Information Security Policy

Document reference	CIV-IMS-01
Date	2222/01/2025
Document author	Nathan Davies
Document owner	Tony Summers

Revision history

Version	Date	Revision author	Summary of changes
0.1	14/01/2025	Rob Pragnell	Initial Draft
0.2	15/01/2025	Nathan Davies	Final Draft
1.0	17/01/2025	Nathan Davies	Published
1.1	22/01/2025	Nathan Davies	Corrected Owner

Contents

1. Introduction

This document defines the information security policy of Civiteq.

As a modern, forward-looking business, Civiteq Senior Management recognises the need to ensure that we operate securely, smoothly and without interruption for the benefit of our Customers, Partners, Stakeholders and Shareholders.

To meet this aim, Civiteq has implemented an Integrated Management System (IMS) in line with the Internation Standard for Information Security, ISO/IEC 27001. This standard sets out the requirements for an IMS based on internationally recognised best practice.

Civiteq 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).

Civiteq uses the ISMS.online platform as their preferred location to manage the IMS.

2. Information Security Policy

2.1. Information security requirements

A clear definition of the requirements for information security within Civiteq will be agreed and maintained to ensure all IMS activity is focussed on the fulfilment of those requirements. The IMS will also document and take account of Statutory, Regulatory and Contractual requirements. Specific security requirements for new or changed systems and processes shall be considered and captured in the early stages of each project.

It is a fundamental principle of the Civiteq Integrated Management System that the controls implemented are driven by best practice, business needs and without placing an unnecessary administrative burden on our teams. This will be regularly communicated to all Colleagues.

2.2. Framework for setting objectives

A regular cycle will be used for the setting of objectives for information security. These objectives will be based upon a clear understanding of the business requirements, informed by the management review process during which the views of relevant interested parties may be obtained.

Information security objectives will be documented, together 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.

2.3. Continual improvement of the IMS

Civiteq's policy regarding continual improvement is to:

- Continually improve the effectiveness of the IMS

- 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
- 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.

2.4. Information security policy areas

Civiteq defines policy in a wide variety of information security-related areas which are described in detail within the Management System that accompanies this overarching Information Security Policy.

Each of the clauses and controls within the Management System is defined and agreed by one or more people with competence in the relevant area and formally approved.

2.5. Application of Information Security Policy

The IMS will satisfy applicable requirements related to information security, which are captured via the clauses and controls, and ensure continual improvement (section 2.3).

This policy applies to all systems, people and processes that constitute the organization's information systems, including board members, directors, employees, suppliers and other third parties who have access to Civiteq systems.