Information Security Management System Policy

Version	1.03
Classification	Public
Effective Date	15/05/23
Date for Review	30/5/2025
Document Owner	Matt Parker
Document Approver	Matt Parker
Document Summary	This document defines Lamplight Database System Ltd's overarching Information Security Management System Policy for its ISO 27001 certification.

Contents

STATEMENT

1. Lamplight is trusted by charities to store and help them manage their information, information which is frequently personal and potentially sensitive. The security of this information is fundamental to our success, that of our customers, and the wellbeing of their service users. Our internal information assets are just as vital to our on-going ability to operate effectively.

2. This policy ensures that all information assets are appropriately protected, and provide assurance that they are. This is a Board level commitment and all staff are required to contribute to maintaining our security posture.

3. The policy covers the behaviours of our staff, and the technical controls we put in place.

4. Lamplight will establish an Information Security Management System (ISMS) compliant with the standards set out in ISO27001:2022 and seek and maintain accreditation against the standard.

5. The scope of the ISMS is the entire organisation. It covers the development and hosting of a software solution for charities, and associated implementation, training, data migration, support, and other services. All internal business information and systems are also in scope.

6. The ISMS establishes standards that represent the minimum-security requirements that apply to all our information systems, and the processes that support them. It also gives important responsibilities to managers who must ensure compliance within their areas of control. This will ensure that there is a correct balance between the objectives of creating and maintaining an open, trusting environment in which information, with limited exceptions, is made freely available to all employees, while protecting our data from accidental or deliberate loss, alteration, or disclosure.

7. It is essential that this Policy is fully implemented and that all employees are aware of their responsibilities regarding the protection of data and systems against unauthorised access or disclosure and we make continuous improvements to our information security framework. I would therefore ask that you read this document and direct any questions to your manager.

8. The Board will monitor the ISMS regularly and ensure that it continues to evolve and improve to meet the needs of the business and our customers. The Technical Director will be responsible for the development and day-to-day oversight of the ISMS.

Name: Matt Parker

For and on behalf of Lamplight Database System Limited Ltd

APPROVAL AND COMMUNICATION OF THIS POLICY

This Policy has been approved by Lamplight Database System Limited's Board, having been reviewed by the Information Security Management Forum (ISMF) and any other persons considered appropriate by the approving party.

The current, approved version of this Policy will be made available internally within Lamplight Database System Limited. Specific excerpts will be published on Lamplight Database System Limited as part of the ISO 27001 Certification process.

This Policy will be reviewed on a not less than annual basis, by the ISMF.

INFORMATION SECURITY OBJECTIVES

Based on the requirements and factors set out in this document, the following major objectives are set out for information security:

- Implement and maintain an ISMS, certified to ISO 27001:2022.
- Ensure that the Lamplight Database System Limited solutions we host for our customers provides 99.5% uptime availability.
- Establish a programme to ensure that all employees (existing and new) are made aware of the implications and key requirements concerning Information Security and obtain 100% employee sign-off confirming such awareness.
- Protect the confidentiality, integrity and availability of the ISMS by establishing schedules to ensure all repeatable ISMS activities are performed for:
    - Policy reviews
    - Annual External Security tests
    - 6 monthly vulnerability scans
    - 6 monthly software reviews
    - A robust patch management system
    - All regulatory, legal and other requirements
    - Half yearly access control company and customer reviews
    - Annual Business Continuity tests

POLICY

The principal focus on Information Security is to provide the following:

- Confidentiality: the restriction of access to information by authorised persons, entities and processes at authorised times and in an authorised manner;
- Integrity: safeguarding the accuracy and completeness of information and information processing systems; and
- Availability: ensuring that authorised users have access to information and associated assets when required.

The purpose of the policy is to ensure that:

- Information assets(1) are protected from all threats, whether internal or external, deliberate or accidental
- Information is made available with minimal disruption to staff and clients as required by the business process(2);
- The integrity of this information is maintained(3);
- Confidentiality of information is assured(4);
- Regulatory and legislative requirements are met(5);

- A Business Continuity Framework is implemented and Business Continuity plans produced to counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters. Business continuity plans are maintained and tested(6);
- Information security education, awareness and training is available to staff(7);
- All breaches of information security, actual or suspected, are reported to, and investigated by the ISMF and the Incident Response team(8); and
- Appropriate access control maintained and information is protected against unauthorised access.
- Effectiveness and monitoring is in place to ensure continual improvement(9)
- Policies, Procedures and Guidelines, not limited to Information Security, will be made available on the internal Sharepoint system to support this ISMS Policy.
- The Board has direct accountability for maintaining the ISMS Policy and has appointed the Information Security Management Forum ("ISMF") to write and/or manage the development of relevant policies, procedures and guidelines to support the ISMS policy.
- The Senior Management Team are directly responsible for implementing the ISMS Policy within their units, and for adherence by their staff.
- It is the responsibility of each member of staff to adhere to the ISMS Policy and those related to it.
- Information security is managed through Lamplight Database System Limited's ISMS framework.
- The availability of information and information systems will be met as required by the core and supporting business operations.
- Internal Audit shall assess compliance with this ISMS policy and system
- The services that our suppliers provide will be security assured based on a risk assessment.
- The ISMF will monitor and implement continual improvement.

1 Information takes many forms and includes data stored on computers, transmitted across networks, printed out or written on paper, stored on tapes, USB, or spoken in conversation and over the telephone.

2 This will ensure that information and vital services are available to users when and where they need them.

3 Safeguarding the accuracy and completeness of information by protecting against unauthorised modification.

4 The protection of valuable or sensitive information from unauthorized disclosure or unavoidable interruptions.

5 This will ensure that Lamplight Database System Limited remains compliant to relevant business, national and international laws and it include meeting the requirements stated in legislations such as the Companies Act and GDPR.

6 Business Continuity Management should be implemented effectively to ensure continuity of business operations in the event of a crisis or disaster.

7 Ensure that relevant and effective trainings are provided to staff.

8 Ensure that the staff understand their roles and responsibilities in handling incidents and have a comprehensive and well-tested incident response plan ready.

9 Effectiveness of the policies and controls as well as monitoring will be co-ordinated and reported to the ISMF and escalated to the Directors as appropriate to ensure continual improvement.

Document History

Revision Version	Revision Date	Description of Revision	Revision Author(s)
1.00	11/9/21	Approved by Board	Matt Parker
1.0	15/05/23	Review.	Matt Parker
1.02	1/9/2023	Review and add objectives re. patch and legal reqs.	Matt Parker
1.03	27/5/2024	Review, clarify ISO27001:2022. ISMF still to review objectives so not updated.	Matt Parker
1.03	8/11/2024	Reformat (no content change)	Matt Parker