FINANCIAL

ASSOCIATES

ELECTRONIC DATA &

CYBER SECURITY

POLICY

FINANCIAL ASSOCIATES SPECIALIST ADVISORY SERVICES (PTY) LTD

Authorised Financial Services Provider Registered with the FSB
FSB Number: 44829

ELECTRONIC DATA & CYBER SECURITY POLICY

POLICY STATEMENT

- Any reference to the “organisation” shall be interpreted to include the “policy owner”.
- The organisation’s governing body, its employees, volunteers, contractors, suppliers and any other persons acting on behalf of the organisation are required to familiarise themselves with the policy’s requirements and undertake to comply with the stated processes and procedures.

TABLE OF CONTENTS

1 INTRODUCTION

In 2022, South Africa was listed as the country with the sixth-highest number of cybercrimes victims in the world and losing R2.2 billion a year to cybercrimes. In 2019, there were 577 attempted malware attacks per hour, and the number is still increasing. Given the constant rise in cybercrime and its extensive cost, there is a need for organisations to adopt effective cyber security measures.

Some examples of the forms of cybercrimes affecting businesses include:

1. The unlawful access to a computer system or computer data storage medium for purpose of committing an offence listed in the Cybercrimes Act, 19 of 2020 ("the Act");
2. The unlawful interception of data including electromagnetic emissions from a computer;

   The unlawful use or possession of hardware or software for purpose of committing an offence listed in the Act;

   The unlawful interference with data or computer program, including the deletion, alteration, damage ~~,~~or deterioration, obstruction or interruption thereof and denial of access to it;
3. The unlawful interference with computer data storage medium or computer system;
4. The unlawful acquisition, possession provision, receipt or use of password, access code or similar data or device for the purposes of committing an offence listed in the Act;
5. Intentionally defrauding another person making false data or computer program to that person's actual or potential prejudice;
6. Unlawfully intercepting data, interfering with data or a computer program or with computer data or storage medium, or unlawfully acquires, possesses, provides, receives or uses a password, access code or similar data or device from a restricted computer;
7. Theft of incorporeal property; and
8. Malicious communications.

Given the negative socio-economic impact of cybercrime, this policy sets out the organisational rules aimed at ensuring that the organisation's technology, computers, staff members, information systems, processes, organisational culture and physical surroundings are effectively managed.

It is important to note that certain cybercrime may be interconnected with the Protection of Personal Information Act, 4 of 2013 ("POPIA") and, in those instances, the POPIA Information Security policies and procedures should be studied.

Some common cyber threats include:

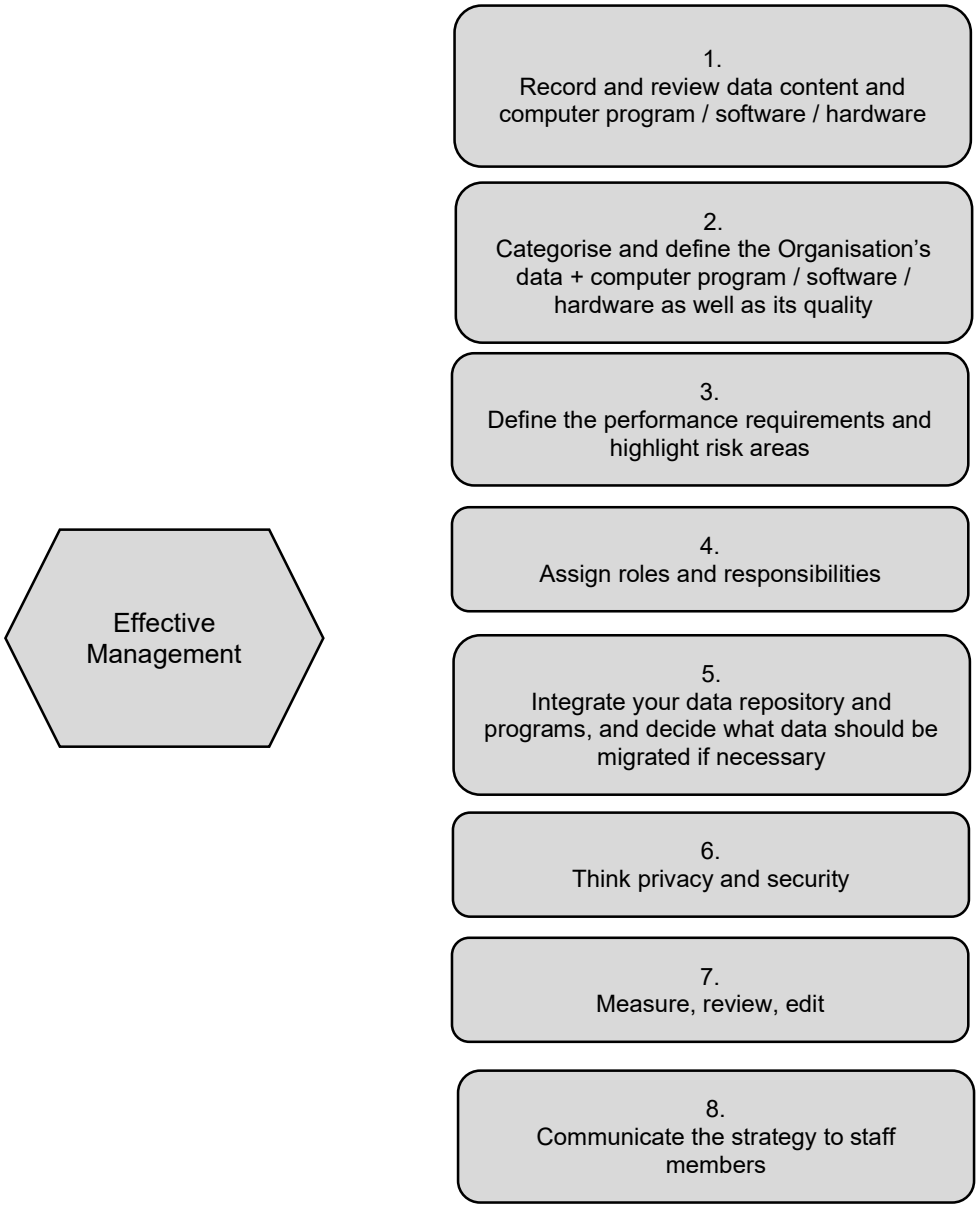
- Malware (worms, viruses, Trojans and spyware);
- Ransomware (type of malware that locks down files, data or systems and threatens to erase or destroy the data);
- Phishing / social engineering (emails or text messages that appear to be from a legitimate company asking for sensitive information);
- Insider threats (current or former employees, partners, contractors or anyone who has accessed to systems/networks in the past, abusing their access permissions);
- Distributed denial-of-service attacks (attempt to crash a server, website or network by overloading it);
- Advanced persistent threats (intruder or group infiltrate a system and remain undetected for an extended period whilst spying on business activity and stealing sensitive data, avoiding the activation of defensive countermeasures); and
- Man-in-the-middle attacks (eavesdropping attack by which a criminal intercepts and relays messages between parties).

(Source: IBM)

The primary goal of this policy is two-fold:

1. To effectively manage data, computer programs, systems, hardware and software; and
2. To secure data, and in the case of a data breach, ensure that the organisation can efficiently respond and recover from the breach in a manner that minimises any loss to the organisation and its clients.

The following diagram sets out the effective data and computer program / software / hardware management:



2 DEFINITIONS

2.1 Computer System

Computer system means one computer; or two or more inter-connected or related computers, which allow these inter-connected or related computers to exchange data or any other function with each other.

2.2 Confidential Information

Examples of confidential information include trade secrets, financial methods, policies and philosophies, marketing methods, incentive schemes, formulae, processes, systems, sources of supply, business methods, inventions, specialised knowledge of training material and training programmes, staff welfare, business connections, internal control systems, policies and strategies, financing techniques, software and/or database information, unpublished financial information, data of customers/partners/ vendors, patents, formulas or new technologies and client lists. Personal information is to be treated as confidential.

2.3 Cybercrime

Cybercrime is not defined in the Act, but refers to the crimes mentioned in Part I to III of Chapter 2 of the Act. The general definition of a cybercrime is a criminal activity carried out by means of computers or the internet.

2.4 Cyber Security

IBM defines cyber security as the practice of protecting critical systems and sensitive information from digital attacks and includes: critical infrastructure security, network security, application security, cloud security, information security, end-user education, disaster recovery/business continuity planning, storage secrity and mobile security. It involves people, information systems, processes, culture and physical surroundings as well as the effective management of technology.

2.5 Personal Information

POPIA defines personal information (“PI”) as information related to the race, gender, sex, pregnancy, marital status, national or ethnic origin, colour, sexual orientation, age, physical or mental health, disability, religion, conscience, belief, culture, language and birth of a person; information relating to the education or the medical, financial, criminal or employment history of the person; any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or other particular assignment to the person; the biometric information of the person; the personal opinions, views or preferences of the person; correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence; the views or opinions of another individual about the person whether the information is recorded electronically or otherwise.

3. POLICY PURPOSE

3.1 Protecting the Organization

This policy aims to protect the organisation from those who wish to:

- Harm the organisation’s business;
- Harm the organisation’s reputation;
- Steal the organisation’s information or financial resources;
- Use the organisation’s computer system to target peers in the market; and
- Use the organisation’s computer system to gain access to clients’ PI.

South Africa’s Cybercrimes Act, 19 of 2020 creates new (cybercrimes and places a duty for financial institutions) to report these crimes.

In terms of section 54(1) of the Act, where a financial institution is aware, or becomes aware, that its computer system has been involved in the commission of any of the offences described under part 1 of Chapter 2 of the Bill, the organisation must without undue delay and, where feasible, within 72 hours after having become aware of the offence, report the offence in the prescribed form and manner to the South African Police Service.

The organisation must also preserve any information which may be of assistance to the law enforcement agencies in investigating the offence.

The privacy of the organisation’s own confidential information and that of its clients, is of the utmost importance and is to be protected at every level of the organisation.

The main purpose of this Electronic Data and Cyber Security policy is therefore to communicate the organisation's commitment towards securing the organisation's systems and data, and any supplementary Standards, Procedures and Best Practice Principles which provide support and direction to this policy.

4. POLICY APPLICATION

There is a misconception that cyber security is the sole responsibility of the IT department only. The reality is however, that cybersecurity is a shared responsibility. It is of the utmost importance that a holistic approach be adopted and that staff members, processes, tools, and technologies are managed together to protect the organisation's data and technological systems.

This policy therefore applies to all staff members, contractors, volunteers and anyone who has permanent or temporary access to the organisation's technological systems and hardware.

This policy is geared towards South African organisations.The Act and POPIA apply within the South African context. Organisations are to note jurisdictional prescriptions in both pieces of legislation. The General Data Protection Regulation ("GDPR"), a regulation in European Union law, has been consulted since it was one of the first regulations of data protection and privacy laws and it has extra-territorial application (outside the boarders of South Africa). It is up to the organisation to determine the whether it will consult the GDPR and related principles (or which other jursidictional laws to apply), and apply them to their organisation by tailoring this policy to the specific needs and risks facing the organisation. The Act and POPIA, and any other related subordinate legislation, requires mandatory compliance with its provisions, unless an exemption applies.

5. CYBERSECURITY RISK REGISTER

The organisation will identify and catalogue potential risk areas:

a. Risk Rating

Insignificant	1	The event poses a very low risk, with an insignificant impact to the organisation. The status of the risk should, however, be reviewed occasionally.
Minor	2	This risk poses a minor threat and would have an impact, but only minor. No immediate remedial response is required, but an action plan should be considered by management. The status of the risk should be reviewed periodically (for example every three months or monthly).
Medium	3	The risk poses a moderate threat to the organisation's daily operations and budget. Some immediate action is required to address the risk. An action plan should be developed. This risk area should be monitored regularly.
Serious	4	This risk could have severe consequences. There is the potential for disrupting project timelines and daily operations. The personal data of clients and customers is at risk.
Disastrous	5	This risk is above the organisation's tolerance level. The consequences would have a debilitating impact upon the organisation's daily operations, budget and its reputation. The personal data of clients and customers is at risk. Comprehensive action is required immediately.

b. Risk Register

Risk ID	Last Review Date	Risk Description	Risk Owner	Likelihood Rating	Impact Rating	Risk Rating (L x I)	Control Measures
		Operational risks, weak passwords, a lack of end-user education.					

6. STAFF MEMBER DUTIES

a. Awareness and Compliance

Every staff member is expected to carefully read, understand and comply with this policy. Violations of this policy may lead to the suspension or revocation of system privileges and/or to disciplinary action up to and including termination of employment.

b. Confidentiality

Any confidential information that is accessed by staff members must be kept confidential. This information should only be accessed by people (or systems) that have been given express permission to do so. Information that staff memebers have access to is only to be used for the specific purpose for which access was granted. The use of information for any other purpose will be treated as a serious transgression by the organisation and will lead to disciplinary measures.

c. Integrity

Staff members are required to maintain the integrity of information assets and to keep information assests and systems secure and uncorrupted. When staff members use their digital devices to access the organisation's emails or accounts, they potentially introduce security risks to the organisation. All staff members are advised to keep both their personal and company-issued computer, tablet and cell phone secure.

Staff members are advised to adopt the following practices:

- Keep all devices password protected in terms of a Password policy and/or passwords should be changed regularly;
- Choose and upgrade a complete and reputable antivirus software;
- Ensure that devices are not left unattended or exposed;
- Install security updates of browsers and systems monthly or as soon as updates are available;
- Log into company accounts and systems through secure and private networks only; and

- All staff members are discouraged from accessing internal systems through other people's or external devices.

E-mails often host scams and malicious software.

To avoid virus infection or data theft staff members are advised to:

- Avoid opening attachments and clicking on links when the content is not adequately explained. For example, videos with the tagline of "Watch this video, it's amazing" "Or what she does next, will amaze you", should be treated with caution;
- Be suspicious and vigilant against suspicious email titles. For example, an email that offers an extravagant prize;
- Carefully check the names of the sender to ensure that the email is from a legitimate source;
- Carefully scan the email for inconsistencies or giveaways, such as unusual language or grammar patterns or errors; and
- If a staff member is unsure about an e-mail, they can consult the policy owner or the organisation's deputy information officer.

d. Availability of Systems

Staff members are expected to maintain the availability of systems, services, and information when required by the business or its clients. In the case of a cybercrime, reasonable measures must be taken by all staff members involved to maintain evidence of the crime, which is to be handed over to the South African Police Services.