HybrIT Services

Information Security Statement

hybrIT services

Head Office & Service Centre: Building 3, Royal Ordnance Depot, Weedon Bec, Northamptonshire, NN7 4PS

Introduction

At HybrIT, we view Information security as a critical aspect of protecting organisational assets, ensuring business continuity, and safeguarding sensitive information from threats. Our Information Security Management Systems (ISMS), provides a comprehensive framework for establishing, implementing, maintaining, and continuously improving information security management and is certified to the ISO27001 standard. This document outlines an overview of key aspects of our ISMS, aligned with the organisation's information security objectives. We are committed to protecting the privacy and security of our customers' information. This policy outlines our practices for safeguarding customer data.

Purpose and Scope

The primary purpose of aligning with ISO 27001 is to mitigate information security risks, protect the confidentiality, integrity, and availability (CIA) of data, and comply with legal and regulatory requirements. This standard applies to all information systems, business processes, and personnel involved in managing and protecting organisational and customer data, whether it is stored, processed, or transmitted.

Key Components of the HybrIT Information Security Management System

Risk Management

A core aspect of ISO 27001 is a risk-based approach. HybrIT conduct a thorough risk assessment to identify information security risks that could impact business operations or data assets. This assessment involves:

- Identifying assets, vulnerabilities, and threats.
- Evaluating the impact and likelihood of potential risks.
- Prioritising risks based on business impact This process leads to the creation of a risk treatment plan that implements appropriate controls to reduce or eliminate the risks.

Information Security Policies

ISO 27001 mandates the development of a comprehensive set of security policies that guide the organisation's approach to information security. Key policies include:

- Access control policy: Ensures that only authorized individuals have access to critical systems and data.
- Data classification policy: Classifies information based on sensitivity to ensure proper handling and protection.
- Incident response policy: Establishes procedures for managing and responding to security incidents to minimise damage.

Leadership Commitment

HybrIT executive leadership plays a crucial role in driving the success of the ISMS. Executive management must demonstrate their commitment by:

- Defining the information security objectives aligned with business goals.
- Allocating resources to support the ISMS.
- Ensuring that roles and responsibilities related to information security are well-defined.

Asset Management

Effective management of information assets is critical. ISO 27001 emphasises the identification, classification, and management of assets to ensure appropriate levels of protection. This includes hardware, software, data, and intellectual property.

Legal and Regulatory Compliance

ISO 27001 ensures compliance with all relevant legal and regulatory requirements. HybrIT identify applicable laws and regulations related to information security (such as GDPR, DPA) and implement controls to ensure ongoing compliance.

Tel: 0333 0156 701 Email: hello@hybrit.co.uk

Continuous Improvement and Monitoring

Continuous monitoring and regular auditing are vital components of the ISMS. This includes:

- Internal audits to assess the effectiveness of the ISMS and identify areas for improvement.
- Regular reviews of security incidents, performance metrics, and audit results.
- Implementation of corrective and preventive actions to address any identified weaknesses.

Key Benefits of ISO 27001 Certification

- **Enhanced Risk Management:** ISO 27001 helps to systematically address information security risks, minimising the chances of security breaches.
- **Reputation and Trust:** Achieving ISO 27001 certification demonstrates a commitment to security, which strengthens the trust of customers, partners, and stakeholders.
- **Regulatory Compliance:** Aligning with ISO 27001 ensures that the organisation meets relevant legal and regulatory obligations.
- **Operational Efficiency:** By following a structured framework for managing information security, the HybrIT can streamline processes, reduce inefficiencies, and prevent security incidents.

Customer Rights

Customers have the right to access, correct, or delete their personal data in alignment with GDPR. Requests can be made through hello@hybrit.co.uk and once validated will be actioned.

Contact Information

For any questions or concerns about our information security practices and specifically our ISO controls, please contact us at hello@hybrit.co.uk.