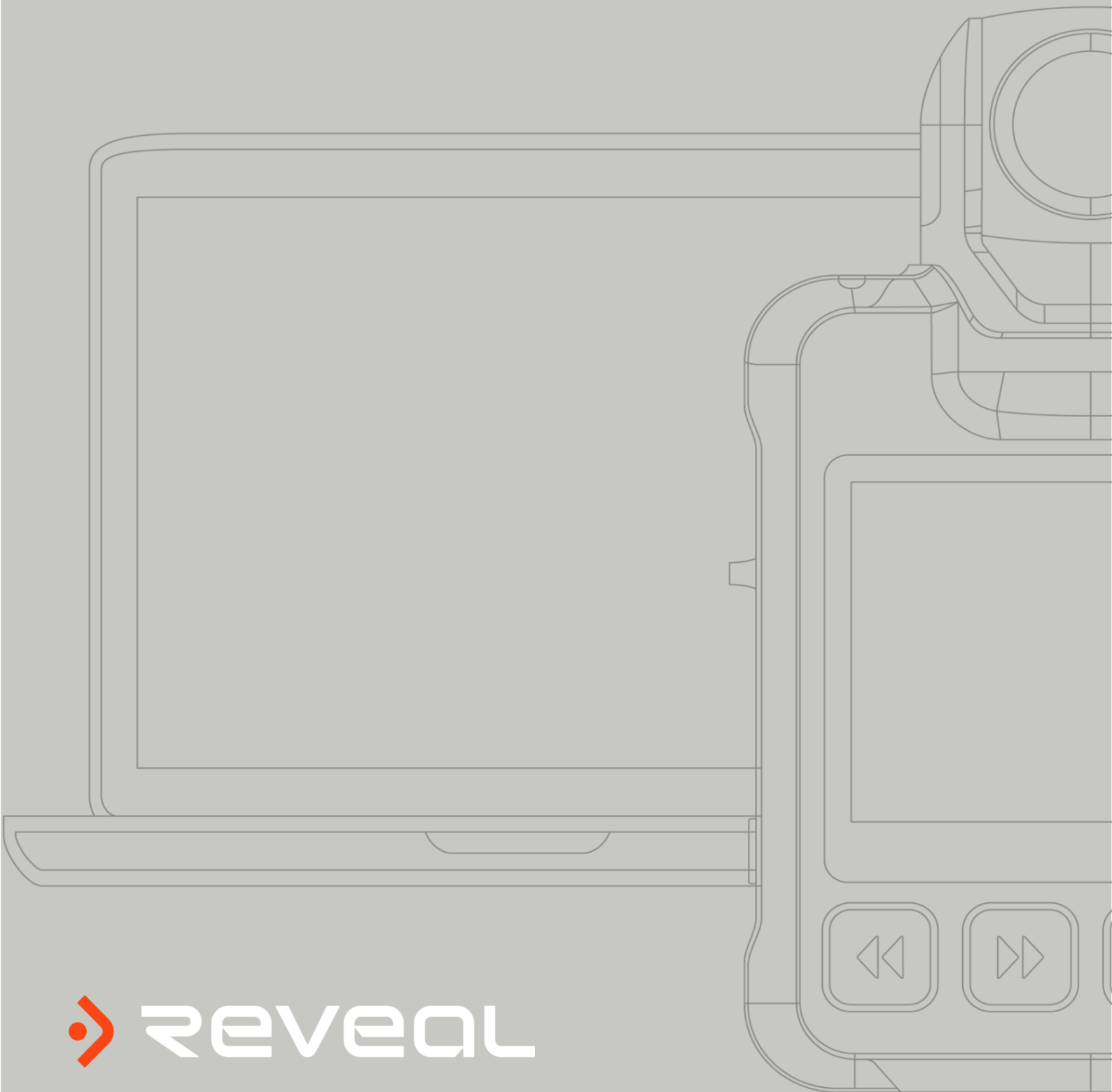


Information Security Policy



Information Security Policy

Description	Information Security Policy
Initial Issue Date	1 July 2024
Author/Owner	Guy Peverell
Classification	Public -Internal-Internal restricted-Confidential
Document Ref.	L-IMS-502-V1-GAP-Quality Policy-PUB

Document History

Version	Date	Change Notes	Author
0.9	01/05/2023	Initial draft	Guy Peverell
1.0	01/07/2024	The original ISMS policy has been reviewed and re-written to reflect the move to an Integrated Management System and the transition to ISO 27001 2022.	Guy Peverell
1.0	17/11/2025	Reviewed no change	Guy Peverell

Approval History

Version:	1.0	1.0								
Author:	GAP	GAP								
Reviewed by:	IMC	IMC								
Approved by:	IMC	LC								

This document is uncontrolled when printed. Before use, please verify that this is the current version.

Intellectual Property and Confidentiality Notice: Unless otherwise agreed in writing all copyright and intellectual property rights embodied in this document are and shall remain the property of Reveal Media Ltd. The information contained herein is the property of Reveal Media Ltd and is supplied without liability for errors or omissions. The information supplied herein is provided solely for the intended purpose and no other rights whatsoever to use such information are granted. The contents of this document are confidential information and must not be disclosed to any third party without the written consent of Reveal Media Ltd. No part may be reproduced or used except as authorised in writing by Reveal Media Ltd. The copyright and the foregoing restriction on reproduction and use extend to all media in which the information may be embodied.

Statement

The Board of Directors of Reveal Media Ltd. approves and directs the following policy.

All employees of Reveal Media Ltd. are required to comply with this policy and take individual responsibility for the achievement of the policy aims by complying with the information security policies, procedures, and instructions which extend from it, and by promptly completing all related training provided by the company.

The Board and Management of Reveal Media Ltd. are committed to preserving the confidentiality, integrity, and availability (known as CIA) of the physical and electronic information assets throughout the organisation to maintain customer confidence, commercial image, legal and regulatory compliance, contractual compliance, and profitability.

Reveal Media Ltd. will operate an Integrated Management System (IMS) which incorporates our Information Security Management System (ISMS), in order to reduce to an acceptable level, risks associated with the processing of data regardless of format.

Reveal Media Ltd.'s current strategic business plan and risk management framework provide the context for identifying, assessing, evaluating and controlling information-related risks through establishing and maintaining an integrated ISMS. Information and information security requirements will continue to be aligned with Reveal Media Ltd.'s goals.

The Risk Assessment and Risk Treatment Plan identify how information-related risks shall be controlled. The ISO Manager is responsible for managing and maintaining the risk treatment plan. Additional risk assessments may, where necessary, be carried out to determine appropriate controls for specific risks. The Statement of Applicability identifies which controls have been implemented.

Business continuity and contingency plans, data backup procedures, anti-malware systems, access control to systems, and information security incident reporting shall remain fundamental to this policy.

SMART objectives which support the continual improvement of our IMS are contained within 'Objectives and opportunities' document which is regularly reviewed at our Management System Review meeting and subsequently communicated.

Reveal Media Ltd are committed to meeting and exceeding the requirements of ISO/IEC 27001:2022 and maintaining certification through a UKAS approved certification body.

This policy will be regularly reviewed to respond to any changes impacting the IMS.