



Information Security Management System (ISMS) Policy

INTERNAL USE ONLY

Version
1.1

DOCUMENT CONTROL

Document Information

Document Title	Information Security Management Policy
Version	1.1
Publication Date	1 November 2017
Status	Approved
Review Date	24 January 2024

Revision History

Version	Date	Author/Reviewer	Details
1.0	1 November 2017	Q.Sheikh	Initial Release
1.0	06 January 2020	J Holmes	Reviewed
1.0	06 January 2021	Q.Sheikh	Reviewed
1.0	06 January 2022	Q.Sheikh	Reviewed
1.1	24 January 2023	Q.Sheikh	Reviewed

Distribution

Name	Position	Organisation

Classification

PROTECT - INTERNAL

Legal Notice

This document may contain valuable trade secrets and confidential information of VISAV Ltd, and shall not be disclosed to any person, organisation, or entity unless such disclosure is subject to the provisions of a written non-disclosure and proprietary rights agreement or intellectual property license agreement approved by VISAV Ltd

Contents

INTERNAL USE ONLY.....	0
DOCUMENT CONTROL.....	1
DOCUMENT INFORMATION	1
REVISION HISTORY	1
CLASSIFICATION	1
LEGAL NOTICE	1
1 INTRODUCTION.....	3
2 PURPOSE.....	3
3 SCOPE.....	3

1 Introduction

VISAV Ltd provides essential services and functions which rely on resources including information. The use of information assets must be in line with good professional working practices and procedures as well as statutory, regulatory and contractual requirements and must ensure the confidentiality, integrity and availability of all information assets.

Information is an extremely important business asset and enables the company to fulfil its business functions and obligations to customers. ISO/IEC 27001:2013, the international security standard for information security management systems provides mandatory requirements for implementing, reviewing and continuously improving an Information Security Management System (ISMS).

VISAV Ltd's ISMS shall ensure the company meets its statutory, regulatory and contractual information security requirements including those provided by the Data Protection Act (1998) and the Information Commissioner's Office (ICO). The ICO is the UK's independent authority established to uphold information rights in the public interest, promoting openness by public bodies and data privacy and security for individuals. Some external partners are only willing to deal with other partner agencies which adhere to high information security standards and this increasingly means achieving and maintaining ISO 27001 compliance.

VISAV Ltd Scope Statement: -

"The Information Security Management System (ISMS) applies to the control of VISAV Ltd's business, premises and resources."

2 Purpose

This policy defines the ISMS policy in terms of the characteristics of the business, the organisation and its assets. It establishes VISAV Ltd's principles, ambitions and objectives when utilising a management system for information security.

3 Scope

The scope of this policy extends to all VISAV Ltd's departments, employees, contractors, vendors and partner agencies who use/access the company's information assets.

4 Policy statement

- The Security and Infrastructure Director is charged with the management and approval of functions associated with the ISMS.
- The Security and Infrastructure Director is charged with establishing and continually improving the ISMS.
- The Security and Infrastructure Director will provide the framework for setting objectives and will establish an overall sense of direction of principles for action with regard to security.
- The ISMS will take into account business and legal or regulatory requirements and contractual security obligations.
- The approach to information security will be based on risk, as per the ISO 27001 standard and best practice.

- The creation of the ISMS will include listing all information assets and the security risks that may arise for each. The resultant information will inform the Managing Director and Security and Infrastructure Director of prospective mitigation priorities.
- This ISMS policy covers all policies and procedures material to the Information Security Policy.
- The Security and Infrastructure Director will periodically review the company's current practices, policies and guidance and recommend any changes or improvements to ensure we apply appropriate security measures.