Cyber Security Policy

APPLICATION

This policy applies to all employees, and affiliates of:

Company/ies:	Laudian Investment Holdings (Pty) Ltd
	Company Reg. No. 2015/385366/07

These companies are collectively referred to as “Laudian”.

SCOPE

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

The policy addresses the protection of electronic records, especially those of a confidential or private nature.

The Information Officer will be responsible for ensuring the implementation of the procedures described in this policy.

This policy should be read together with Laudian’s Privacy Policy, Record Retention Policy and the information technology disaster recovery section of the Business Continuity Policy.

PURPOSE

The purpose of this policy is to provide guidelines for the protection of data security and our technology infrastructure, outline protocols that govern cyber security measures and define the rules for company and personal use.

POLICY

Laudian takes data security seriously and we are committed to implementing cyber security measures aimed at ensuring the confidentiality, integrity, and availability of data.

STAFF RESPONSIBILITIES

Staff are responsible for complying with this policy document and all other ICT (Information and Communication Technologies) policies and procedures of Laudian. Staff are also responsible for protecting the ICT systems and resources of Laudian from unauthorized access, disclosure, modification, loss, or damage.

Staff are expected to:

- Read, comply with, and understand this policy document and all other ICT policies and procedures of Laudian.
- Complete any ICT training or awareness programs that are provided by Laudian.
- Not compromise Laudian systems or data by providing access or knowledge of the Laudian network systems or cyber security measures to third parties known or unknown without authorisation from department managers and informing the ICT manager of access.
- Make use of pre-approved or provided communications platforms (such as Teams, Outlook etc.) to conduct primary work communications, ensuring communications security and lowering the likelihood of interception.
- Report any ICT issues, incidents, breaches, or violations to the ICT manager as soon as possible; and
- Cooperate with any ICT investigations, audits or reviews that are conducted by Laudian.

Staff who fail to comply with this policy document or any other ICT policies and procedures of Laudian may face disciplinary action up to and including termination of employment. Staff may also be held liable for any damages or losses that result from their non-compliance.

The following principles underpin this policy:

- ICT resources are provided by Laudian for business purposes and should be used primarily for such purposes.
- ICT users are responsible for the security and appropriate use of the ICT resources they use and the data they access or create.
- ICT users must comply with all applicable laws, regulations, policies, and standards relating to ICT use and data protection.
- ICT users must respect the rights, privacy and dignity of others when using ICT resources and data.
- ICT users must protect the confidentiality, integrity and availability of data and ICT resources from unauthorized access, disclosure, modification, or destruction.
- ICT users must report any actual or suspected breaches of this policy or any incidents affecting the security or performance of ICT resources or data.
- ICT users must comply with the Disaster Recovery Plan when implemented.

PROCEDURES

Use of Company Devices

Company devices refer to the devices such as laptops, tablets, smartphones, or wearable devices that are owned and provided by Laudian for staff to use for work purposes. Company devices are intended to facilitate the work performance and communication of staff and are subject to the ICT policies and procedures of Laudian.

Staff are expected to use company devices in a responsible, ethical, and professional manner. This includes but is not limited to:

- Using company devices only for work-related purposes and not for personal or unauthorized purposes such as gaming, gambling, streaming, downloading, or accessing inappropriate or illegal content.
- Protecting company devices from loss, theft, damage, or misuse by keeping them in a secure location when not in use, locking them when unattended, using protective cases or covers etc.
- Maintaining the security and functionality of company devices by following the instructions and guidelines of the ICT department such as updating software, installing patches, scanning for viruses etc.
- Not modifying, altering, tampering with, or repairing company devices without the authorization of the ICT department.
- Not inserting unknown or insecure storage devices (such as USB drives) into company devices at any time.
- Never leave devices exposed or unattended.
- Not sharing company devices with other staff or third parties without the approval of the ICT manager; and
- Returning company devices to the ICT department when they are no longer needed or when leaving Laudian.

Laudian owns and controls all company devices and the information or data stored on them. Laudian has the right to monitor, audit, access, wipe or disable any company device at any time without prior notice.

BYOD (Bring Your Own Device)

Using personal digital devices to access company emails or accounts introduces a data security risk. This includes computing devices as well as mobile handheld devices, amongst others.

The following is required:

- Keep all devices password-protected.
- Use and regularly update comprehensive antivirus software.
- Never leave devices exposed or unattended nor lend your own devices to others
- Install security updates of browsers and systems monthly or as soon as updates are available.
- Abiding by the ICT policy and procedures of Laudian when using a personal device for work purposes.

- Keeping personal and work data separate on the personal device by using different accounts or partitions.
- Not storing sensitive or confidential information or data on the personal device unless necessary and authorized by the ICT manager.
- Deleting any work-related information or data from the personal device when it is no longer needed or when leaving Laudian.
- Reporting any loss, theft, damage, or compromise of the personal device to the ICT manager or supervisor as soon as possible.
- Login to company accounts and systems through secure and private networks only; and
- users must avoid accessing internal systems and accounts from other people's devices or lending their own devices to others.

Keep emails safe

Emails often host scams and malicious software. To avoid virus infection or data theft, you must:

- If an email requests your username and password to access a document, it has an extremely high chance of being a phishing scam. Do not supply your Laudian.co.za username or password to any external websites.
- Be aware of imitation phishing emails appearing to be from Exco or senior management as this is an oft-used spear-phishing method deployed against Laudian.
- 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 addresses and names of people messages are received from to ensure they are legitimate; and
- Look for inconsistencies or giveaways (e.g., grammar mistakes, capital letters, an excessive number of exclamation marks.)

If you are not sure that an email received is safe, report it to the ICT department.

Manage passwords properly

Employees at Laudian are required to manage and maintain their own primary passwords ensuring accountability, privacy, and security.

Password leaks are dangerous since they can compromise our entire infrastructure. Not only should passwords be secure so they will not be easily hacked, but they should also remain secret. For this reason, we advise you to:

- 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.).
- Remember passwords instead of recording them. If you need to write down/save a password, keep the paper or digital document confidential and destroy it when it is not required anymore.
- Exchange credentials only when absolutely necessary. When exchanging them in person is not possible, use the phone instead of email, and only if you recognize the person you are talking to.

Transfer data securely

Transferring data introduces a security risk. We will:

- Avoid transferring sensitive data (e.g., customer information, employee records) to other devices or accounts unless absolutely necessary.
- Ensure approved and provided methods for transfer of digital files are used.
- Ensure work data or files are not transferred to or via personal accounts or avenues.
- Share confidential data over the company network / system and not over public Wi-Fi or private connection; and
- Ensure that the recipients of the data are properly authorized people or organizations that have adequate security policies.

Additional measures

To reduce the likelihood of security breaches, we also instruct you to:

- Lock your devices when leaving your desk.
- Report stolen or damaged equipment as soon as possible to either HR or ICT.
- Change all account passwords at once when a device is stolen.
- Report a perceived threat or possible security weakness in company systems.
- Refrain from downloading suspicious, unauthorized, or illegal software on company equipment; and
- Avoid accessing suspicious websites.

Our ICT Team should:

- Install firewalls, anti-malware software and access authentication systems.
- Inform employees regularly about new scam emails or viruses and ways to combat them.
- Investigate security breaches thoroughly; and
- Follow this policy's provisions as other employees do.
- Ensure physical access to any servers is restricted.

Remote employees

Remote employees accessing our company's accounts and systems are obliged to follow all data encryption, protection standards and settings, and ensure their private network is secure.

Termination of employment

The employee / contractor's supervisor must confirm to the Information Officer that the employee / contractor's access to any electronic records of Laudian has been terminated (this includes, without limitation, access to Laudian's computer systems, emails, and third-party provider login details).

After returning electronic records to Laudian, the employee / contractor is obliged to delete all FSP Name's electronic records kept on personal devices.

Back-ups of electronic records

Data kept on internal systems stored on local and international servers are backed up continuously and automatically and to a cloud server.

It is the employee's responsibility to ensure the backup tool (OneDrive) remains functional and to report any disruption / sync issues to the ICT department as soon as it is noticed.

External service providers

We have performed a reference check / due diligence on external providers and specifically information technology providers who have access to the confidential and Personal Information that we keep and have concluded formal agreements with such providers to govern information security-related responsibilities.

Consequences of Non-Adherence

Action that leads or may lead to a security breach will be viewed in a serious light and Laudian will take disciplinary action or consider terminating agreements with the relevant contractor, employee, or provider.

Training and Awareness

All staff will receive a copy of this policy.

All cyber security training is mandatory and will negatively impact performance reviews if the training is not attended.

Review

This document will be reviewed at least annually to ensure it remains relevant, but also as and when required when for example new regulations are published.