

Cyber Crime Warning and Disclosure

Compliance Collective (Pty) Ltd

Table of Contents

1. Overview	3
1.1 Document history	3
1.2 Governance approvals.....	3
2. Introduction.....	3
3. Scope	4
4. Purpose	4
5. Policy Statement.....	4
6. Cybersecurity.....	4
7. Cybercrime	5
8. Cybersecurity risk examples	5
9. Cybercrime examples.....	6
10. Cybercrime categories.....	6
11. How to protect yourself against cybercrime	6
12. Steps to identify risks, to address it, and ensure cybersecurity awareness	7
12.1 Identifying threats:.....	8
12.2 Identifying vulnerabilities:.....	8
12.3 Assessing risk exposure:.....	8
12.4 Developing protection and detection measures:.....	8
12.5 Establishing contingency plans:	8
12.6 Responding to cyber security incidents:	8
13. Minimum security controls	8
14. Responsibilities.....	9
15. Incident response	9
16. Review of this Policy.....	10

1. Overview

1.1 Document history

Revision date	Document version	Summary changes	Author / Reviewer
June 2026	1	Initial drafting	Madeleen van Schalkwyk
October 2026	1.1	Compliance review: legal basis corrected, scope widened, training commitments scaled, minimum security controls and incident response added	Madeleen van Schalkwyk

1.2 Governance approvals

Name	Nature	Document version	Approval signature	Date of approval
Director	Approval	1.1	Approved	07/10/2026

2. Introduction

There is various legislation in SA that addresses Cybersecurity and Crimes issues, of which the most important recent legislation is the Cybercrimes Act 19 of 2020. It aims to address cybercrime and criminalises offences such as unlawful access to data, unlawful interception of data, unlawful intentional use or possession of software/ tools used to conduct cybercrimes, cyber fraud, cyber extortion, cyber forgery and uttering and malicious communications aiming to cause damage/ violence etc. It also contains provisions dealing with investigation of cybercrimes, the provision of mutual assistance between States, as well as reporting obligations of electronic communications service providers and financial institutions. The Company is not an electronic communications service provider or a financial institution, so the reporting obligation in section 54 of that Act does not apply to it.

The Company is a responsible party under the Protection of Personal Information Act 4 of 2013 (POPIA). Section 19 of POPIA requires the Company to secure the integrity and confidentiality of the personal information in its possession by taking appropriate, reasonable technical and organisational measures. Section 22 requires it to notify the Information Regulator and the affected data subjects if that information is compromised.

The Company is also an accountable institution under the Financial Intelligence Centre Act 38 of 2001 (FICA) and must keep its client due diligence and transaction records secure and available for the periods prescribed by that Act.

3. Scope

This policy applies to the director and all employees of the Company, including full-time, part-time and temporary staff, and to contractors and third-party service providers who have access to the Company's systems or information (together, "staff").

4. Purpose

This Policy aims to make staff aware of Cyber security risks and crimes, their responsibility to report any risks to the director of the Company without delay and the steps to be taken by the Company to ensure that risks are identified and addressed as to prevent cybersecurity attacks and breaches in the Company's business. It also sets the minimum security rules that staff must follow when using the Company's systems and handling client information.

The Policy also aims to foster a culture of continuous learning and development, ensuring that the Company's staff are equipped with up-to-date knowledge and skills relevant to their roles, particularly in cybersecurity and the protection of client information.

5. Policy Statement

- **Induction:** The director, all employees and any contractor given access to the Company's systems will be made aware of this Policy before that access is given, and will confirm in writing that they have read it.
- **Annual awareness training:** The director and all employees will complete cybersecurity and cybercrime awareness training at least once a year. The training may be delivered in-house, online or by an external provider.
- **Alerts:** The Company will inform staff of new or emerging threats as they arise.
- **Records:** The Company will keep a register of the training completed by each person and the date on which it was completed.

6. Cybersecurity

Cybersecurity, also known as information technology (IT) security, is the practice of protecting critical systems and sensitive information from digital attacks. Cybersecurity measures are designed to combat threats against networked systems and applications, whether those threats originate from inside or outside of an organisation.

7. Cybercrime

Cybercrime is criminal activity that either targets or uses a computer, a computer network or a networked device. Most cybercrime is committed by cybercriminals or hackers who want to make money and can be carried out by individuals or organisations. Some cybercriminals are organised and can use advanced techniques and may also be highly technically skilled, where others may only be novice hackers.

8. Cybersecurity risk examples

The following are examples of recent well-known Cybersecurity risks:

- **Malware:** Refers to malicious software e.g., worms, viruses, Trojans, and spyware. It provides unauthorised access or cause damage to a computer. A computer compromised by malware could be used by cybercriminals for several purposes. These include stealing confidential data, using the computer to carry out other criminal acts, or causing damage to data.
- **Ransomware:** Is a type of malware that locks down files, data or systems and threatens to erase or destroy the data or to make private or sensitive data available to the public, unless a ransom is paid to the cybercriminals who launched the attack.
- **Phishing / social engineering:** It tricks users into providing personal or sensitive information. In phishing scams, the emails or text messages appear to be from a legitimate company asking for sensitive information, such as credit card data or login information. The intention is of tricking users into doing something that undermines their security or the security of the organisation they work for.
 - Mass phishing campaigns, which are very general in style, may contain infected attachments or links to malicious sites. Or they may ask the receiver to respond with confidential information.
 - Spear-phishing is another type of phishing which try to trick specific individuals into jeopardising the security of the organisation they work for. Spear-phishing messages are typically crafted to look like messages from a trusted source. For example, they are made to look like they have come from the CEO or the IT manager. They may not contain any visual clues that they are fake.
- **Insider threats:** Current or former employees, business partners, contractors, or anyone who has had access to systems or networks of an organisation can be considered an insider threat if they abuse their access permissions.
- **Distributed denial-of-service attacks (DDoS):** Attempts to crash a server, website, or network by overloading it with traffic, usually from multiple coordinated systems. DDoS is a type of cybercrime attack that the cybercriminals use to bring down a system or network. Sometimes connected IoT (internet of things) devices are used to launch DDoS attacks. It overwhelms a system by using one of the standard communication protocols it uses to spam the system with connection requests. Cybercriminals who are carrying out cyberextortion may use the threat of a DDoS attack to demand money. Alternatively, a DDoS may be used as a distraction tactic while other type of cybercrime takes place.
- **Advanced persistent threats:** An intruder or group of intruders infiltrate a system and remain undetected for an extended period. The intruder leaves networks and

systems intact so that the intruder can spy on business activity and steal sensitive data while avoiding the activation of defensive countermeasures.

- **Man-in-the-middle attacks:** Man-in-the-middle is where a cybercriminal intercepts and relays messages between two parties in order to steal data. For example, on an unsecure Wi-Fi network, an attacker can intercept data being passed between guest's device and the network.

9. Cybercrime examples

Specific examples of Cybercrimes include:

- Email and internet fraud,
- Identity fraud (where personal information is stolen and used), theft of financial or card payment data, theft, and sale of corporate data,
- Cyberextortion (demanding money to prevent a threatened attack),
- Ransomware attacks (a type of cyberextortion),
- Cryptojacking (where hackers mine cryptocurrency using resources they do not own),
- Cyberespionage (where hackers access government or company data).

10. Cybercrime categories

Cyber Crime falls under the following categories:

- **Criminal activity that *targets* computers:** This often involves viruses and other types of malware. Cybercriminals may infect computers with viruses and malware to damage devices or stop them working. They may also use malware to delete or steal data. Cybercrime that stops users using a machine or network or prevents a business providing a software service to its customers, is called a Denial-of-Service (DoS) attack.
- **Criminal activity that uses computers to commit other crimes:** This may involve using computers or networks to spread malware, illegal information, or illegal images. Cybercriminals may also carry out what is known as a Distributed-Denial-of-Service (DDoS) attack. This is similar to a DoS attack, but cybercriminals use numerous compromised computers to carry it out.
- **Combination:** Sometimes Cyber Criminals conduct both categories of cybercrime at once. They may target computers with viruses first. Then, use them to spread malware to other machines or throughout a network.

11. How to protect yourself against cybercrime

The following are tips to protect the Company and staff against Cybersecurity risks and Cybercrimes:

- **Keep software and operating system updated:** Keeping software and operating system up to date ensures that you benefit from the latest security patches to protect your computer.
- **Use anti-virus software and keep it updated:** Using anti-virus or a comprehensive internet security solution is a smart way to protect your system from attacks. Anti-

virus software allows you to scan, detect and remove threats before they become a problem. Having this protection in place helps to protect your computer and your data from cybercrime, giving you peace of mind. If you use anti-virus software, make sure you keep it updated to get the best level of protection.

- **Use strong passwords:** Be sure to use strong passwords that people will not guess and do not write them down or share them. Use a reputable password manager to generate strong passwords randomly to make this easier.
- **Never open attachments in spam emails:** A classic way that computers get infected by malware attacks and other forms of cybercrime is via email attachments in spam emails. Never open an attachment from a sender you do not know.
- **Do not click on links in spam emails or untrusted websites:** Another way people become victims of cybercrime is by clicking on links in spam emails or other messages, or unfamiliar websites. Avoid doing this to stay safe online.
- **Do not give out personal information unless secure:** Never give out personal data over the phone or via email unless you are completely sure the line or email is secure. Make certain that you are speaking to the person you think you are.
- **Contact companies directly about suspicious requests:** If you get asked for data from a company who has called you, hang up. Call them back using the number on their official website to ensure you are speaking to them and not a cybercriminal. Ideally, use a different phone because cybercriminals can hold the line open. When you think you've re-dialled, they can pretend to be from the bank or other organisation that you think you're speaking to.
- **Be mindful of which website URLs you visit:** Keep an eye on the URLs you are clicking on. Do they look legitimate? Avoid clicking on links with unfamiliar or spammy looking URLs. If your internet security product includes functionality to secure online transactions, ensure it is enabled before carrying out financial transactions online.
- **Keep an eye on your bank statements:** Our tips should help you avoid falling foul of cybercrime. However, if all else fails, spotting that you have become a victim of cybercrime quickly is important. Keep an eye on your bank statements and query any unfamiliar transactions with the bank. The bank can investigate whether they are fraudulent.

12. Steps to identify risks, to address it, and ensure cybersecurity awareness

The Company will carry out the risk assessment described below at least once a year, and whenever its systems or service providers change materially, and will record the outcome.

The Company will ensure that the following steps are followed to identify Cybersecurity risks, to address it, and to ensure awareness to staff of applicable Cybersecurity risks in the Company:

12.1 Identifying threats:

Understanding external and internal Cybersecurity risks is important so that the required controls are implemented to avoid/ minimise these risks. Attackers are always looking for new ways to access sensitive information by exploiting weaknesses e.g. work-from-home environments, remote access tools and new cloud services.

12.2 Identifying vulnerabilities:

When identifying vulnerabilities, it is important to understand the consequences of cyber security threats in systems and the capabilities and limitations of existing protection measures in systems e.g., a system with direct or indirect communication links.

12.3 Assessing risk exposure:

Risk exposure can be assessed by means of determining the likelihood of vulnerabilities:

- being exploited by external threats;
- being exposed by inappropriate use; or
- in respect of the security and safety impact of any individual or combination of vulnerabilities being exploited.

12.4 Developing protection and detection measures:

Developing protection and detection measures will result in reducing the likelihood of vulnerabilities being exploited through protection measures and reducing the potential impact of a vulnerability being exploited.

12.5 Establishing contingency plans:

Developing a response plan to reduce the impact of threats in respect of the safety and security of the Company.

12.6 Responding to cyber security incidents:

Responding to cyber security threats that are realised by using the response plan, to assess the impact of the effectiveness of the response plan and re-assess the threats and vulnerabilities.

13. Minimum security controls

The Company and its staff will apply the following minimum controls:

- Access to the Company's systems and to client information is limited to staff who need it for their work, and is removed promptly when a staff member or contractor leaves.

- Multi-factor authentication must be enabled wherever it is available, in particular on email, cloud storage, SARS eFiling, CIPC, goAML and the Company's client due diligence platform.
- Login details for these platforms are personal to the user and may not be shared. Passwords must be unique to each platform and may only be stored in a password manager approved by the Company.
- Laptops, phones and other devices used for Company work must be protected by a password or biometric lock, encrypted where the device allows it, kept up to date and protected by anti-virus software.
- Client information may only be stored on systems approved by the Company. It may not be saved to personal email accounts, personal cloud storage or removable media.
- Documents containing identity numbers, tax information or banking details must be sent by a secure method, such as a password-protected file or a secure sharing link.
- Any instruction received by email to change banking details or to make a payment must be verified by telephone, using a number already on record, before it is acted on.
- Public Wi-Fi may not be used for Company work unless a secure connection, such as a VPN or a personal hotspot, is used.
- Company data is backed up at least weekly, and the director tests at least twice a year that the backups can be restored.
- Third-party service providers who host or have access to the Company's information must be bound by a written agreement that requires them to keep the information secure, to notify the Company immediately of any suspected compromise of personal information, and to cooperate with the Company's investigation, including by preserving evidence.

14. Responsibilities

Staff is required to inform the director immediately, by telephone and by email, should they become aware of any of these Cybersecurity risks or if any new Cybersecurity risks would come to their attention, so that the Company can address it without delay. Likewise, the Company will keep staff informed of any risks staff should be aware of. Failure to report and especially involvement in any of these activities by staff will result in the required action being taken against staff, which may include disciplinary action and dismissal, if appropriate.

15. Incident response

When a cybersecurity incident or suspected incident is reported, the director will:

- take immediate steps to contain the incident, such as isolating the affected device, changing passwords and revoking access, while preserving logs and other evidence;
- establish what information, and which clients or other data subjects, are affected;
- where there are reasonable grounds to believe that personal information has been accessed or acquired by an unauthorised person, notify the Information Regulator through its eServices portal, and the affected data subjects in writing, as soon as reasonably possible, as required by section 22 of POPIA;
- consider whether the incident must also be reported to the South African Police Service, the Company's bank, the South African Revenue Service or any other affected platform or regulator;

- restore affected systems and data from verified backups, and confirm that the cause of the incident has been addressed; and
- record the incident, the action taken, the lessons learned and the date on which the incident was closed in the Company's incident register.

Emergency contacts: Director: 072 513 2683. IT service provider: Crimson Line 086 111 4496 . Alternate contact if the director is unavailable: Nic van Schalkwyk 072 513 2684.

16. Review of this Policy

This Policy will be reviewed at least once a year, and after any significant cybersecurity incident or material change to the Company's systems or service providers.