Information Security Policy

Introduction

This Information Security Policy outlines the policy we adhere to in order to ensure the security of any of ours and our clients' data and systems, or any other data processed, accessed or stored by ABCA Systems as a result of the provision of any service to a client or its internal operations.

General Principles

The security and integrity of our clients' data is of the highest importance to us. We operate a multi-layered approach to IT security, utilising systems that adhere to this approach. We use a number of third-party applications in the support and management of our clients' assets and data.

Policy Detail

ABCA Systems information assets and those of its clients are valuable to its objectives. For the purposes of this document all client sensitive data such as client credentials is considered part of ABCA Systems information assets.

The confidentiality, integrity and availability of ABCA Systems information assets are essential to the success of its operational and strategic activities. ABCA Systems aims to secure its information assets by establishing an information security strategy that will enable the implementation of a robust information security risk management system and foster good security practices.

This Information Security Policy is a key component of ABCA Systems' Information Security Strategy built on a framework of information security management standards and best practices. The Information Security Policy will serve as an overarching policy document to provide a high-level overview of information security management within ABCA Systems.

Policy Objectives

The objectives of the Information Security Policy are:

- To ensure that information assets are available when required to authorised users.
- To ensure that information assets are adequately protected against unauthorised access, malicious or accidental loss, misuse or damage.
- To ensure that all users are aware of and fully comply with this policy and supplementary policies, processes, standards, procedures and guidelines.
- To ensure that all users understand their responsibilities for protecting the confidentiality and integrity of ABCA Systems information assets.
- To ensure that the risks to ABCA Systems information assets are appropriately managed.
- To ensure that information security incidents are resolved promptly and appropriately.
- To ensure that ABCA Systems meets relevant audit and statutory requirements.
- To ensure there is an efficient disaster recovery plan in place.
- To protect ABCA Systems from any legal liability resulting from information security incidents.

Policy Scope

The Information Security Policy applies to all forms of information stored, used or processed by ABCA Systems. The policy also applies to all information systems owned or leased by ABCA Systems including information systems managed by third parties on behalf of ABCA Systems.

The policies apply to all staff, contractors and third-party agents who access, use, handle or manage all ABCA Systems information assets.

Principles

The following principles govern ABCA Systems' information security approach:

- The Information Security Policy and supplementary policies, processes, standards, procedures and guidelines will be communicated to all users via training and awareness sessions, inductions, ABCA Systems intranet and internet, bulletins and other appropriate communication channels.
- ABCA Systems data will be classified and provided with appropriate safeguards commensurate to their value, ensuring they are available when needed and protected against unauthorised or inappropriate access or use.
- User access to ABCA Systems' information assets will be based on job requirements rather than job titles. Access rights will be reviewed at regular intervals and revoked if or where necessary.
- ABCA Systems will establish and promote an information security awareness culture amongst its information asset users through user awareness and training, publications on information security risks and incidents, and guidelines for managing them.
- Disaster recovery plans for mission critical information assets and related services will be established, tested and maintained.
- ABCA Systems will implement an incident reporting and management system to enable prompt and appropriate incident resolution activities and inform risk assessments and management.
- ABCA Systems will enforce and monitor compliance with the Information Security Policy, supplementary policies, processes, standards, procedures and guidelines.

Compliance

ABCA Systems has an obligation to comply with relevant legal and statutory requirements. The Information Security Policy and supplementary policies, processes, standards, procedures and guidelines are to promote and enforce compliance with applicable laws by providing directions and guidelines on good information security practices to underpin ABCA Systems' compliance with these laws.

The applicable laws include but are not limited to:

- General Data Protection Regulation (2018)

- Copyright, Designs and Patents Act (1988)
- Computer Misuse Act (1990)
- Other relevant legislations that may influence this policy

All users of ABCA Systems information assets must comply with the Information Security Policy and supplementary policies, processes, standards, procedures and guidelines and must also keep abreast of updates to these policies.

Failure to adhere to the Information Security Policy and supplementary policies, processes, standards, procedures and guidelines will be addressed by necessary disciplinary actions in accordance to ABCA Systems' Staff Disciplinary Procedures, Procedures and relevant contractor and third party contractual clauses relating to non-conformance with the Information Security Policy and related policies.

Responsibilities for Information Security

The Managing Director (MD) is ultimately responsible for information security management and compliance with related statutory laws. The MD is responsible for the strategic direction of information security within ABCA Systems including:

- Ensuring the information security strategy aligns with ABCA Systems objectives.
- Endorsing the implementation of approved policies, processes, standards and procedures.
- Resourcing and supporting information security initiatives.
- Ensuring risks are mitigated to acceptable levels.
- Ensuring that information security is properly managed across ABCA Systems.
- Driving the allocation of resources and supporting the implementation of information security initiatives.
- To facilitate an information security awareness culture.
- To review, recommend and approve relevant policies, procedures, standards and processes.
- To ensure compliance with relevant policies, audit and statutory requirements.
- To facilitate the implementation of information security initiatives and provide governance oversight on progress and outcomes.
- To review information security requirements for major IT and data sharing/migration projects and recommend best practices.
- To review major information security incidents and lessons learned and make recommendations.
- To advise and recommend response plans to related internal and external audit findings.
- Monitoring compliance with the Information Security Policy and supplementary policies, processes, standards, procedures and guidelines.

- Updating the Information Security Policy and supplementary policies, processes, standards, procedures and guidelines to ensure they remain fit for purpose.
- Managing the implementation of information security risk assessments and relevant mitigation controls;
- Monitoring the state of ABCA Systems information security and reporting on findings and key performance indicators
- Monitoring and analysing external information security attack trends and advising of related risks to ABCA Systems.

All Users (staff, guests, contractors and third-party agents) who access, use, handle and manage ABCA Systems information assets are responsible for:

- Familiarising themselves with the Information Security Policy, related policies, processes, standards, procedures and guidelines.
- Familiarising themselves and agreeing to comply with their legal responsibilities for appropriate use and safety of ABCA Systems information assets.
- Completing relevant information security awareness and training courses.
- Reporting information security incidents via the appropriate procedure promptly.

Awareness and Training

Information Security awareness and training will be a key component of ABCA Systems' information security strategy designed to strengthen users' compliance with ABCA Systems information security policies and ABCA Systems' compliance with audit and statutory requirements.

Through information security awareness and training, ABCA Systems aims to establish an information security conscious culture, providing basic knowledge and relevant skills that will enable users to carry out their information security responsibilities, and promoting good security practices amongst users of its information assets.

ABCA Systems staff must complete relevant awareness and training courses made available by ABCA Systems. Contractors and third parties will be responsible for providing necessary awareness and training to their staff, where not made available by ABCA Systems.

Data Classification and Information Handling

Data classification and appropriate information handling procedures will facilitate good information management within ABCA Systems to ensure that ABCA Systems data (from creation to retention and/or destruction) is handled in a manner that safeguards the confidentiality, integrity and availability of the data.

In order to achieve this, ABCA Systems will establish policies and procedures that will set out how ABCA Systems

data should be accessed, used and handled, and the appropriate controls that should be implemented commensurate with the sensitivity and criticality of the data.

All users of ABCA Systems data are required to familiarise themselves with the policies and procedures in order to engage in suitable security practices to protect ABCA Systems data from unauthorised access, disclosure, modification, loss, theft or damage.

Disaster Recovery Plan

ABCA Systems has a responsibility to establish processes that will ensure essential business operations and services are sustained while recovering from a major information system failure or a disaster.

There is an ABCA Systems IT Disaster Recovery Plan, which provides the procedures to be followed in order to optimise continuity of IT services, and then enable a return to normal operations in the event of a disaster.

The MD in consultation with relevant staff and parties across ABCA Systems will undertake business impact analyses and risk assessments of critical systems and services within ABCA Systems' IT infrastructure, identifying the levels of risks to the company as a result of a system or service unavailability. This includes the risk to operations, teaching, research, legal obligations and reputation. The outcomes of the risk assessments will serve to indicate the criticality of each system and related service and therefore determine the appropriate recovery and continuity provision for each component.

Incident Management

The management of information security incidents in a prompt and appropriate manner will enable ABCA Systems to efficiently mitigate the risks and any legal implications that may be associated with information security incidents.

ABCA Systems' Data Breach and Complaints Reporting Procedure sets out the procedure and guidelines for reporting information security and data breach incidents. All users are responsible for complying with the statements and steps detailed in the Policy.

Policy Review and Maintenance

This policy will be reviewed and updated regularly to ensure that it remains appropriate in light of changes to business requirements, statutory laws or contractual obligations.