Information Security Policy

Document Classification:	**OFFICIAL**
Document Ref.	**BOS-DOC-1119**
Version:	**1.4**
Dated:	**01 February 2023**
Document Author:	**Adrian McMullan**
Document Owner:	**Lightbulb Analytics**

Revision History

Version	Date	Revision Author	Summary of Changes
1.0	15/10/18	Paul Ashton	Updates to first draft
1.1	19/11/18	Paul Ashton	Amendments
1.2	19/01/21	Paul Ashton	Amendments
1.3	25/01/22	Adrian McMullan	Amendments
1.4	01/02/23	Adrian McMullan	Amendments

Distribution

Name	Title
A McMullan	Commercial Director
A Ahearne	Technical Director
S Kennell	Product Manager

Approval

Name	Position	Date
A McMullan	Commercial Director	01/02/2023

Contents

List of Tables

1 Introduction

This document defines the information security policy of Lightbulb Analytics Ltd.

As a modern, forward-looking business, Lightbulb Analytics Ltd recognises at senior levels the need to ensure that its business operates smoothly and without interruption for the benefit of its customers, shareholders and other stakeholders.

In order to provide such a level of continuous operation, Lightbulb Analytics Ltd has implemented an Information Security Management System (ISMS) in line with the International Standard for Information Security, ISO/IEC 27001. This standard defines the requirements for an ISMS based on internationally-recognized best practice.

The operation of the ISMS has many benefits for the business, including:

- Protection of revenue streams and company profitability
- Ensuring the supply of goods and services to customers
- Maintenance and enhancement of shareholder value
- Compliance with legal and regulatory requirements

Lightbulb Analytics Ltd has decided to maintain full certification to ISO/IEC 27001 in order that the effective adoption of information security best practice may be validated by an independent third party, a Registered Certification Body (RCB). In addition, the guidance contained in the codes of practice ISO/IEC 27017 and ISO/IEC 27018 has been adopted as these have particular relevance for Cloud Service Providers (CSPs).

This policy applies to all systems, people and processes that constitute the organisation's information systems, including board members, directors, employees, suppliers and other third parties who have access to Lightbulb Analytics Ltd systems.

The following supporting documents are relevant to this information security policy and provide additional information about how it is applied:

- *Risk Assessment and Treatment Process*
- *Statement of Applicability*
- *Supplier Information Security Evaluation Process*
- *Internet Acceptable Use Policy*
- *Cloud Computing Policy*
- *Mobile Device Policy*
- *Teleworking Policy*
- *Access Control Policy*

- *User Access Management Process*
- *Cryptographic Policy*
- *Physical Security Policy*
- *Anti-Malware Policy*
- *Backup Policy*
- *Software Policy*
- *TechNetwork Security Policy*
- *Electronic Messaging Policy*
- *Secure Development Policy*
- *Information Security Policy for Supplier Relationships*
- *Privacy and Personal Data Protection Policy*
- *Clear Desk and Clear Screen Policy*

2 Information Security Policy

2.1 Information Security Requirements

A clear definition of the requirements for information security within Lightbulb Analytics Ltd will be agreed and maintained with the internal business and cloud service customers so that all ISMS activity is focussed on the fulfilment of those requirements. Statutory, regulatory and contractual requirements will also be documented and input to the planning process. Specific requirements with regard to the security of new or changed systems or services will be captured as part of the design stage of each project.

It is a fundamental principle of the Lightbulb Analytics Ltd Information Security Management System that the controls implemented are driven by business needs and this will be regularly communicated to all staff through team meetings and briefing documents.

2.2 Framework for Setting Objectives

A regular cycle will be used for the setting of objectives for information security, to coincide with the budget planning cycle. This will ensure that adequate funding is obtained for the improvement activities identified. These objectives will be based upon a clear understanding of the business requirements, informed by the management review process during which the views of relevant interested parties may be obtained.

Information security objectives will be documented for an agreed time period, together with details of how they will be achieved. These will be evaluated and monitored as part of management reviews to ensure that they remain valid. If amendments are required, these will be managed through the change management process.

In accordance with ISO/IEC 27001 the reference controls detailed in Annex A of the standard will be adopted where appropriate by Lightbulb Analytics Ltd. These will be reviewed on a regular basis in the light of the outcome from risk assessments and in line with information security risk treatment plans. For details of which Annex A controls have been implemented and which have been excluded please see the *Statement of Applicability*.

In addition, enhanced and additional controls from the following codes of practice will be adopted and implemented where appropriate:

- ISO/IEC 27002 – Code of practice for information security controls
- ISO/IEC 27017 – Code of practice for information security controls based on ISO/IEC 27002 for cloud services

- ISO/IEC 27018 – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

The adoption of these codes of practice will provide additional assurance to our customers and help further with our compliance with international data protection legislation.

2.3 Continual Improvement of the ISMS

Lightbulb Analytics Ltd policy with regard to continual improvement is to:

- Continually improve the effectiveness of the ISMS
- Enhance current processes to bring them into line with good practice as defined within ISO/IEC 27001 and related standards
- Achieve ISO/IEC 27001 certification and maintain it on an on-going basis
- Increase the level of proactivity (and the stakeholder perception of proactivity) with regard to information security
- Make information security processes and controls more measurable in order to provide a sound basis for informed decisions
- Review relevant metrics on an annual basis to assess whether it is appropriate to change them, based on collected historical data
- Obtain ideas for improvement via regular meetings and other forms of communication with interested parties, including cloud service customers
- Review ideas for improvement at regular management meetings in order to prioritise and assess timescales and benefits

Ideas for improvements may be obtained from any source including employees, customers, suppliers, IT staff, risk assessments and service reports. Once identified they will be recorded and evaluated as part of management reviews.

2.4 Information Security Policy Areas

Lightbulb Analytics Ltd defines policy in a wide variety of information security-related areas which are described in detail in a comprehensive set of policy documentation that accompanies this overarching information security policy.

Each of these policies is defined and agreed by one or more people with competence in the relevant area and, once formally approved, is communicated to an appropriate audience, both within and external to, the organisation.

The table below shows the individual policies within the documentation set and summarises each policy's content and the target audience of interested parties.

Policy Title	Areas addressed	Target audience
Internet Acceptable Use Policy	Business use of the Internet, personal use of the Internet, Internet account management, security and monitoring and prohibited uses of the Internet service.	Users of the Internet service
Cloud Computing Policy	Due diligence, signup, setup, management and removal of cloud computing services.	Employees involved in the procurement and management of cloud services
Mobile Device Policy	Care and security of mobile devices such as laptops, tablets and smartphones, whether provided by the organisation or the individual for business use.	Users of company-provided and BYOD (Bring Your Own Device) mobile devices
Teleworking Policy	Information security considerations in establishing and running a teleworking site and arrangement e.g. physical security, insurance and equipment	Management and employees involved in setting up and maintaining a teleworking site
Access Control Policy	User registration and deregistration, provision of access rights, external access, access reviews, password policy, user responsibilities and system and application access control.	Employees involved in setting up and managing access control
Cryptographic Policy	Risk assessment, technique selection, deployment, testing and review of cryptography, and key management	Employees involved in setting up and managing the use of cryptographic technology and techniques
Physical Security Policy	Secure areas, paper and equipment security and equipment lifecycle management	All employees

Anti-Malware Policy	Firewalls, anti-virus, spam filtering, software installation and scanning, vulnerability management, user awareness training, threat monitoring and alerts, technical reviews and malware incident management.	Employees responsible for protecting the organisation's infrastructure from malware

Policy Title	**Areas addressed**	**Target audience**
Backup Policy	Backup cycles, cloud backups, off-site storage, documentation, recovery testing and protection of storage media	Employees responsible for designing and implementing backup regimes
Software Policy	Purchasing software, software registration, installation and removal, in-house software development and use of software in the cloud.	All employees
Technical Vulnerability Management Policy	Vulnerability definition, sources of information, patches and updates, vulnerability assessment, hardening and awareness training.	Employees responsible for protecting the organisation's infrastructure from malware
Network Security Policy	Network security design, including network segregation, perimeter security, wireless networks and remote access; network security management, including roles and responsibilities, logging and monitoring and changes.	Employees responsible for designing, implementing and managing networks
Electronic Messaging Policy	Sending and receiving electronic messages, monitoring of electronic messaging facilities and use of email.	Users of electronic messaging facilities

Secure Development Policy	Business requirements specification, system design, development and testing and outsourced software development.	Employees responsible for designing, managing and writing code for bespoke software developments
Information Security Policy for Supplier Relationships	Due diligence, supplier agreements, monitoring and review of services, changes, disputes and end of contract.	Employees involved in setting up and managing supplier relationships
Availability Management Policy	Availability requirements and design, monitoring and reporting, non-availability, testing availability plans and managing changes.	Employees responsible for designing systems and managing service delivery
IP and Copyright Compliance Policy	Protection of intellectual property, the law, penalties and software license compliance.	All employees
Policy Title	**Areas addressed**	**Target audience**
Records Retention and Protection Policy	Retention period for specific record types, use of cryptography, media selection, record retrieval, destruction and review.	Employees responsible for creation and management of records
Privacy and Personal Data Protection Policy	Applicable data protection legislation, definitions and requirements.	Employees responsible for designing and managing systems using personal data
Clear Desk and Clear Screen Policy	Security of information shown on screens, printed out and held on removable media	All employees

Table 1 - Set of policy documents

2.5 Application of Information Security Policy

The policy statements made in this document and in the set of supporting policies listed in Table 1 have been reviewed and approved by the top management of Lightbulb Analytics Ltd and must be complied with. Failure by an employee to comply with these policies may result in disciplinary action being taken in accordance with the organisation's Employee Disciplinary Process.

Questions regarding any Lightbulb Analytics Ltd policy should be addressed in the first instance to the immediate line manager.