Meridian Software Ltd

ISO 27001:2022 Information Security Management System

Policy Documentation

Version 1 — Initial certification

Export 1

Generated 2 August 2026

DOCUMENT CONTROL

Version	Date	Approved by	Summary of changes
1	14 July 2026	Sarah Chen, Chief Information Security Officer	Initial certification

5.x — Organisational

ISO 27001:2022 · 5.1

Policies for information security

Meridian Software Ltd maintains a formal information security policy approved by senior management and reviewed annually. The policy establishes the organisation's commitment to protecting information assets in accordance with ISO/IEC 27001:2022 and applicable legal requirements. All staff are required to read and acknowledge the policy upon joining and following each annual review.

v1 · Approved by Sarah Chen (Chief Information Security Officer) · 14 July 2026

ISO 27001:2022 · 5.2

Information security roles and responsibilities

Meridian Software Ltd designates the Chief Information Security Officer as the owner of the information security management system. Individual responsibilities for protecting company and customer information assets are defined in role-specific security responsibility matrices and included in job descriptions. The CISO reports directly to the CEO and is empowered to escalate security concerns to the board.

v1 · Approved by Sarah Chen (Chief Information Security Officer) · 14 July 2026

ISO 27001:2022 · 5.15

Access control

Access to Meridian Software Ltd's information systems and data is granted on the basis of business need and the principle of least privilege. All access rights are provisioned through Okta and reviewed quarterly by system owners. Access to production environments is restricted to engineers with a documented business justification and is subject to approval by the Engineering Director.

v1 · Approved by Sarah Chen (Chief Information Security Officer) · 14 July 2026

ISO 27001:2022 · 5.16

Identity management

All user identities within Meridian Software Ltd are managed centrally through Okta. Identities are created, modified and deactivated through a documented joiner-mover-leaver process owned by HR and executed within one business day of the triggering event. Generic or shared accounts are prohibited; every identity is attributable to a named individual.

v1 · Approved by Sarah Chen (Chief Information Security Officer) · 14 July 2026

ISO 27001:2022 · 5.31

Legal, statutory and regulatory requirements

Meridian Software Ltd identifies and documents all relevant legal, statutory, regulatory and contractual requirements relating to information security. These include UK GDPR, the Computer Misuse Act 1990, and data-processing obligations set out in customer agreements. Compliance with these requirements is reviewed annually by the CISO with input from legal counsel.

v1 · Approved by Sarah Chen (Chief Information Security Officer) · 14 July 2026

6.x — People

ISO 27001:2022 · 6.1

Screening

Background checks are conducted for all employees and contractors with access to sensitive information or production systems prior to commencement of employment. Checks include verification of identity, right to work in the UK, employment history and professional references. Where a role involves access to financial systems or customer data, an enhanced DBS check is also required.

v1 · Approved by Sarah Chen (Chief Information Security Officer) · 14 July 2026

ISO 27001:2022 · 6.3

Information security awareness, education and training

All Meridian Software Ltd employees complete information security awareness training within their first two weeks of employment and annually thereafter. The training programme covers phishing recognition, password hygiene, acceptable use of company devices and incident reporting procedures. Completion rates are tracked by HR and reported to the CISO quarterly.

v1 · Approved by Sarah Chen (Chief Information Security Officer) · 14 July 2026

ISO 27001:2022 · 6.7

Remote working

Meridian Software Ltd operates a remote-first working policy and has implemented controls commensurate with the associated risks. All remote workers must connect to company systems via a VPN, use company-issued encrypted devices and ensure their home working environment is not overlooked by unauthorised individuals during sensitive calls. Remote access credentials are managed through Okta with phishing-resistant MFA enforced.

v1 · Approved by Sarah Chen (Chief Information Security Officer) · 14 July 2026

7.x — Physical

ISO 27001:2022 · 7.1

Physical security perimeters

Meridian Software Ltd's primary office premises are secured with access-card entry systems, CCTV coverage of common areas and a staffed reception during business hours. Production infrastructure is hosted in AWS data centres that operate under ISO 27001 and SOC 2 certifications, with physical access controls managed by AWS. Physical access to the company's offices is reviewed and updated by the Office Manager when employment changes occur.

v1 · Approved by Sarah Chen (Chief Information Security Officer) · 14 July 2026

ISO 27001:2022 · 7.7

Clear desk and clear screen

Meridian Software Ltd requires all employees to clear their desks of sensitive materials at the end of each working day and when leaving their workstation unattended. All computers are configured to lock automatically after five minutes of inactivity. Printed documents containing personal data or confidential business information must be stored in locked drawers or shredded when no longer required.

v1 · Approved by Sarah Chen (Chief Information Security Officer) · 14 July 2026

8.x — Technological

ISO 27001:2022 · 8.1

User end point devices

All user endpoint devices used to access Meridian Software Ltd systems are enrolled in the company's mobile device management solution. Devices must have full-disk encryption enabled, endpoint protection software installed and automatic OS updates configured. Personal devices are not permitted to access production systems or customer data.

v1 · Approved by Sarah Chen (Chief Information Security Officer) · 14 July 2026

ISO 27001:2022 · 8.2

Privileged access rights

Privileged access to Meridian Software Ltd's infrastructure and production systems is granted only to engineers with a documented operational requirement. Privileged accounts are managed separately from standard user accounts, are subject to mandatory multi-factor authentication and their use is logged and reviewed monthly. Shared or generic privileged accounts are prohibited; all privileged access is attributable to a named individual.

v1 · Approved by Sarah Chen (Chief Information Security Officer) · 14 July 2026

ISO 27001:2022 · 8.5

Secure authentication

Multi-factor authentication is mandatory for all access to Meridian Software Ltd's systems, including cloud infrastructure, version control and internal applications. Authentication is managed via Okta, with phishing-resistant FIDO2 authenticators required for access to production environments and administrative consoles. Password policies enforce a minimum length of 16 characters and reuse is prohibited.

v1 · Approved by Sarah Chen (Chief Information Security Officer) · 14 July 2026

ISO 27001:2022 · 8.7

Protection against malware

Meridian Software Ltd deploys endpoint detection and response software on all company-managed devices. Email filtering is configured to scan attachments and links for malicious content before delivery. A formal process exists for escalating and responding to suspected malware incidents within two hours of detection, with staff trained to identify and report suspicious communications.

v1 · Approved by Sarah Chen (Chief Information Security Officer) · 14 July 2026

ISO 27001:2022 · 8.8

Management of technical vulnerabilities

Meridian Software Ltd operates a vulnerability management programme including automated scanning of infrastructure and application dependencies on each code commit and weekly for production systems. Critical vulnerabilities are remediated within five business days; high-severity vulnerabilities within fifteen. The Engineering Director tracks open vulnerabilities and reports status to the CISO monthly.

v1 · Approved by Sarah Chen (Chief Information Security Officer) · 14 July 2026

ISO 27001:2022 · 8.13

Information backup

Meridian Software Ltd's production database and application configuration data are backed up daily to a separate AWS region. Backup integrity is verified through automated restore tests conducted monthly. The Recovery Point Objective is 24 hours and the Recovery Time Objective is four hours; these targets are validated as part of the annual business continuity exercise.

v1 · Approved by Sarah Chen (Chief Information Security Officer) · 14 July 2026