Pollitt
&
Partners

Information Security Policy

July 2022

Contents

List of Tables

1 Introduction

This document defines the information security policy of Pollitt and Partners.

Pollitt and Partners have an obligation and need to ensure that its business operates smoothly and without interruption for the benefit of its customers, shareholders and other stakeholders.

In order to provide such a level of continuous operation, Pollitt and Partners has implemented an Information Security Management System (ISMS) in line with the International Standard for Information Security, ISO/IEC 27001. This standard defines the requirements for an ISMS based on internationally-recognised best practice.

The operation of the ISMS has many benefits for the business, including:

- Assisting in winning new business by having the right standards in place to enable Pollitt and Partners to work with them.
- Compliance with legal and regulatory requirements including the GDPR
- Protection of IP, confidential and personal information
- Business continuity in the event of system failures, security breaches or disaster scenarios

Pollitt and Partners has decided to maintain full certification to ISO/IEC 27001 in order that the effective adoption of information security best practice may be validated by an independent third party, a Registered Certification Body (RCB).

This policy applies to all systems, staff and other third parties who have access to Pollitt and Partners systems.

The following supporting documents are relevant to this information security policy and provide additional information about how it is applied:

- Risk Assessment and Treatment Process
- Statement of Applicability
- Supplier Information Security Evaluation Process
- Internet Acceptable Use Policy
- Cloud Computing Policy
- Mobile Device Policy
- Remote Working Policy
- Access Control Policy
- User Access Management Process
- Cryptographic Policy
- Physical Security Policy
- Anti-Malware Policy
- Backup Policy
- Software Policy
- Technical Vulnerability Management Policy
- Network Security Policy
- Electronic Messaging Policy

— Secure Development Policy
— Information Security Policy for Supplier Relationships
— Availability Management Policy
— IP and Copyright Compliance Policy
— Records Retention and Protection Policy
— Privacy and Personal Data Protection Policy

Latest versions of these documents can be found in The Guide, there may be access restrictions to some of these documents so please contact either the CISO or FOD if access is required.

1.1 Information Security Requirements

A clear definition of Pollitt and Partners information security requirements will be agreed so that all ISMS activity is focussed on the fulfilment of those requirements. Statutory, regulatory and contractual requirements will also be documented and input to the planning process. Specific requirements with regard to the security of new or changed systems or services will be captured as part of the design stage of each project.

The controls within the ISMS will be driven by business needs and will be regularly communicated to all staff through team meetings, briefing documents and internal communications including email and notice boards.

1.2 Framework for Setting Objectives

Objectives for information security will be reviewed on annual basis at the same time as the annual IT review and budget planning cycle. These objectives will be based upon a clear understanding of the business requirements provided by the management team.

Information security objectives will be documented with details of how they will be achieved. These will be evaluated and monitored as part of management reviews to ensure that they remain valid. If amendments are required, these will be managed through the change management process.

Where appropriate and in accordance with ISO/IEC 27001 the reference controls detailed in Annex A of the standard will be applied to the ISMS. The risk assessment and treatment plans will be used to highlight controls for review. For details of which Annex A controls have been implemented and which have been excluded please see the *Statement of Applicability*.

In addition, enhanced and additional controls from the following code of practice will be adopted and implemented where appropriate:

— ISO/IEC 27002 – Code of practice for information security controls

The adoption of these codes of practice will provide additional assurance to our customers and help further with our compliance with international data protection legislation.

1.3 Continual Improvement of the ISMS

Pollitt and Partners policy with regard to continual improvement is to:

- Continually improve the effectiveness of the ISMS
- Enhance current processes to bring them into line with good practice as defined within ISO/IEC 27001 and related standards
- Achieve ISO/IEC 27001 certification and maintain it on an on-going basis
- Increase the level of proactivity across the businesses with regard to information security
- Review relevant metrics on an annual basis to assess whether it is appropriate to change them, based on collected historical data
- Obtain ideas for improvement via regular meetings and other forms of communication with interested parties.
- Review ideas for improvement at regular management meetings in order to prioritise and assess timescales and benefits

Ideas for improvements may be obtained from any source including employees, customers, suppliers, IT staff, risk assessments and service reports. Once identified they will be recorded and evaluated as part of management reviews.

1.4 Information Security Policy Areas

Pollitt & Partners defines policy in a wide variety of information security-related areas which are described in detail in a comprehensive set of policy documentation that accompanies this overarching information security policy.

Each of these policies is defined and agreed by one or more people with competence in the relevant area and, once formally approved, is communicated to an appropriate audience, both within and external to, the organization.

The table below shows the individual policies within the documentation set and summarises each policy's content and the target audience of interested parties.

Policy Title	Areas addressed	Target audience
Internet Acceptable Use Policy	Business use of the Internet, personal use of the Internet, Internet account management, security and monitoring and prohibited uses of the Internet service.	Users of the Internet service
Cloud Computing Policy	Due diligence, signup, setup, management and removal of cloud computing services.	Employees involved in the procurement and management of cloud services
Mobile Device Policy	Care and security of mobile devices such as laptops, tablets and smartphones, whether provided by the organization or the individual for business use.	Users of company-provided and BYOD (Bring Your Own Device) mobile devices
Remote Working Policy	Information security considerations in establishing and running remote workers sites and arrangement e.g. physical security, insurance and equipment	Management and employees involved in setting up and maintaining a remote workers site
Access Control Policy	User registration and deregistration, provision of access rights, external access, access reviews, password policy, user responsibilities and system and application access control.	Employees involved in setting up and managing access control
Cryptographic Policy	Risk assessment, technique selection, deployment, testing and review of cryptography, and key management	Employees involved in setting up and managing the use of cryptographic technology and techniques
Physical Security Policy	Secure areas, paper and equipment security and equipment lifecycle management	All employees
Anti-Malware Policy	Firewalls, anti-virus, spam filtering, software installation and scanning, vulnerability management, user awareness training, threat monitoring and alerts, technical reviews and malware incident management.	Employees responsible for protecting the organisation's infrastructure from malware
Backup Policy	Backup cycles, cloud backups, off-site storage, documentation, recovery testing and protection of storage media	Employees responsible for designing and implementing backup regimes
Software Policy	Purchasing software, software registration, installation and removal, in-house software development and use of software in the cloud.	All employees

Policy Title	Areas addressed	Target audience
Technical Vulnerability Management Policy	Vulnerability definition, sources of information, patches and updates, vulnerability assessment, hardening and awareness training.	Employees responsible for protecting the organisation's infrastructure from malware
Network Security Policy	Network security design, including network segregation, perimeter security, wireless networks and remote access; network security management, including roles and responsibilities, logging and monitoring and changes.	Employees responsible for designing, implementing and managing networks
Electronic Messaging Policy	Sending and receiving electronic messages, monitoring of electronic messaging facilities and use of email.	Users of electronic messaging facilities
Secure Development Policy	Business requirements specification, system design, development and testing and outsourced software development.	Employees responsible for designing, managing and writing code for bespoke software developments
Information Security Policy for Supplier Relationships	Due diligence, supplier agreements, monitoring and review of services, changes, disputes and end of contract.	Employees involved in setting up and managing supplier relationships
Availability Management Policy	Availability requirements and design, monitoring and reporting, non-availability, testing availability plans and managing changes.	Employees responsible for designing systems and managing service delivery
IP and Copyright Compliance Policy	Protection of intellectual property, the law, penalties and software license compliance.	All employees
Records Retention and Protection Policy	Retention period for specific record types, use of cryptography, media selection, record retrieval, destruction and review.	Employees responsible for creation and management of records
Privacy and Personal Data Protection Policy	Applicable data protection legislation, definitions and requirements.	Employees responsible for designing and managing systems using personal data

Table 1 - Set of policy documents

1.5 Application of Information Security Policy

The policy statements made in this document and in the set of supporting policies listed in Table 1 have been reviewed and approved by the senior management team and must be complied with. Failure by an employee to comply with these policies may result in disciplinary action being taken in accordance with the organisation's *Employee Disciplinary Process*.

Questions regarding any of P&P's policies should be addressed in the first instance to the Finance and Operations Director.