Information Security Policy

Author: Vikki Williams

Date: 11/092023

Version: 1.0

1. Document Control

Version	Revised By	Date	Status	Release Notes
0.1	Vikki Williams	13/03/2023	Draft	Initial version for review.
0.2	Vikki Williams	11/09/2023	Draft	Updated based on comments received.
1	Vikki Williams	19/09/2023 20/11/2023	Final	Approved by Information Security Board Approved by CEO

2. Table of Contents

3. Background

This document presents the philosophy of information security within Arden University and represents the endorsement of Arden University's executive management team. It identifies the motivation for security, describes information security principles and terms, and defines the scope of information security policies and responsibilities of the various security functions.

4. Objective

The Board of Directors and management of Arden University are committed to preserving the confidentiality, integrity and availability of all information and information assets, including personal data, throughout the organisation by maintaining an information security management system (ISMS),

5. Responsibilities

CEO	Responsible for approving the Information Security policy
Board of Directors	Accountable for information security and responsible for ensuring that the appropriate assets are available to ensure the effectiveness of the ISMS
Line Managers	Accountable for information security and must ensure compliance with the ISMS and associated policies, procedures, standards and practices within their respective areas of responsibility
Information Security Governance Board	Responsible for ensuring that appropriate security controls are in existence and in force throughout the organisation. ISGB is responsible for determining methods of implementing and enforcing security policies and for advising on security-related issues. ISGB ensures that information security awareness is increased, and audits are performed, and management reviews are regularly undertaken. ISGB appoints and manages suitably skilled people to staff information security teams as deemed appropriate.
Information Security Working Group	Reviews and endorses the ISMS. They agree to the roles and responsibilities for information security across the enterprise as defined in specific policies. They visibly promote and provide business support for information security initiatives throughout the enterprise. The working group is led by the Head of Cyber Security and includes representatives from all major business units.
Head of Cyber Security	Manages and implements the ISMS across the organisation and ensure it remains fit-for-purpose. Lead on the organisation's approach to information security risks and risk treatment. First point of contact for information / cyber security queries.
All staff members and employees	To comply with this policy, the wider ISMS and all associated policies, procedures, standards and practices. Reporting of information security risks, events and incidents to the appropriate individual. To undertake regular information security training in accordance with the requirements of their role.
Third parties	To undertake / provide appropriate information security training where appropriate and agree to follow the relevant policies and procedures prior to accessing Arden's information and assets.

The consequences of breaching the information security and privacy policies will be subject to disciplinary action, as detailed in the disciplinary policy or in contracts with third parties.

6. Policy

- Arden University are committed to ensuring compliance with all applicable legislative, regulatory and contractual requirements across the information security arena.

- Arden University are committed to preserving the confidentiality, integrity and availability of all information and the assets processing that information in line with the requirements of ISO27001:2022.

- Arden University's current business objectives and risk management framework provide the context for identifying, assessing, evaluating, controlling and reviewing information risks via the implementation of an ISMS. The Head of Cyber Security is responsible for the risk register and risk treatment plan. Individual asset owners are responsible for reviewing and accepting the risks and risk treatments related to their assets. Additional risk assessments may take place, where required, to determine the appropriate controls for specific risks.

- Business continuity, backup procedures, anti-virus and anti-malware, access control and incident reporting are key areas of information security and are fundamental to the ISMS. Control objectives for the key areas relating to the ISMS will be available within the ISMS Manual, supported by a number of further policies, procedures and work instructions.

- Arden University aims to achieve defined information security objectives, developed in line with the requirements of the ISO27001:2022, risk assessments and risk treatment plans. The university is committed to achieving certification of its ISMS to ISO27001:2022.

- All employees, students and certain third parties will be required to comply with the Information Security policy and the wider ISMS and will receive appropriate training. The consequences of breaching this, or other policies within the ISMS, are set out in Arden University's Disciplinary Policy and within agreements and contracts with suppliers and third parties.

- The ISMS is subject to ongoing review and improvement, managed via the Information Security Working Group and the Information Security Governance Board (who report into the Board of Directors via the Arden Executive Committee).

- This policy will be reviewed at least annually or in response to any major changes in the risk assessment or the business objectives of Arden University.