents of Polygon, who may be held personally accountable for any breaches of information security for which they may be held responsible. Polygon shall comply with the following legislation and other legislation as appropriate:

- The Data Protection Act (2018)
- The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) if for any reason data is processed in the EEA.
- The Data Protection (Processing of Sensitive Personal Data) Order 2000.
- The Copyright, Designs and Patents Act (1988)
- The Computer Misuse Act (1990)
- The Health and Safety at Work Act (1974)
- Human Rights Act (1998)
- Regulation of Investigatory Powers Act 2000
- The Privacy and Electronic Communications Regulations (PECR)

6. Information Security Coordination

6.1. The security of information will be managed within an approved framework through assigning roles and co-ordinating implementation of this security policy across the organisation and in its dealings with third parties.

6.2. Specialist external advice will be drawn upon where necessary to maintain the Information Security Policy, processes and procedures to address new and emerging threats and standards.

7. Information Security Responsibilities

10.1 The Data Protection Officer is the designated owner of the Information Security Policy and is responsible for the maintenance and review of the Information Security Policy, processes and procedures.

10.2 Heads of Department are responsible for ensuring that all staff and employees, contractual third parties and agents of the organisation are made aware of and comply with the Information Security Policy, processes and procedures.

10.3 The Organisation's auditors will review the adequacy of the controls that are implemented to protect the organisation's information and recommend improvements where deficiencies are found.

10.4 All staff and employees of Polygon, contractual third parties and agents of the Organisation accessing Polygon's information are required to adhere to the Information Security Policy, processes and procedures.

10.5 Failure to comply with the Information Security Policy processes and procedures may lead to disciplinary or remedial action.

8. Asset Management

8.1. The Organisation's assets will be appropriately protected.

8.2. All assets (data, information, software, computer and communications equipment, service utilities and people) will be accounted for and have an owner.

8.3. Owners will be identified for all assets, and they will be responsible for the maintenance and protection of their assets.

9. Human Resources Security

9.1. The Organisation's security policies will be communicated to all employees, contractors and third parties to ensure that they understand their responsibilities.

9.2. Security responsibilities will be included in job descriptions and in terms and conditions of employment.

9.3. Verification checks will be carried out on all new employees, contractors and third parties.

10. Physical and Environmental Security

10.1. Personal and Sensitive information processing facilities will be housed in secure areas where it is deemed appropriate by Heads of Department.

10.2. The secure areas will be protected by defined security perimeters with appropriate security barriers and entry controls.

10.3. Personal and Sensitive information will be physically protected from unauthorised access, damage and interference.

11. Communications and Operations Management

11.1. The Organisation will operate its information processing facilities securely.

11.2. Responsibilities and procedures for the management, operation and ongoing security and availability of all data and information processing facilities will be established.

11.3. Appropriate operating procedures will be put in place.

11.4. Segregation of duties will be implemented, where appropriate, to reduce the risk of negligent or deliberate system misuse.

12. Access Control

12.1. Access to all information will be controlled.

12.2. Access to information and information systems will be driven by business requirements. Access will be granted, or arrangements made for employees, partners, suppliers according to their role, only to a level that will allow them to carry out their duties.

12.3. A formal user registration and de-registration procedure will be implemented for access to all information systems and services.

13. Information Systems Acquisition, Development & Maintenance

13.1. The information security requirements will be defined during the development of business requirements for new information systems or changes to existing information systems.

13.2. Controls to mitigate any risks identified will be implemented where appropriate.

14. Information Security Incident Management

14.1. Information security incidents and vulnerabilities associated with information systems will be communicated in a timely manner. Appropriate corrective action will be taken.

14.2. Formal incident reporting and escalation will be implemented.

14.3. All employees, contractors and third-party users will be made aware of the procedures for reporting the different types of security incident, or vulnerability that might have an impact on the security of the organisation's assets.

14.4. Information security incidents and vulnerabilities will be reported as quickly as possible to line management and the IT Service Desk.

15. Business Continuity Management

15.1. The Organisation will put in place arrangements to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.

15.2. A business continuity management process will be implemented to minimise the impact on the Organisation and recover from loss of information assets. Critical business processes will be identified.

15.3. Business impact analysis will be undertaken of the consequences of disasters, security failures, loss of service, and lack of service availability.

16. Compliance

16.1. The organisation will abide by any law, statutory, regulatory or contractual obligations affecting its information systems.

16.2. The design, operation, use and management of information systems will comply with all statutory, regulatory and contractual security requirements.

17. Remote Working (e.g. home or mobile)

17.1. Any Polygon worker working remotely, will only access the Polygon network and applications via an approved method. The only exceptions to this are applications which have publicly facing access methods with the relevant controls in place which have been approved by Polygon IT Department.

17.2. All users must ensure that they maintain a clear desk policy so that personal or sensitive information is not exposed to non-authorized individuals.

17.3. In accordance with the Polygon HR Policy, only Polygon employees can use Polygon IT assets

18. General Policy Framework

18.1. Information Security Awareness Training

- Information security awareness training shall be included in the staff induction process.
- An ongoing awareness programme shall be established and maintained to ensure that staff awareness is refreshed and updated as necessary.

18.2. Contracts of Employment

- Staff security requirements shall be addressed at the recruitment stage and all contracts of employment shall contain a confidentiality clause.
- Information security expectations of staff shall be included within appropriate job definitions.

18.3. Computer Access Control

Access to computer facilities shall be restricted to authorised users who have business need to use the facilities.

18.4. Equipment Security

In order to minimise loss of, or damage to assets, equipment shall be physically protected from threats and environmental hazards.

18.5. Computer and Network Procedures

Management of computers and networks shall be controlled through standard documented procedures that have been authorised by the Polygon IT Department.

18.6. Information Risk Assessment

Once identified, information security risks shall be managed on a formal basis. They shall be recorded within a baseline risk register and action plans shall be put in place to effectively manage those risks. The risk register and all associated actions shall be reviewed at regular intervals. Any implemented information security arrangements shall also be a regularly reviewed feature of Polygon's risk management programme. These reviews shall help identify areas of continuing best practice and possible weakness, as well as potential risks that may have arisen since the last review was completed.

18.7. Classification of Information

Polygon shall implement appropriate information classifications controls, based upon the results of formal risk assessment.

18.8. Protection from Malicious Software

The organisation shall use software and hardware counter measures and management procedures to protect itself against malicious software. All staff shall be expected to co-operate fully with this policy. Users shall not install software on the organisation's assets without permission from the Data Protection Officer. Users breaching this requirement may be subject to disciplinary action.

18.9. User media

Removable media of all types that contain software or data from external sources, or that have been used on external equipment, require the approval of the Data Protection Officer before they may be used on Polygon's systems. Such media must also be fully virus checked before being used on the organisation's equipment. This media must also have sufficient security measures on it to ensure that unauthorised access to the data upon it is not possible. Users breaching this requirement may be subject to disciplinary action.

18.10. Monitoring System Access and Use

An audit trail of system access and data use by staff shall be maintained and reviewed on a regular basis.

Polygon has in place routines to regularly audit compliance with this and other policies. In addition, it reserves the right to monitor activity where it suspects that there has been a breach of policy. The Regulation of Investigatory Powers Act (2000) permits monitoring and recording of employees' electronic communications (including telephone communications) for the following reasons:

- Establishing the existence of facts
- Investigating or detecting unauthorised use of the system
- Preventing or detecting crime
- Ascertaining or demonstrating standards which are achieved or ought to be achieved by persons using the system (quality control and training)
- In the interests of national security
- Ascertaining compliance with regulatory or self-regulatory practices or procedures
- Ensuring the effective operation of the system.

Any monitoring will be undertaken in accordance with the above act and the Human Rights Act

18.11. Accreditation of Information Systems

The organisation shall ensure that all new information systems, applications and networks include a security plan and are approved by the Data Protection Officer before they commence operation.

18.12. System Change Control

Changes to information systems, applications or networks shall be reviewed and approved by the Data Protection Officer.

18.13. Intellectual Property Rights

The organisation shall ensure that all information products are properly licensed and approved by the Data Protection Officer. Users shall not install software on the organisation's assets without permission from the Data Protection Officer. Users breaching this requirement may be subject to disciplinary action.

18.14. Further Information

Further information and advice on this policy can be obtained from Data Protection Officer.