

## 1 Purpose and Scope

### 1.1 Purpose

This information security policy statement defines the commitment made by Modern Networks to meet, and where possible exceed, the requirements of ISO 27001:2013. It also sets out our commitment to upholding information security best practice across our UK domain.

### 1.2 Scope

This policy sets out the responsibilities and requirements for implementing an IMS in relation to information security management and the requirements of ISO 27001:2013 within Modern Networks Limited. Modern Networks information security policy applies to all staff and all workplaces, events, situations, tasks, buildings, equipment, methods and products used in carrying out the company's activities.

## 2 Policy Statement

The Modern Networks leadership team recognise the importance of securing our clients' and our own information. We aim to maintain the highest standard of confidentiality, integrity and availability of internal, customer and supplier information. We have implemented an Integrated Management System (IMS) that includes governance of information security, to protect our information assets from all threats, whether internal or external, deliberate or accidental.

Information security is controlled through the preservation of:

- **Confidentiality:** ensuring that information is accessible only to those authorised to have access
- **Integrity:** safeguarding the accuracy and completeness of information and processing methods
- **Availability:** ensuring that authorised users have access to information and associated assets.

Client and corporate information are critical business assets. These assets are identified and managed in accordance with the risk assessment methodology that endorses the acceptable risk levels. The success of Modern Networks business is dependent upon the company's ability to store information securely and retrieve and process it as and when required. Such information and the way it may be processed is subject to applicable legislation and contractual requirements.

Our information security policy is achieved and implemented through a stringent set of controls, including policies, processes, procedures and software and hardware functions. These controls are continuously monitored, reviewed, improved, and approved by Modern Networks Senior Management to ensure that specific security and business objectives are met.

A robust system is in place to continually improve the security controls to:-

- Take account of changes to business requirements and priorities
- Consider new threat and vulnerabilities
- Confirm that controls remain highly effective and appropriate

The overall effectiveness of the IMS is reviewed via a formal Management Review process. This strategic review is conducted with representation and approval from the Senior Management Team.

# Modern Networks Information Security Policy

Security awareness is incorporated in our induction process and training program and our policy is readily accessible internally and presented to existing and prospective clients upon request.

In addition to employees, Modern Networks suppliers, contractors and sub-contractors are required to adhere to our policy. All employees are empowered to take responsibility for information security and a robust process for identifying and reporting security risks and incidents is in place and is regularly reviewed.

Modern Networks has committed staff and resources to comply with applicable requirements and continually strives to improve the effectiveness of the integrated management system (IMS). Personnel are required to adopt and comply with all controls implemented to achieve and exceed these policy objectives.

Through maintaining our certification to ISO27001, and on-going compliance to regulatory, legal and contractual requirements, Modern Networks will demonstrate confidence, integrity and credibility both internally and externally to our Integrated Management System.

## 3 Compliance with Policy

In order to comply with this policy and to ensure its key objectives are met, Modern Networks will:

- Ensure policies and accompanying processes are aligned with this overarching policy
- Ensure all staff are made aware of this policy through inductions and training
- Put in place appropriate and processes to enable adherence to this policy
- Review on an annual basis adherence, efficiency and effectiveness of this policy.

## 4 Roles & Responsibilities

Role	Responsibility
The Senior Management Team	Is responsible at an executive level for ensuring that appropriate provisions are in place in order for the policy to be implemented and embedded in practice.
The IMS Team	Is responsible to ensure that: <ul style="list-style-type: none"><li>• This policy is reviewed at least once annually to ensure its continued suitability and effectiveness.</li><li>• Opportunities for improvement are identified and implemented.</li></ul>
Heads of Departments and Line Managers	Are responsible for ensuring staff members are aware of their responsibilities under this policy and any relevant supporting processes
All members of staff	Are responsible for reading, understanding, and following this policy and any relevant supporting processes.

## 5 Document Information

<b>Document Author:</b>	Devi Kroll
<b>Document Owner:</b>	Matthew Reeve - CEO
<b>Document Classification:</b>	Public

## 6 Amendment Record/Document Control

This document is reviewed to ensure its continuing relevance to the systems and process that it describes. A record of is given below:

Author	Context	Version	Approval Date
Rachel Churchman	Initial Draft	0.1	
Rachel Churchman	Final approved following review	1.0	18 January 2022

## 7 IMS Document Review

It is the policy of Modern networks to review all policies at least annually. The review will be recorded and if changes are required a new major or minor version of the document will be issued.

Review Date	Reviewer(s)	Review Notes	Next Review Date
22- May 2023	Devi Kroll, Geraint Williams	Version 1.0 Document reviewed. No changes required.	May 2024

## 8 Approvals

Date	Name and Signature	Position
18/01/22	Matthew Reeve	CEO