

Electronic Data and Cyber Security Policy for Prime Circle Finance (Pty) Ltd, FSP Number 53768

1. INTRODUCTION

According to the 2021 Norton Cyber Insights Report, despite a year of restrictions and lock downs, cyber criminals were undeterred in their attacks against consumers in 10 countries including Australia, France, Germany, India, Japan, New Zealand, UK, and US.

In the past 12-months:-

- Nearly 330 million people experienced cyber crime
- Nearly 2.7 billion hours were lost, with people spending an average of nearly 7-hours trying to resolve the issues created
- Nearly 208 million people in 10 countries have experienced identity theft and 55 million people were victimised in the past 12-months alone.

Globally consumers are taking steps to hide their online footprint, i.e., to protect their online activity and personal information with:-

- 48% created stronger passwords
- 38% limited information shared on social media

With the insurance sector's high use of data and technology, the door has been opened to a wide range of cyber risks. Cyber risk management is one of the biggest business risks facing 21st century firms and cyber risk management has to be taken seriously at the highest level. Employees represent the biggest vulnerability in cyber defences, with the smallest IT security 'slip' being enough to bring down an entire firm.

Up until recently, there was no dedicated cybersecurity statute in South Africa. Provisions relating to cybersecurity are fragmented and found in various pieces of legislation.

- The Electronic Communications and Transactions Act No 25 of 2002 ("ECTA") contains several provisions specifically addressing cybercrime.
- The Regulation of Interception of Communications and Provision of Communication-related Information Act No 70 of 2002 ("RICA") is aimed at, amongst others, regulating the interception of certain communications.
- The Criminal Procedure Act No 51 of 1977 ("CPA") contains provisions dealing with the investigation and prosecution of crimes (including cybercrimes) in South Africa.
- POPI promotes the protection of personal information processed by public and private bodies and introduces certain conditions to establish minimum requirements for the processing of personal information. See "Data Protection" section above for full details of data protection laws.

The partial commencement of the new Cybercrimes Act 19 of 2020 ("Act") on 1 December 2021, brings a sigh of relief to internet users as it aims to combat and prosecute cybercrime. South Africa is heavily targeted by cybercriminals due to its lack of infrastructure, security, legislation, enforcement, and understanding of online security. Legal authorities and the judiciary will now have more concrete legal grounds on which to investigate and prosecute cybercrimes than ever before.

However, it still remains to be seen how the Act will be interpreted and applied, especially considering its interrelation with the Protection of Personal Information Act 4 of 2013 (POPIA). What is clear is that the Act bolsters the position of POPIA and creates different forms of liability under each piece of legislation for the same data breach.

A wide net has been cast to include a range of activities involving data, computers, networks, and electronic communications that will be impacted. Significant progress has been made in criminalising certain online conduct such as distributing intimate images (better known as 'revenge porn') and inciting or threatening violence or damage to property. Another form of cybercrime is being in possession of or using someone else's access code or passwords to gain

access to unauthorised information, where no exculpatory explanation can be provided.

It is vital for companies to understand the impact of the Act and its interplay with POPIA, as a company may have obligations under both, but to varying degrees. It is quite possible that a single event can trigger both pieces of legislation and a company will be required to act within varying timeframes that run concurrently. The Act also imposes additional obligations on certain institutions such as financial institutions and electronic communications service providers.

The Act imposes a specific duty on financial institutions and electronic communications service providers (such as internet service providers, telecommunications network operators, etc.) to report any cybercrime that it becomes aware of, within 72 hours to the South African Police Service and to assist them (at the institution's cost) by preserving any evidence in relation to the cybercrime. Failing to do so, will result in a fine of R50 000 being imposed on these institutions. Notably, these obligations do not apply to the Financial Sector Conduct Authority or the Reserve Bank.

The Act criminalises the possession or use of access codes to restricted computer systems used by financial institutions. Training and awareness on the impact of the Act will be an unquestionable necessity.

Offences and penalties created by the Act, which companies and institutions should take into account, include:

Offence	Penalty
Acquiring, viewing, or copying non-public information through the use of hardware or software, to disclose that information to a person who is not the lawful owner or holder	Fine and / or imprisonment of up to 5-years
Permanently or temporarily deleting or altering	Fine and / or imprisonment

data, computer program, system, or storage medium	of up to 10-years
Revenge pornography and other malicious communications inciting violence or damage to property	Fine and / or imprisonment of up to 5-years
Acquisition, possession, or use of passwords or access codes	Fine and / or imprisonment of up to 5 to 10-years

Given the rise in cybercrime and its extensive cost, there is a need for organisations to adopt effective cyber security measures.

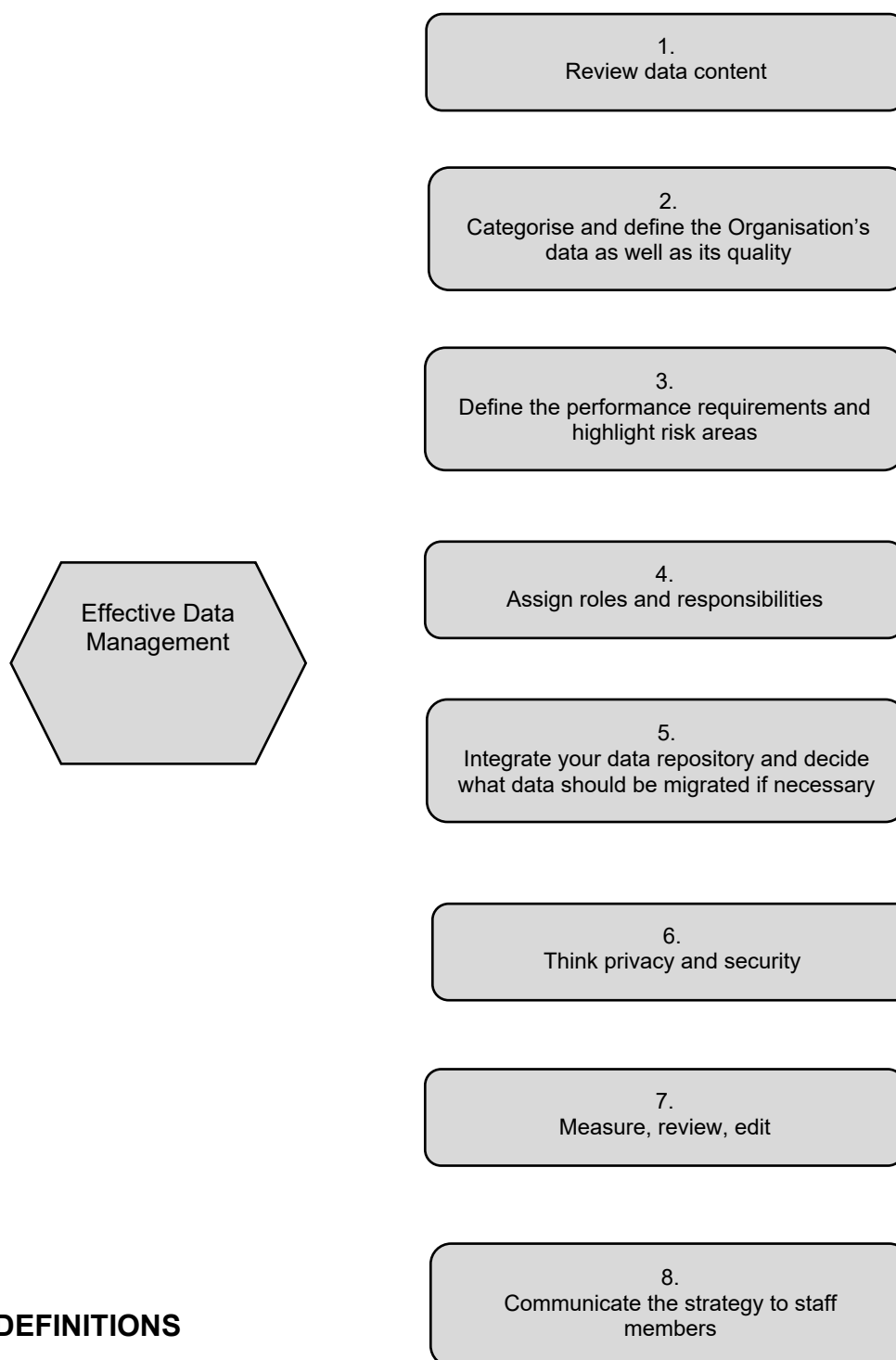
Some examples of the forms of Cyber Crime affecting businesses include:-

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.

Cyber Security management involves



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

The organisation must also preserve any information, at the institution's own cost, which may be of assistance to the law enforcement agencies in investigating the offence with the obligation in terms of the new Cybercrimes Act of reporting any cybercrime that it becomes aware of, within 72 hours to the South African Police Service.

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 jurisdictional 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:

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.

RISK REGISTER

Risk ID	Last Review	Risk Description	Risk Owner	Likelihood Rating	Impact Rating	Risk Rating	Control Measures
---------	-------------	------------------	------------	-------------------	---------------	-------------	------------------

	Date					(L x I)	
		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 members 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 assets 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 mobile 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.

7. POLICY ADOPTION

By signing this document, I authorise the organisation's approval and adoption of the processes and procedures outlined herein.

Name & Surname	Joly Joseph Zziwa Taboola
Capacity	CEO
Signature	
Date	05/05/2025