MEAGO

# ELECTRONIC DATA CYBER SECURITY POLICY

2022

www.meago.coza

## 2018.04 ELECTRONIC DATA & CYBER SECURITY POLICY (v.1)

- A policy is a formal statement of intent that is uniform across the organisation.
- Policies are implemented as high-level building foundations and should reflect the organisation's objectives.
- Policies must be created with the intent to be in place for several years and regularly reviewed with approved changes made as needed.
- Any member of the organisation's governing body may authorise the adoption of this policy by signing the Policy Adoption section.
- The contents and format of this document are provided as an example only. It is the responsibility of the user to customise the document to the user's specific needs, circumstances and applicable legislation.
- Disclaimer: This document is of a generic nature and was compiled taking relevant statutory requirements into consideration. This document is provided as a guideline only and any reliance the user places on this document will be at the user's own risk. Moonstone accepts no liability for any damages suffered or losses incurred arising from the use of this document.
- Copyright: The content of this document is the copyright of Moonstone Compliance (Pty) Ltd. All rights reserved. You may not, except with Moonstone's express written permission, distribute or commercially exploit the contents of this document.

# TABLE OF CONTENTS

## 1. INTRODUCTION

According to the 2017 Norton Report on Cyber Crime, 978 million people in 20 countries were affected by cybercrime in the year of 2017 alone. The report goes on to state that, consumers who were victims of cybercrime globally lost $172 billion. Given the rise in cybercrime and its extensive cost, there is a need for organisations to adopt effective cyber security measures.

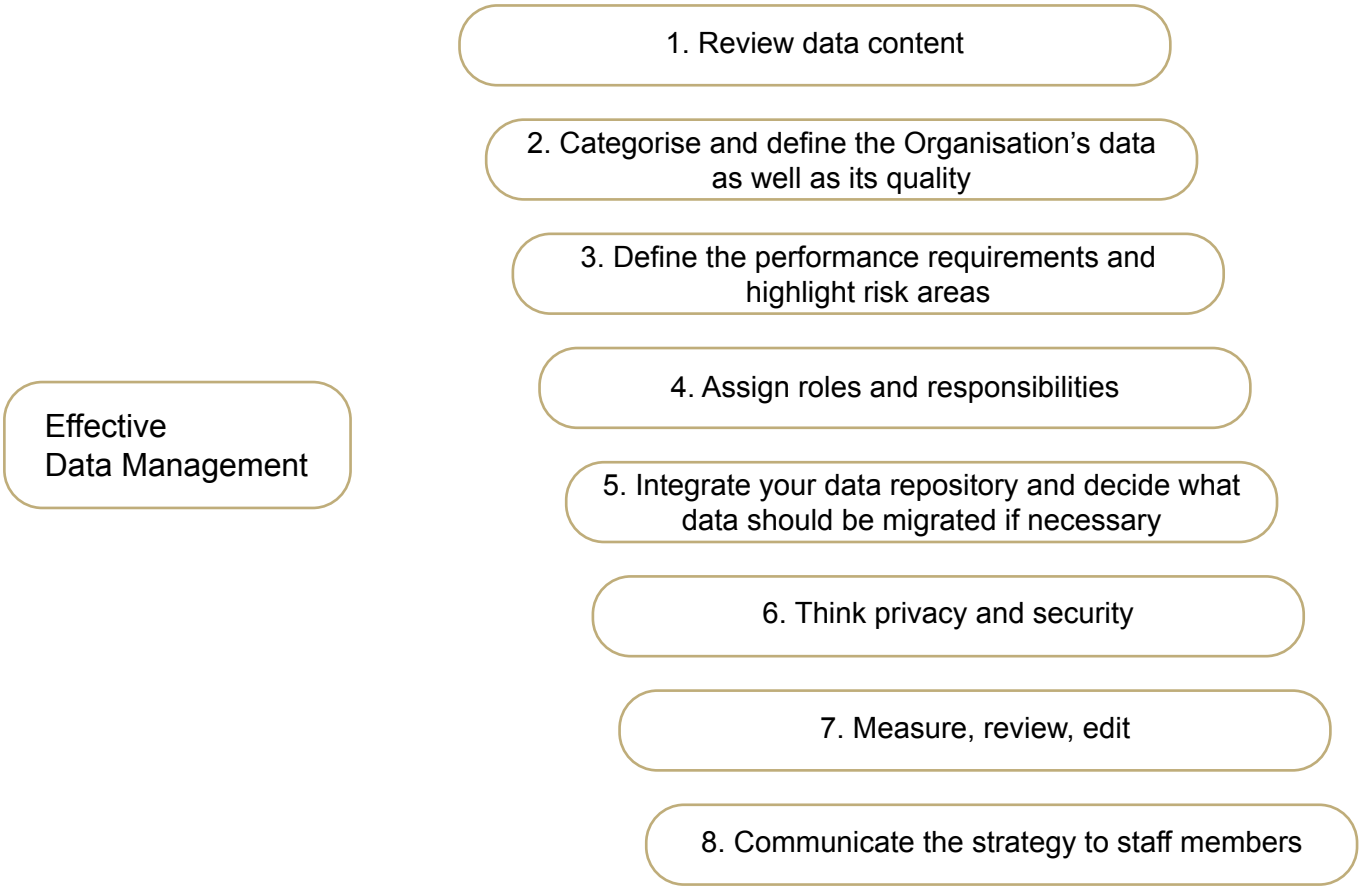
Some examples of the forms of Cyber Crime affecting businesses include:

1. Email spoofing (creating email messages with a forged sender address);
2. Malware (software used to disable or damage computers);
3. Phishing (attempting to obtain personal information, such as a password, by disguising as a trustworthy source in an email); and
4. Ransomware (malicious software designed to block access to a computer system, until a ransom amount is paid).

Given the negative socio-economic impact of cyber-crime, 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.

The primary goal of this policy is to secure data. However, in the case of a data breach, this policy also aims to ensure that the organisation is able to efficiently respond and recover from the breach in a manner that minimises any loss to the organisation and its clients.

Effective Data



## 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 defined as a crime in which a computer or the internet is the object of the crime (examples of this include hacking, phishing or spamming). Cyber crimes also encompasses crimes where computers or the internet are used as the tool to commit the offense (examples of this include child pornography and hate crimes). Other common types of cybercrime include online bank information theft, identity theft, online predatory crimes and unauthorised computer access.

### 2.4 Cyber Security
Cyber security is not just about technology and computers. It involves people, information systems, processes, culture and physical surroundings as well as the effective management of technology.

### 2.5 Extra-Territorial
The GDPR has extra-territorial application, meaning that if an organisation processes personal data through the provision of goods and services (even free services) in the EU or even outside the EU (to EU customers) the organisation must comply with the GDPR requirements. This application also includes companies based in the EU who are transferring data to be processed outside of the EU.

### 2.6 GDPR
The General Data Protection Regulation (GDPR) is a legal framework that sets guidelines for the collection and processing of personal information of individuals within the European Union (EU) The GDPR comes into effect across the EU on May 25, 2018.

### 2.7 Personal Information
Both the South African Protection of Personal Information Act of 2013 (“POPI”) and the EU’s General Data Protection Regulation of 2016 (“GDPR”) protect and define personal information. As POPI contains a broader definition of personal information (PI), POPI’s definition is used in this policy. PI refers 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.

### 2.8 Privacy by Design
The concept of privacy by design is mandated by Article 25 of the GDPR. Privacy by Design is a framework based on proactively embedding privacy into the design and operation of IT systems, networked infrastructure, and business practices. The foundational principles of privacy by design include:

- A proactive approach- as opposed to a reactive approach.
- The default position must be one based on protecting privacy.
- Privacy must be embedded into the design and architecture of information technology systems and business processes.
- Privacy should not be seen as a zero-sum game. It can be a win-win situation.
- Security should be extended to the entire life cycle of the Personal Information / data.
- The emphasis is on visibility and transparency.
- User privacy must be respected.

## 3. POLICY PURPOSE

### 3.1 PROTECTING THE ORGANISATION

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 new Cyber Security Bill introduces new crimes such as hacking, unlawful interception of data, ransomware, cyber forgery and uttering and cyber extortion. The Bill also creates new duties (for financial institutions) to report these crimes.

While not yet enacted, the Cybercrimes and Cybersecurity Bill states that if 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 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. While the Bill has not yet been enacted, it is considered a best practice to report cyber crimes to the South African Police Services and to retain and hand over any evidence that can be used by the Police Services.
The privacy of the organisation's 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 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. Given that the GDPR has extra-territorial application, the GDPR has also been consulted in drafting this policy. This comparative approach is further justified as the GDPR will inevitably influence South Africa while providing guidance on best practices concerning data protection. The extra-territorial application of the GDPR also includes companies based in the EU who are transferring data to be processed outside of the EU.
- It is up to the organisation to determine the extent to which the GDPR applies (or to which other

jursidictional laws apply) to their organisation and to tailor this policy to the specific needs and risks facing the organisation.

## 5. CYBERSECURITY RISK REGISTER

The organisation will identify and catalogue potential risk areas:

### 5.1 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 on a monthly basis). |
| **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. |

### 5.2 RISK REGISTER

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

## 6. STAFF MEMBER DUTIES

### 6.1 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.

### 6.2 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.

### 6.3 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
- Choose and upgrade a complete 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.
- All staff members are discouraged from accessing internal systems through other people's devices.

Emails 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.
- If a staff member is unsure about an email, they can consult the policy owner or the organisation's data protection officer.

### 6.4 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.