Contents

1.0 Policy statement

The Mauritius Data Protection Act 2017 regulates the future processing of all personal data in the Mauritius. Drafted around a set of internationally recognised privacy principles, the new law provides a framework of rights and duties designed to give individuals greater control over their personal data and will stand as the most comprehensive data protection law in the region. We are committed to implement appropriate measures to protect all data that we are responsible for as well as comply with all provisions of the Mauritius Data Protection & Cybersecurity Laws.

2.0 Purpose

This is the Cyber Security Policy of Oneprime Ltd and serves several purposes. Oneprime Ltd with the tradename ('Tredero') is a company registered in Mauritius, with Principal and Registered Office at King George VI Avenue, Floreal, Mauritius (hereinafter 'the Company'). The Company is authorized and regulated by the Mauritius Financial Services Commission ('FSC') with licence number GB20025316.

The main purpose of the Cyber Security Policy is to inform Company users: employees, contractors and other authorized users of their obligatory requirements for protecting the technology and information assets of the company. The Cyber Security Policy describes the technology and information assets that we must protect and identifies many of the threats to those assets.

The Cyber Security Policy also describes the user's responsibilities and privileges. What is considered acceptable use? What are the rules regarding Internet access? The policy answers these questions, describes user limitations and informs users there will be penalties for violation of the policy. This document also contains procedures for responding to incidents that threaten the security of the company computer systems and network.

Our Company Cyber Security Policy outlines our guidelines and provisions for preserving the security of our data and technology infrastructure.

The more we rely on technology to collect, store and manage information, the more vulnerable we become to severe security breaches. Human errors, hacker attacks and system

malfunctions could cause great financial damage and may jeopardize our company's reputation.

For this reason, we have implemented a number of security measures. We have also prepared instructions that may help mitigate security risks. We have outlined both provisions in this policy.

3.0 Scope

This policy applies to all our employees, contractors, volunteers and anyone who has permanent or temporary access to our systems and hardware.

4.0 Key Elements of the Policy

The following are the key elements of this policy:

- Cybersecurity governance and risk assessment processes
- Access Rights and Controls
- Data Loss Prevention
- Vendor Management
- Training
- Incident response plan

5.0 Plan and Processes

Measure	Key Provisions
Keep all devices password protected.	1. Choose and upgrade a complete antivirus software. 2. Ensure they do not leave their devices exposed or unattended. 3. Install security updates of browsers and systems monthly or as soon as updates are available. 4. Log into company accounts and systems through secure and private networks only. 5. We also advise our employees to avoid accessing internal systems and accounts from other people's devices or lending their own devices to others.

	6. When new hires receive company-issued equipment they will receive instructions for: • [Disk encryption setup] • [Password management tool setup] • [Installation of antivirus/ anti-malware software] • They should follow instructions to protect their devices and refer to our [Security Specialists/ Network Engineers] if they have any questions.
Keep emails safe	Emails often host scams and malicious software (e.g. worms.) To avoid virus infection or data theft, we instruct employees to: • Avoid opening attachments and clicking on links when the content is not adequately explained (e.g. "watch this video, it's amazing.") • Be suspicious of clickbait titles (e.g. offering prizes, advice.) • Check email and names of people they received a message from to ensure they are legitimate. • Look for inconsistencies or give-aways (e.g. grammar mistakes, capital letters, excessive number of exclamation marks.) • If an employee isn't sure that an email they received is safe, they can refer to our [IT Specialist.]
Manage passwords properly	Password leaks are dangerous since they can compromise our entire infrastructure. Not only should passwords be secure so they won't be easily hacked, but they should also remain secret. For this reason, we advice our employees to: 1. Choose passwords with at least eight characters (including capital and lower-case letters, numbers and symbols) and avoid information that can be easily guessed (e.g. birthdays.) 2. Remember passwords instead of writing them down. If employees need to write their passwords, they are obliged to keep the paper or digital document confidential and destroy it when their work is done.

	3. Exchange credentials only when absolutely necessary. When exchanging them in-person isn't possible, employees should prefer the phone instead of email, and only if they personally recognize the person they are talking to. 4. Change their passwords every two months. 5. We will purchase the services of a password management tool which generates and stores passwords. Employees are obliged to create a secure password for the tool itself, following the abovementioned advice.
Transfer data securely	Transferring data introduces security risk. Employees must: 1. Avoid transferring sensitive data (e.g. customer information, employee records) to other devices or accounts unless absolutely necessary. When mass transfer of such data is needed, we request employees to ask our [Security Specialists] for help. 2. Share confidential data over the company network/ system and not over public Wi-Fi or private connection. 3. Ensure that the recipients of the data are properly authorized people or organizations and have adequate security policies.
Report scams, privacy breaches and hacking attempts	Our [IT Specialists/ Network Engineers] need to know about scams, breaches and malware so they can better protect our infrastructure. For this reason, we advise our employees to report perceived attacks, suspicious emails or phishing attempts as soon as possible to our specialists. Our [IT Specialists/ Network Engineers] must investigate promptly, resolve the issue and send a companywide alert when necessary. Our Security Specialists are responsible for advising employees on how to detect scam emails. We encourage our employees to reach out to them with any questions or concerns.
Additional measures	To reduce the likelihood of security breaches, we also instruct our employees to: 1. Turn off their screens and lock their devices when leaving their desks.

	2. Report stolen or damaged equipment as soon as possible to [HR/ IT Department]. 3. Change all account passwords at once when a device is stolen. 4. Report a perceived threat or possible security weakness in company systems. 5. Refrain from downloading suspicious, unauthorized or illegal software on their company equipment.
Avoid accessing suspicious websites.	We also expect our employees to comply with our social media and internet usage policy. Our [Security Specialists/ Network Administrators] should: ● Install firewalls, anti-malware software and access authentication systems. ● Arrange for security training to all employees. ● Inform employees regularly about new scam emails or viruses and ways to combat them. ● Investigate security breaches thoroughly. ● Follow this policies provisions as other employees do. ● Our company will have all physical and digital shields to protect information. *Remote employees* *Remote employees must follow this policy's instructions too. Since they will be accessing our company's accounts and systems from a distance, they are obliged to follow all data encryption, protection standards and settings, and ensure their private network is secure.* *We encourage them to seek advice from our [Security Specialists/ IT Administrators.]*
Take security seriously	Everyone, from our customers and partners to our employees and contractors, should feel that their data is safe. The only way to gain their trust is to proactively protect our systems and databases. We can all contribute to this by being vigilant and keeping cyber security top of mind.

6.0 Classification of Computer Systems

Security Level	Description	Example
RED	This system contains confidential information – information that cannot be revealed to personnel outside of the company. Even within the company, access to this information is provided on a "need to know" basis. The system provides mission-critical services vital to the operation of the business. Failure of this system may have life threatening consequences and/or an adverse financial impact on the business of the company.	Server containing confidential data and other department information on databases. Network routers and firewalls containing confidential routing tables and security information.
GREEN	This system does not contain confidential information or perform critical services, but it provides the ability to access RED systems through the network.	User department PCs used to access Server and application(s). Management workstations used by systems and network administrators.
WHITE	This system is not externally accessible. It is on an isolated LAN segment, unable to access RED or GREEN systems. It does not contain sensitive information or perform critical services.	A test system used by system designers and programmers to develop new computer systems.

BLACK	This system is externally accessible. It is isolated from RED or GREEN systems by a firewall. While it performs important services, it does not contain confidential information.	A public Web server with non-sensitive information.

7.0 Local Area Network (LAN) Classifications

A LAN will be classified by the systems directly connected to it. For example, if a LAN contains just one RED system and all network users will be subject to the same restrictions as RED systems users. A LAN will assume the Security Classification of the highest-level systems attached to it.

8.0 Threats to Security

The following is a summary of key threats to cybersecurity:

Employees

One of the biggest security threats is employees. They may do damage to your systems either through incompetence or on purpose. You have to layer your security to compensate for that as well. You mitigate this by doing the following.

- Only give out appropriate rights to systems. Limit access to only business hours.
- Don't share accounts to access systems. Never share your login information with co-workers.
- When employees are separated or disciplined, you remove or limit access to systems.
- Advanced – Keep detailed system logs on all computer activity.
- Physically secure computer assets, so that only staff with appropriate need can access.

Amateur Hackers and Vandals.

These people are the most common type of attackers on the Internet. The probability of attack is extremely high and there is also likely to be a large number of attacks. These are usually crimes of opportunity. These amateur hackers are scanning the Internet and looking for well-known security holes that have not been plugged. Web servers and electronic mail are their favorite targets. Once they find a weakness they will exploit it to plant viruses,

Trojan horses, or use the resources of your system for their own means. If they do not find an obvious weakness they are likely to move on to an easier target.

Criminal Hackers and Saboteurs.
The probability of this type of attack is low, but not entirely unlikely given the amount of sensitive information contained in databases. The skill of these attackers is medium to high as they are likely to be trained in the use of the latest hacker tools. The attacks are well planned and are based on any weaknesses discovered that will allow a foothold into the network.

9.0 User Responsibilities

This section establishes usage policy for the computer systems, networks and information resources of the office. It pertains to all employees and contractors who use the computer systems, networks, and information resources as business partners, and individuals who are granted access to the network for the business purposes of the company.
Acceptable Use
User accounts on company computer systems are to be used only for business of the company and not to be used for personal activities. Unauthorized use of the system may be in violation of the law, constitutes theft and can be punishable by law. Therefore, unauthorized use of the company computing system and facilities may constitute grounds for either civil or criminal prosecution.

Users are personally responsible for protecting all confidential information used and/or stored on their accounts. This includes their logon IDs and passwords. Furthermore, they are prohibited from making unauthorized copies of such confidential information and/or distributing it to unauthorized persons outside of the company.

Users shall not purposely engage in activity with the intent to: harass other users; degrade the performance of the system; divert system resources to their own use; or gain access to company systems for which they do not have authorization.

Users shall not attach unauthorized devices on their PCs or workstations, unless they have received specific authorization from the employees' manager and/or the company IT

designee. Users shall not download unauthorized software from the Internet onto their PCs or workstations.

Users are required to report any weaknesses in the company computer security, any incidents of misuse or violation of this policy to their immediate supervisor.

Use of the Internet
The company will provide Internet access to employees and contractors who are connected to the internal network and who has a business need for this access. Employees and contractors must obtain permission from their supervisor and file a request with the Security Administrator.

The Internet is a business tool for the company. It is to be used for business-related purposes such as: communicating via electronic mail with suppliers and business partners, obtaining useful business information and relevant technical and business topics.

The Internet service may not be used for transmitting, retrieving or storing any communications of a discriminatory or harassing nature or which are derogatory to any individual or group, obscene or pornographic, or defamatory or threatening in nature for "chain letters" or any other purpose which is illegal or for personal gain

10.0 User Classification

All users are expected to have knowledge of these security policies and are required to report violations to the Security Administrator. Furthermore, all users must conform to the Acceptable Use Policy defined in this document. The company has established the following user groups and defined the access privileges and responsibilities:

User Category	Privileges & Responsibilities
Department Users (Employees)	Access to application and databases as required for job function. (RED and/or GREEN cleared)
System Administrators	Access to computer systems, routers, hubs, and other infrastructure technology required for job function. Access to confidential information on a "need to know" basis only.

Security Administrator	Highest level of security clearance. Allowed access to all computer systems, databases, firewalls, and network devices as required for job function.
Systems Analyst/Programmer	Access to applications and databases as required for specific job function. Not authorized to access routers, firewalls, or other network devices.
Contractors/Consultants	Access to applications and databases as required for specific job functions. Access to routers and firewall only if required for job function. Knowledge of security policies. Access to company information and systems must be approved in writing by the company director/CEO.
Other Agencies and Business Partners	Access allowed to selected applications only when contract or inter-agency access agreement is in place or required by applicable laws.
General Public	Access is limited to applications running on public Web servers. The general public will not be allowed to access confidential information.

Monitoring Use of Computer Systems

The company has the right and capability to monitor electronic information created and/or communicated by persons using company computer systems and networks, including e-mail messages and usage of the Internet. It is not the company policy or intent to continuously monitor all computer usage by employees or other users of the company computer systems and network. However, users of the systems should be aware that the company may monitor usage, including, but not limited to, patterns of usage of the Internet (e.g. site accessed, on-line length, time of day access), and employees' electronic files and messages to the extent necessary to ensure that the Internet and other electronic communications are being used in compliance with the law and with company policy.

11.0 Access Control

A fundamental component of our Cyber Security Policy is controlling access to the critical information resources that require protection from unauthorized disclosure or modification. The fundamental meaning of access control is that permissions are assigned to individuals or systems that are authorized to access specific resources. Access controls exist at various

layers of the system, including the network. Access control is implemented by logon ID and password. At the application and database level, other access control methods can be implemented to further restrict access. The application and database systems can limit the number of applications and databases available to users based on their job requirements.

User System and Network Access – Normal User Identification

All users will be required to have a unique logon ID and password for access to systems. The user's password should be kept confidential and MUST NOT be shared with management & supervisory personnel and/or any other employee whatsoever. All users must comply with the following rules regarding the creation and maintenance of passwords:

- Password must not be found in any English or foreign dictionary. That is, do not use any common name, noun, verb, adverb, or adjective. These can be easily cracked using standard "hacker tools".
- Passwords should not be posted on or near computer terminals or otherwise be readily accessible in the area of the terminal.
- Password must be changed every (# of days).
- User accounts will be frozen after (# of days) failed logon attempts.
- Logon IDs and passwords will be suspended after (# of days) days without use.

Users are not allowed to access password files on any network infrastructure component. Password files on servers will be monitored for access by unauthorized users. Copying, reading, deleting or modifying a password file on any computer system is prohibited.

Users will not be allowed to logon as a System Administrator. Users who need this level of access to production systems must request a Special Access account as outlined elsewhere in this document.

Employee Logon IDs and passwords will be deactivated as soon as possible if the employee is terminated, fired, suspended, placed on leave, or otherwise leaves the employment of the company office.

Supervisors / Managers shall immediately and directly contact the company IT Manager to report change in employee status that requires terminating or modifying employee logon access privileges.

Employees who forget their password must call the IT department to get a new password assigned to their account. The employee must identify himself/herself by (e.g. employee number) to the IT department.

Employees will be responsible for all transactions occurring during Logon sessions initiated by use of the employee's password and ID. Employees shall not logon to a computer and then allow another individual to use the computer or otherwise share access to the computer systems.

System Administrator Access

System Administrators, network administrators, and security administrators will have (type of access) access to host systems, routers, hubs, and firewalls as required to fulfil the duties of their job.

All system administrator passwords will be DELETED immediately after any employee who has access to such passwords is terminated, fired, or otherwise leaves the employment of the company.

Special Access

Special access accounts are provided to individuals requiring temporary system administrator privileges in order to perform their job. These accounts are monitored by the company and require the permission of the user's company IT Manager. Monitoring of the special access accounts is done by entering the users into a specific area and periodically generating reports to management. The reports will show who currently has a special access account, for what reason, and when it will expire.

Connecting to Third-Party Networks

This policy is established to ensure a secure method of connectivity provided between the company and all third-part companies and other entities required to electronically exchange information with company.

"Third-party" refers to vendors, consultants and business partners doing business with company, and other partners that have a need to exchange information with the company.

Third-party network connections are to be used only by the employees of the third-party, only for the business purposes of the company. The third-party company will ensure that only authorized users will be allowed to access information on the company network. The third- party will not allow Internet traffic or other private network traffic to flow into the network. A third-party network connection is defined as one of the following connectivity options:

- A network connection will terminate on a (to be specified) and the third-party will be subject to standard company authentication rules.

- This policy applies to all third-party connection requests and any existing third-party connections. In cases where the existing third-party network connections do not meet the requirements outlined in this document, they will be re-designed as needed.

All requests for third-party connections must be made by submitting a written request and be approved by the company.

Connecting Devices to the Network

Only authorized devices may be connected to the company network(s). Authorized devices include PCs and workstations owned by company that comply with the configuration guidelines of the company. Other authorized devices include network infrastructure devices used for network management and monitoring.

Users shall not attach to the network: non-company computers that are not authorized, owned and/or controlled by company. Users are specifically prohibited from attaching (specify) to the company network.

NOTE: Users are not authorized to attach any device that would alter the topology characteristics of the Network or any unauthorized storage devices, e.g. thumb drives and writable CD's.

Remote Access

Only authorized persons may remotely access the company network. Remote access is provided to those employees, contractors and business partners of the company that have a

legitimate business need to exchange information, copy files or programs, or access computer applications. Authorized connection can be remote PC to the network or a remote network to company network connection. The only acceptable method of remotely connecting into the internal network is using a secure ID.

Unauthorized Remote Access

The attachment of (e.g. hubs) to a user's PC or workstation that is connected to the company LAN is not allowed without the written permission of the company. Additionally, users may not install personal software designed to provide remote control of the PC or workstation. This type of remote access bypasses the authorized highly secure methods of remote access and poses a threat to the security of the entire network.

12.0 Penalty for Security Violation

The company takes the issue of security seriously.

Those people who use the technology and information resources of company must be aware that they can be disciplined if they violate this policy. Upon violation of this policy, an employee of company may be subject to discipline up to and including discharge. The specific discipline imposed will be determined by a case-by-case basis, taking into consideration the nature and severity of the violation of the Cyber Security Policy, prior violations of the policy committed by the individual, state and federal laws and all other relevant information. Discipline which may be taken against an employee shall be administrated in accordance with any appropriate rules or policies and the company Policy Manual.

In a case where the accused person is not an employee of company the matter shall be submitted to the (company designee). The (company designee) may refer the information to law enforcement agencies and/or prosecutors for consideration as to whether criminal charges should be filed against the alleged violator(s).

13.0 Security Incident Handling

This section provides some policy guidelines and procedures for handling security incidents. The term "security incident" is defined as any irregular or adverse event that threatens the

security, integrity, or availability of the information resources on any part of the company network. Some examples of security incidents are:

- Illegal access of a company computer system. For example, a hacker logs onto a production server and copies the password file.
- Damage to a company computer system or network caused by illegal access. Releasing a virus or worm would be an example.
- Denial of service attack against a company web server. For example, a hacker initiates a flood of packets against a Web server designed to cause the system to crash.
- Malicious use of system resources to launch an attack against other computer outside of the company network. For example, the system administrator notices a connection to an unknown network and a strange process accumulating a lot of server time.
- Employees, who believe their terminal or computer systems have been subjected to a security incident, or has otherwise been improperly accessed or used, should report the situation to their (company designee) immediately. The employee shall not turn off the computer or delete suspicious files. Leaving the computer in the condition it was in when the security incident was discovered will assist in identifying the source of the problem and in determining the steps that should be taken to remedy the problem.

14.0 Review and approval

This Cybersecurity policy shall be reviewed and approved by the board every once a year.

In case if any inconsistency between the policy and applicable legislations, rules and regulations, the latter shall prevail.

15.0 References and related documents

Associated policies	▪ Risk Management Policy

	▪ Corporate Governance Framework
References /statutory references	▪ Data Protection Act 2017