Information Security Policy

Policy and Procedure

Version:	1.6
Date of version:	01/09/2025
Owner:	Mark McGrath (CTO)
Approved by:	John Ingram (CEO)
Confidentiality level:	PUBLIC

Change history

Date	Version	Edited by	Description of change
29/03/2022	1v1	John Ingram	Reviewed and amended during the annual management meeting
08/02/2023	1v2	John Ingram	Updated NCSC security principles, reviewed and signed off during management meeting.
06/02/2024	1v3	Bryan Parsons	Updated layout, reviewed and signed off during management meeting.
09/12/2024	1v4	Mark McGrath	Updated certification reference to ISO/IEC 27001:2022 standard.
25/02/2025	1v5	Bryan Parsons	Added AI commitment
01/09/2025	1.6	Bryan Parsons	Removed reference to ESFA and grammar corrections.

Purpose and Objective

The purpose of this document is to define the role that Bud Systems Limited's top management takes in the Information Security Management System (ISMS). This ensures the commitment to information security, the development and propagation of the information security policy, and the assignment of information security roles, responsibilities, and authorities.

The main goal of this Information Security Policy is to guarantee clients and service users access to information with the quality and level of service needed for the agreed performance, as well as avoiding serious loss or alteration of information, and unauthorised access.

Scope

The scope of the Information Security Policy coincides with the scope of the Information Security Management System (ISMS), documented in Bud System's relevant ISMS documentation.

Responsibilities

The Board is responsible for setting and approving the information security policy. The Chief Technology Officer (CTO) is responsible for ensuring that roles, responsibilities, and authorities are appropriately assigned, maintained, and updated, as necessary.

All staff are responsible for meeting the requirements of this Policy and being conversant in any other policies which relate to information security and data protection, which apply to their roles and responsibilities within Bud.

Relevant roles and responsibilities regarding information security and the ISMS are expanded upon in Bud System's ISMS documentation.

Information Security Policy

The Board is committed to the protection of the confidentiality, integrity, and availability of all information assets within the company. Managed through an ISO/IEC 27001:2022 certified information security management system (ISMS) that maintains and continually improves internal processes.

Bud Systems' Board understands the centrality to its sustainable growth of information security and the expectations of both the internal and external stakeholders. In particular, the training providers that will use Bud's services, the Department of Education (DfE) and other funding providers/agencies.

Further, Bud must satisfy various legal and regulatory requirements, including, but not limited to the Data Protection Act 2018 (DPA 2018) and the UK General Data Protection Regulation (2018), which places specific obligations to protect the privacy of the learners, whose details Bud process.

Objectives, Strategy and Principles

A framework is established to achieve the Information Security objectives for the Organisation. These objectives will be achieved through a series of organisational measures and specific and clearly defined rules.

The principles that must be respected, based on the basic dimensions of security, are the following:

1. **Confidentiality**: the information can only be accessed by whoever is authorised to do so, subject to identification, at the authorised time and by the authorised means.
2. **Integrity**: guarantees the validity, accuracy, and completeness of the information, without any type of manipulation and allowing it to be modified only by whoever is authorised to do so.
3. **Availability**: The information is accessible and usable by authorised and identified customers and users at all times, guaranteeing its own persistence in the event of any foreseen eventuality.

Additionally, given that any Information Security Management System must comply with current legislation, the following principle will apply:

4. **Legality**: in reference to compliance with the laws, rules, regulations, or provisions that govern Information Systems and Technology, especially regarding the protection of personal data.

The ISMS must guarantee:

- policies, regulations, procedures, and operational guides are developed to support the Information Security Policy.
- information assets to be protected are identified, classified and ownership established.
- risk management is established and maintained in line with the requirements of the ISMS Policy.
- a methodology is established for risk assessment and management.
- criteria are established with which to measure the level of compliance with the ISMS and that the ISMS compliance level is reviewed through regular auditing.
- nonconformities are rectified through the implementation of corrective actions.
- personnel receive information security training and awareness.
- all personnel are informed about the obligation to comply legislation and company policies.
- the necessary resources are assigned to manage the ISMS.
- all legal, regulatory, and contractual requirements are identified and met.
- the information security implications are identified and analysed with respect to business requirements.
- the successful application of the Information Security Management System itself is measured.
- the safe and ethical use of artificial intelligence, ensuring regulatory compliance to protect data and uphold privacy.

Document Owner and Approval

Authority for the management of this Policy is with the CTO, as provided by the Board of Directors.

Any changes to this information security policy are approved by the Board of Directors and is issued on a version-controlled basis by the CTO.

This policy will be reviewed to respond to any changes in the risk assessment or risk treatment plan and at least annually.