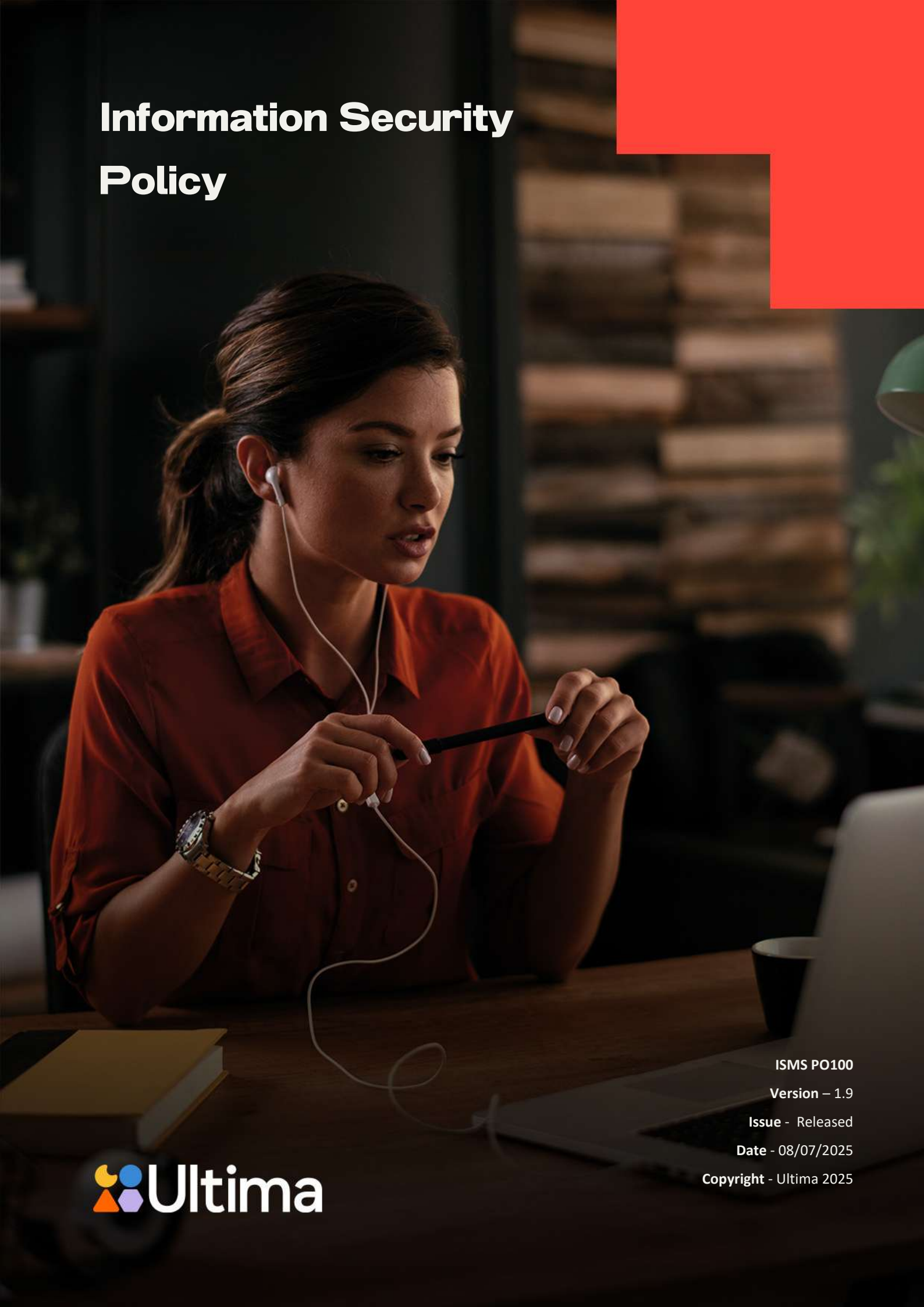
Information Security Policy



ISMS PO100

Version – 1.9

Issue - Released

Date - 08/07/2025

Ultima

CONTENTS

1.0 Purpose

Define the requirements of *Ultima*[1] in relation to its policy for information security. This *Information Security Policy* establishes Ultima's requirements for achieving an effective and appropriate system of control measures to protect the Company's business activities, information assets and internal/external information processing facilities. The selected measures shall be:

- Based on the risks identified through a formal, business focussed assessment process.
- Cost effective and justifiable commercial decisions; and
- Acceptable and managed risk is achieved and proportionate to meet the relevant needs of Ultima, its customers and relevant statutory or regulatory requirements.

The objectives of this Policy are to:

- Protect information assets of the Company and its customers, which is contained within the Ultima environment, from threats, whether internal or external, deliberate or accidental; and
- Minimise the risk of damage by seeking to prevent the occurrence of security incidents and reducing their potential impact.

Ultima is committed to continual improvement in all aspects of security, through the implementation and maintenance of its certified information security management system (ISMS), which is based on the framework and requirements of ISO/IEC 27001:2013 Standard (ISO 27001).

2.0 Scope

The scope of this Policy encompasses all forms of information, including knowledge generated, used or shared in the performance of the business or information entrusted to Ultima by its staff, customers, business partners and suppliers. Information processing facilities include premises, IT systems, networks and associated media such as data stored on computers, transmitted across networks, recorded on paper or held on other storage mediums owned or operated by Ultima or its suppliers.

3.0 Responsibilities

- The **Board** is responsible for information security governance and shall provide staff with education and training to support adherence to this Policy and other information security policies.
- The **Board** shall be responsible for approving this Policy and the **Information Security Forum (ISF)**[2] shall be responsible for maintaining this Policy.
- The **Information Security Forum (ISF)** and **all managers** shall ensure that information and data is processed and managed in accordance with all contractual, legislative, and regulatory requirements.
- **Departmental managers,** in conjunction with the **Compliance Manager**, shall be responsible for implementing and communicating this Policy and associated processes and procedures to their staff and for supervising compliance.
- The **Compliance Manager** shall be responsible for ensuring that regular audits of the processes and procedures that implement this Policy are performed to maintain compliance and facilitate continual improvement.

[1] "Ultima" shall be defined as Ultima Business Solutions Ltd and Ultima Business Solutions South Africa (Pty) Ltd.
[2] The Information Security Forum is responsible for regular meetings to review information security, and for reporting to the Operations Board.

- **All staff**[3] are responsible for maintaining awareness of Ultima's information security policies and procedures applicable to their role.
- **All staff** and third parties are required to comply with this Policy and its supporting policies and processes.

4.0 Policy

Ultima is committed to ensure that:

- The Confidentiality of information shall be assured.
- The Integrity of information shall be maintained.
- The Availability of information for business purposes shall be attained.
- The needs and expectations of external parties are met, where such needs and expectations include legislative, regulatory and contractual security obligations.
- Contractual agreements with third parties supplying goods or services to Ultima, or Ultima's customers, shall contain provisions permitting Ultima to conduct a risk assessment and or an audit of the of the supplier's operations and facilities and its information security, quality, environmental and health and safety procedures and systems, where the supplier is deemed high risk following appropriate risk assessment processes.
- Access to information assets shall be controlled and be based on the 'principle of least privilege';
- An Information Security Forum (ISF) shall be established and shall be maintained with members appointed by the Board.
- An Information Security Management System (ISMS) shall be implemented, operated and maintained.
- The ISMS shall be documented and will incorporate appropriate policies, processes and procedures that underpin and implement this Policy.
- The ISMS shall incorporate a systematic approach to the assessment and management of Information Security risks.
- Objectives for the ISMS shall be set and performance against them reviewed by the ISF and the Board.
- Information security awareness training shall be provided for all staff on a frequent basis.
- All information above, and all other GDPR and legal compliance requirements, will be communicated to all staff members through the onboarding process and through mandatory training webinars.
- All new starters shall complete all mandatory training webinars in their first 30 days of starting their new role and so enabling us to monitor information security awareness across the business.
- The protection of information shall be considered when business continuity strategies and plans are produced, maintained, tested or invoked.
- All actual or suspected information security breaches, events and weaknesses shall be reported, logged and investigated under the direction of the ISF.

5.0 Reporting Security Incidents

All staff are responsible for reporting security incidents, events, weaknesses or concerns. Security incidents, including breaches of this Policy, shall be reported by the fastest possible and most appropriate means initially (e.g. via telephone to the Compliance Manager or another member of the ISF) and shall be followed by an email incident report to Incidents@Ultima.com. Security incidents or concerns

[3] Staff includes permanent, contract and associate staff.

may also be reported in confidence via this Mailbox or to a Director. Failure to report a security incident may be considered a breach of this Policy.

6.0 Consequences of Non-Compliance

Any breaches of this Policy and supporting information security policies may be subject to a formal security investigation. Where proven, failure to comply shall result in disciplinary action being taken against individuals determined to be responsible for the breach under Ultima's Disciplinary Process, up to and including summary dismissal for gross misconduct. Ultima may also initiate legal action or refer the breach to relevant law enforcement authorities where warranted. Non-compliance by contracted third parties or their employees may result in termination of the supplier's contract and/or legal action.

7.0 Performance evaluation

Ultima will conduct logging and monitoring of the ISMS, to evaluate the performance and effectiveness of the ISMS. The scope of Monitoring, measurement, analysis and evaluation; Internal audit; and Management review shall be set out in the *Logging and Monitoring* framework documented information. Any non-compliance shall be reported to the ISF for management review, and the ISF will propose relevant remediation actions and action owners as appropriate.

8.0 Information Classification

Ultima's information security policies are classified as 'internal use only' and no part or extract from them or the associated files held on Ultima computer networks may be distributed to any external organisation without the express permission of the Compliance Manager or the ISF.

9.0 Review and Maintenance

This Information Security Policy shall be reviewed annually, or after significant change, by the Compliance Manager and the ISF to ensure it remains effective and fit for purpose.

10.0 Exceptions

Where an Ultima information security policy requirement cannot be met for any reason, a formal request for exception shall be submitted in writing via the Compliance Manager for approval by the ISF. Failure to obtain an exception approval will be considered a breach of this Policy.

11.0 Related Documents

- Commitment to Security Statement
- Physical Security Standard
- Access Control Framework
- Acceptable Use Policy
- Logging and Monitoring framework documented information
- Backup Framework
- Clear Desk and Clear Screen Standard
- Information Classification Labelling and Handling framework
- Anti-Virus Framework
- Vulnerability Management Framework
- Mobile Device and Teleworking Framework
- Cryptography and Key Management Framework

Executive Approval

Scott Dodds, Chief Executive Officer **Date: 08/07/2025**

12.0 Document Control

12.1 Authority

Signatory	Name	Role	Organisation
Author	Chris Cotterell	Compliance Manager	Ultima
Owner	Jenny Hall	Head of Legal & Compliance	Ultima
Approver	Scott Dodds	Chief Executive Officer	Ultima

12.2 Identity

Issue Type	Released

Date Issued	08/07/2025
Title	Information Security Policy - ISMS PO100

12.3 Revision History

Version	Date	Status	Comment
1.0	06/06/2017	Released	First Release
1.1	16/01/2018	Revised	Revised § 1, 2, and 4 to include applicability to 'Suppliers' prudent to ISO 27001:2013, clause A.15.1
1.2	18/07/2018	Revised	Replaced clause (7) 'Audit', with (7) 'Performance evaluation'
1.3	16/01/2019	Revised	Added another bullet point to (4) 'mandatory training changes'
1.4	17/03/2020	Revised	Clarified language and removal of 'Employee Handbook' reference. Reference to information asset owners IAO has been removed
1.5	06/04/2021	Revised	Annual review and addition of associated policy documents in section 11, to align to section 5.1.1 of ISO 27002
1.6	19/05/2022	Revised	Annual Review, no changes.
1.7	02/05/2023	Released	Annual review of contents, no changes. Transferred to new corporate branded template.
1.8	27/06/2024	Released	Addition of Ultima South Africa into Section 1.
1.9	08/07/2025	Released	Changed to 'Public' as this Policy shall replace the 'Commitment to Security' Statement. Amendment to section, 'principle of least privilege' replaces term 'Business need to know'.

Ultima Business Solutions Ltd
Gainsborough House
Manor Park, Basingstoke Road,
Reading, Berkshire, RG2 0NA