Cyber Security

Item(s) New Policy: Cyber Security	Doc No: 1
Superseded:	Version: 1
Developed by: Human Resources	Date: 12 September 2022
Authorised by: HR	Pages: 3

1. Ascention Purpose Statement

1.1 This policy provides management direction and support for cyber security across Ascention Services.

2. Scope

2.1 The Cyber Security Policy applies to all our people (as defined).

2.2 The policy applies to all interactions with Ascention Services digital infrastructure and/or access to Ascention Services systems, applications, and information.

3. Policy Statement

3.1 This policy aligns with the corporate value of trust. Ascention Services believes that stakeholders trust can be maintained and enhanced through the development of a security culture and an associated technical capability to identify and respond to information security incidents in a timely manner.

4. Cyber Security Objectives

4.1 The information security objectives of Ascention Services ISMS are:

- Maintain the reputation and brand of Ascention Services;
- Ensure Ascention Services complies with all applicable external regulatory requirements
- Ensure the integrity and availability of critical business applications to meet operational needs;
- Develop a culture that sees information security embedded in decision making; and
- Continuously improve the security posture of Ascention Services through the management of risks, threats, and incidents whilst balancing the utility and protection of information.

5. Application of policy

5.1 All our people commit to the following:

5.1.1 Agree to, understand, and exhibit the requirements of the Acceptable Use of Electronic Resources Standard.

5.1.2 Agree to, understand, and exhibit the requirements of the Code of Conduct. Of particular relevance for this policy are the requirements around confidentiality, privacy, intellectual property, and use of corporate assets.

5.1.3 Comply with all requirements surrounding passwords and access to corporate systems including Bring Your Own Device (BYOD) and remote access or elevated privileges.

5.1.4 Be vigilant when using email and internet services to validate attachments or links before opening or clicking them.

5.1.5 Report suspicious emails to the Cybersafe reporting email address for investigation.

5.1.6 Report actual or suspected cyber security incidents to your immediate supervisor and/or Service Desk.

6. Responsibilities

6.1 In addition to the above, Ascention Services directors, executives, managers, and team leaders will:

1. Facilitate and support a culture where cyber security is considered throughout our business processes and decision making.
2. Ensure that they, and those within their area of responsibility, are aware of, understand, and comply with the requirements of the Acceptable use of Electronic Resources Standard and Code of Conduct at all times.
3. Ensure that any new business systems or applications are procured or developed in conjunction with the Digital team from an early stage to ensure that proper consideration can be given to the cyber security requirements of these systems.
4. Actively support our people in reporting actual or suspected cyber security breaches and assist with any questions or concerns people have about cyber security or the requirements of the ISMS
5. Take the appropriate action as outlined in the relevant ISMS standards and procedures if they become aware or actual or suspected breaches of cyber security.

6.2 Failure to comply with any element of this policy may result in disciplinary action, up to and including termination of employment in accordance with Ascention Services Corporation's Code of Conduct, and the Misconduct and Discipline Standard. Each situation will be treated individually on a case-by-case basis.

Item(s) New Policy: Cyber Security	Doc No: 1
Superseded:	Version: 1
Developed by: Human Resources	Date: 12 September 2022
Authorised by: HR	Pages: 3

7. Definitions, acronyms, and abbreviations

Term	Definition
Cyber Security	Cyber Security refers to the processes and tools designed and deployed to protect sensitive business information from modification, disruption, destruction, or inspection by those unauthorised to do so. It also considers the threats posed by physical access to information by physical attendance at corporate premises.
ISMS	Information Security Management System
People	For the purposes of this Policy, this includes: • Directors • Permanent employees, whether full-time or part-time • Temporary or casual employees • Consultants • Individual contractors working for or on behalf of Ascention Services • Employees of contractors providing services to Ascention Services • Volunteers, secondees, work experience students.