Nature Society Singapore

DOCUMENT:	**IT SECURITY POLICY**
DOCUMENT NO:	**DPMP-02**
EFFECTIVE DATE:	**14/05/2025 13:48:28**
REVISION:	**0**

DATE	REVISION	DESCRIPTION OF CHANGES
14/05/2025 13:48:28	0	Initial release

PREPARED BY:

NAME/DESIGNATION	SIGNATURE	DATE
ANDY PRAKASH (DATA PROTECTION OFFICER)	Andy Prakash	**14/05/2025 13:48:28**

APPROVED BY:

NAME/DESIGNATION	SIGNATURE	DATE
HUANG NINGXIN EXECUTIVE DIRECTOR		**20/05/2025**

Contents

1. PURPOSE

Nature Society Singapore ("Company") IT Security Policy ("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 security breaches. Human errors, hacker attacks and system malfunctions could cause great financial damage and may jeopardize our Company's reputation.

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 information, systems and databases. For this reason, we have implemented a number of security measures. We have also prepared a guideline that may help mitigate security risks.

2. SCOPE

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

3. EMPLOYEE

It is the responsibility of the employee to ensure security and protection, and take reasonable care of any Company asset (e.g., tablet, laptop, desktop, software, email account, etc.) and Company information (e.g., data, report, etc.) which may come to them in any format and therefore employees will need to ensure the below requirements:

3.1 Approach Unauthorised Personnel

If you see an unauthorised or unrecognized person in a restricted area of the work premises or physically attempting to access work systems and devices wherever you might be, you should approach them as to their right to be there. Any approached person who does not respond appropriately should be immediately reported to the management and escorted. This applies to any co-working or hotdesking space, serviced office or physical office.

3.2 Company Asset

3.2.1 Used Within Company

Unattended Company devices/equipment should be password locked by the user when leaving the work station. The automatic screen lock function is set to automatically activate upon inactivity and employees are not allowed to make any settings which would override this security function.

3.2.2 Used Outside Company

Company devices/equipment (e.g., laptop, tablet, mobile, etc.) and especially devices/equipment which are portable are unfortunately easy to steal during travelling or outside the company for business activities. Company device/equipment might contain sensitive data either of a business confidential or personal and the utmost care should be taken to ensure that this data is not compromised. Therefore, such device/equipment should never be left unattended, always bring along the device/equipment with you and check before you leave any location.

3.2.3 Home Use

Personal computers supplied by the Company are to be used solely for the Company's business purposes.

3.3 Document

Employees are not encouraged to bring the Company's documents (containing sensitive or confidential information) out of the Company's premises (where applicable). However, if it is necessary to do so, employees should always secure such documents and never leave the documents unattended.

Whereas in the Company's premises, documents (containing sensitive or confidential information) should also not be left unattended and must be secured (e.g., lock in cabinet, etc.) at all times. Such documents should never be made accessible to unauthorised personnel.

3.4 Confidentiality

Employees who handle sensitive, confidential or personal data information belonging to the Company shall use best endeavours to protect it, to keep the data safe, and to use it only for valid business purposes. Employees shall not disclose such information to unauthorised personnel even after the employment relationship has been terminated or completed.

3.5 Reporting

Report promptly to management for:

- misconduct or ill intent relating to company assets and information (e.g., hacking into a system, scam, etc.);
- theft or loss of the Company asset or information;
- unauthorised disclosure of the Company information;
- damage or faulty Company asset (e.g., laptop, desktop, etc.); and/or
- any violation of this policy.

3.6 Retention of Ownership

Asset, resources, and information that are provided by employees, consultants, or contractors for the benefit of the Company are the property of the Company unless covered by a contractual agreement.

4. PROHIBITED ACTIVITIES

Personnel (e.g., employee, visitor, vendor, etc.) are prohibited from the following activities:

- accessing protected system/network without authorisation, hacking Company system/network, crashing an information system;
- attempting to break into an information resource or to bypass a security feature;
- introducing, or attempting to introduce, computer viruses, Trojan horses or other malicious code into an information system (Exception: when conducting Company approved security tests);
- unauthorised accessing or viewing of confidential or sensitive information to which employees have not been authorised;
- all software installation for personal usage; all software installed on computers or systems must be approved by the CEO (Chief Executive Officer) or relevant authority;

- violating or attempting to violate the terms of use or license agreement of any software product used by the Company;
- engaging in any activity for any purpose that is illegal or contrary to the policies, procedures, or business interests of the Company;
- transferring the Company's information to any personal device/equipment (e.g., flash drive, laptop, hard disk, etc.) or any personal platform, application, software, etc.; and
- use of the Company's assets and information for personal purposes;
- use of unauthorized personal devices/equipment (e.g., tablet, laptop, etc) to access Company information systems.

5. SOFTWARE

Only software that is reviewed, approved, and installed by the CEO (Chief Executive Officer) can be used on the Company's equipment, devices, or system. No one is allowed to install any software in the Company's equipment, device, or system without approval from the CEO (Chief Executive Officer). The CEO (Chief Executive Officer) will review (e.g., security, compatibility, etc.) any new software before providing approval to install it on the Company's equipment, devices, or system.

6. AWARENESS AND TRAINING

As technology advances, security risk and threats to IT systems also increase, therefore it is important to keep our employees aware of the relevant and updated threats vectors and ensure they are competent as a user of the Company computer or system.

New employees need to read and understand the IT Security Policy during the orientation period or as part of the employee onboarding process before official work commences. This IT Security Policy will be provided to new employees by the CEO (Chief Executive Officer) / Human Resources (HR) during the orientation period, and if there are any clarifications required, they may approach their direct Supervisor, CEO (Chief Executive Officer) or Data Protection Officer.

When there is a need/requirement, the Company shall send employees for internal or external training in order to ensure the competency of the employee. Current training(s) include PDPA awareness e-learning training offered by Privacy Ninja.

Should there be any relevant information (e.g., system upgrade, threat, etc.) from third parties (e.g., authorities, PDPC, service provider, vendor, industries, etc.) the CEO (Chief Executive Officer) will verify the information and disseminate such information to all employees**.**

7. ACCESS CONTROL

Company information resources are protected by both internal security measures (i.e., passwords, two-factor authentication (2FA), account privileges, etc.) and external security arrangements (i.e., network security - *refer to Section 11*) whereby data from outside the organisation will be scanned before entering into the organisation.

Any physical medium (i.e., hardcopy documents) containing sensitive/confidential company information will be secured in locked cabinets with keys managed by authorised personnel.

Any system (e.g., server, network-attached storage (NAS), records, etc.) will also be secured and locked to prevent unauthorised access.

Dedicated office access is secured with a physical locked door at the entrance and a security video camera to prevent unauthorised entry.

The organization is not situated in a commercial office building.

User Access Management Policy

The Company stores files and information on Cloud-based solutions.

All internal systems are to comply with the following.

- Procedures for approving, granting, and managing user access including user registration/de-registration, password delivery and password reset shall be documented.
- Data access rights shall be granted to users based on a need-to-know basis.
- The granting of special privileges like admin user who has access to all/higher level functions shall be restricted and controlled.
- User privileges and data access rights shall be clearly defined and reviewed annually by the CEO (Chief Executive Officer).
- Records for access rights approval and review shall be maintained.
- All user privileges and data access rights shall be revoked as soon as practicable when no longer required.
- Usage of Google Drive:
- Employees should not use the Google Drive link sharing feature for sharing any files or folder access even with expiry access with co-workers or external vendors, unless explicitly approved by management and documented.
- Folder owners maintain password listing for all files with passwords. All Google Drive admin roles should be the CEO (Chief Executive Officer).

8. LOGIN ACCOUNT

8.1 Only the CEO (Chief Executive Officer) has the right to create a new account or delete inactive accounts. Individual users shall have unique login IDs and passwords. An access control system shall identify each user and prevent unauthorised users from entering or using information resources (e.g., server access, email access, etc.). Security requirements for user identification include:

- Each user shall be assigned a unique identifier (i.e., email address or username etc.).
- Users shall be responsible for the use of their individual login ID.

If a user's work scope changes, their account access rights and/or user privileges, will also be reviewed and approved by the CEO (Chief Executive Officer) and management, to meet the new work scope requirements by the Company.

8.2 Business account for applications/platforms

- Employees should never use personal email accounts e.g., @hotmail or @gmail domain accounts to subscribe accounts for business/company use
- If a Google account is required for any subscription, employees are to inform the CEO (Chief Executive Officer) and seek approval from the management.

9. PASSWORDS

User IDs and passwords are required in order to gain access to all Company networks or work accounts. All passwords are unique to each account user. Users are required to set a unique ID or username for their login accounts and never share passwords or record passwords on paper.

9.1 Password Length
Passwords are required to be a minimum of 12 characters whenever possible.

9.2 Content Requirements
Passwords should be a combination of uppercase letters, lowercase letters, numbers (0-9) and special characters/symbols whenever possible.

9.3 Sharing Password
Writing on paper and sharing passwords is disallowed. Passwords must be kept confidential and the responsibility for the safekeeping and knowledge of passwords shall fall onto the account owner.

9.4 Password Display
Passwords should be masked and not appear as clear text when inputted on screen to protect the password from being viewed by unauthorised personnel.

10. ANTIVIRUS PROTECTION

Company devices/equipment (e.g., laptop, desktop, server, etc.) will be installed with antivirus software to protect company information. Antivirus software should be configured to automatically update its virus definitions to continuously detect any latest virus signature.

All employees are to enable real-time protection functionality and perform automated (if possible) regular (weekly) scheduled full system scans because these features will identify, stop, and quarantine a virus as it attempts to execute.

All employees are to keep laptop Antivirus software connected at ALL time and ensure that virus protection and other security patches are updated to the latest available versions. Our antivirus software brand is Windows Defender (pre-installed with Windows Operating System), XProtect (MacOS built-in antivirus).

The CEO (Chief Executive Officer) will conduct random checks for compliance and keep recorded documentation of such checks.

11. NETWORK

Company / Home Wi-Fi internet network is password protected as additional layers of protection to Company information when it is being transmitted over the Internet, using the latest Wi-Fi security protocols. Such passwords should not be revealed to unauthorised personnel. Should there be any suspected password breach or unauthorised network access, the password must be changed immediately.

Non-Company networks might not be secured and therefore employees must practice extreme caution when accessing such networks especially when sending sensitive / confidential data over

non-company networks. By default, employees are disallowed from transmitting sensitive / confidential data over non-company networks unless the matter is urgent and necessary, or there are no alternatives available.

The company does not issue nor require secured VPN connections when employees are working remotely or from home.

Use of only Secured Wireless Network Policy

- Employees use only secured networks for any connection using company laptops.
  - ✓ company office wireless network is considered secured.
  - ✓ Any outside network needs to be password secured and employees must know the Service Set Identifier (SSID) provider (e.g., at customer site if it is a trusted source).
- If employees need to use their own Internet Service Provider accounts when they connect to the Internet from home, they need to ensure the network used is secured with a password, using the latest Wi-Fi security protocols.
- Do NOT use unsecured connections that are usually offered free in public spaces.
- Limit use of Bluetooth technology
  - ✓ Switch off Bluetooth mode whenever not in use.
  - ✓ Confidential or Sensitive data must not be transmitted or stored on Bluetooth enabled devices.
  - ✓ Do not activate Bluetooth when connected to an unsecured network. This is to avoid Bluesnarfing, the act of stealing information from Bluetooth enabled devices, which may include sensitive information and personal data.

Network Firewall

The organization does not utilize a network firewall in the dedicated office network.

12. CLEAN DESK POLICY

- The purpose for this policy is to establish the minimum requirements for maintaining a “clean desk” where sensitive/critical information about our employees, our intellectual property, our customers and our vendors is secured in locked areas and out of sight. This is necessary to reduce the risk of security breaches in the workplace or where physical documents or electronic media are stored, even for Work From Home arrangements.
  - ✓ Any Sensitive or Confidential information must be removed from the desk and locked in a drawer when the desk is unoccupied at the end of the work day.
  - ✓ Definition of Sensitive or Confidential: E.g., Employee personal data or any personal data in general.
  - ✓ Definition of Sensitive information: E.g., Company quotation and pricing information
  - ✓ File cabinets containing Sensitive or Confidential information must be kept closed and locked when not in use or when not attended to.
  - ✓ Keys used for access to Sensitive or Confidential information must not be left at an unattended desk or left hanging in the lock.

13. COMMUNICATION

Company encourages employees to use only Company issued devices/equipment for business- and work-related communication (e.g., email, any communication software/platform, etc.). All electronic communication systems and all messages or information generated on Company assets are considered the property of the Company.

Employees are not allowed to use company assets for the following:

- personal commercial activities (e.g., promoting a personal online business, etc.);
- political activities (e.g., communicating election information of personal interest, etc.);
- harassment (e.g., offensive message, racial comments, ethnic slurs, discriminatory, threatening etc.); and/or
- junk e-mail (e.g., chain mail etc.).

14. EMAIL

Emails often host phishing scams and malicious software (e.g., worms.) To avoid virus infection or data theft, employees need 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, etc.); and
- check email and names of senders they received messages from to ensure they are legitimate. If suspicious, give a call or find alternate means to verify the message authenticity with the sender.

If an employee isn’t sure that an email they received is safe, they can refer the case to the CEO (Chief Executive Officer).

Email Account Installation Policy on Mobile Device

- Ensure the mobile device is password and biometrics security feature enabled before installation of the Company email account.
- All emails must be sent/received through secure connections (e.g., for Internet Message Access Protocol (IMAP), Simple Mail Transfer Protocol (SMTP) or Post Office Protocol (POP) protocols must be over secure sockets layer and transport layer security (SSL/TLS)).

15. SENDING/TRANSFER OF SENSITIVE/CONFIDENTIAL INFORMATION

Whenever sending or transferring sensitive or confidential information, such information must be password protected and only disclose the password to authorised recipients via a separate medium (e.g., WhatsApp, phone message, etc.). The sender should double-check the correct recipient email address before sending or transferring.

Whenever delivering any sensitive or confidential information via snail mail, ensure that the envelope is sealed and secured. Additionally, the sender should double-check the mailing address before sending it out.

When mass transfer of such data (e.g., more than 500 individual recipients are involved) is needed, employees shall approach the CEO (Chief Executive Officer)/DPO for advice.

16. LAPTOP SECURITY

Guidelines and best practices for ensuring physical security for laptop:

- When leaving your work device/equipment at your workspace at the end of the day, store your laptop in a locked office drawer or cabinet. Keys should be kept securely separately.
- Password protected screensaver timeout to be set with a duration of 15 minutes inactivity.
- Activate the lock screen when you need to be away from your laptop (e.g., washroom, lunch break etc.), for Windows Operating System PC/laptop, this can be achieved by pressing the "Windows Key" + "L".
- Keep food and drinks away from the computer.
- Do not leave your laptop plugged into the docking station or power adapter after it is fully charged. This shortens the ability of the battery to maintain a charge.
- Ensuring laptops are transported and stored in a padded, protective case or bag.
- All working files should only be saved in the company shared file drive folders. This is to avoid any loss of data from being stored in the hard disk storage in the event of loss of laptop.
- Company does not require nor implement data encryption for data at rest.
- Password complexity requirements, should include best practices such as validity expiry (where applicable softwares support this feature) or manually enforced change every 90 to 120 days, and no reuse of previous passwords across all work related accounts.

17. PORTABLE STORAGE DEVICES

Portable storage devices are devices which have the capability to store electronic data, which include but are not limited to SD cards, DVDs, CD-ROMs, Thumb drive, Portable hard disk etc.

Below shall be observed and practiced when using portable devices:

- Employees are NOT allowed to transfer any sensitive or confidential data to any portable storage device unless there is explicit authorisation by management.
- In the event of such authorisation, employees are to use only Company issued portable storage devices provided by the CEO (Chief Executive Officer).
- Do not transfer any sensitive or confidential data to any non-Company portable storage device.
- No sensitive or confidential data should ever be stored on any portable storage device unless the data is secured in a password protected format or the portable device is encrypted.
- Users must never connect their company portable storage device to a computer or system that is not issued by the Company unless authorisation is provided.
- Non-Company's computers or systems may not have the same security protection standards required by the Company therefore users are not allowed to connect their company portable storage device to a computer or system that is not issued by the Company unless authorisation is provided.
- If the Company's portable storage device is used to connect to a non-Company computer or system, the user must conduct an antivirus scan on the non-company computer or system before transferring or using the data inside the portable storage device.
- Company's computers or systems are NOT allowed to connect to a non-Company portable storage device unless the other company or individuals are authorised.
- Report all loss of company portable storage device to management immediately.

All company portable storage devices and its contents remain as company assets and upon completion of use (e.g., completion/termination of employment, after device loan period, etc.) must be returned back to the company's possession.

18. DISPOSAL

18.1 Physical Data

Document (e.g., paper, folders etc.) which contains sensitive information must be checked by the data owner and ensure that such data is no longer needed for business reasons before shredding. Do not dispose of any document directly into the waste bin.

The Company may at times also engage competent third-party service providers for secured document disposal services, and evidence of any document destruction will be obtained from such third service providers.

The Company will perform its due diligence on such service providers before any prior engagement. At this point in time there is not yet any use for engaging any document disposal/destruction service provider.

18.2 Electronic Data

Electronic data are data that can be stored in electronic storage devices or equipment (e.g., flash drive, computer or NAS etc.).
The CEO (Chief Executive Officer) will act as a secondary layer of control to verify that the data owner has deleted data inside storage devices or equipment securely before passing on such equipment for further disposal or usage by other employees, whichever is applicable.

18.3 Equipment / Devices

Device / equipment (e.g., hard disk, flash disk, laptop, desktop, tablet, etc.) may be "phased off" as and when the CEO (Chief Executive Officer) deems that the respective device/equipment's technological capability is causing productivity constraints or may constitute a vulnerability state due to outdated software configuration or end-of-life operating system support.

- Verified by the CEO (Chief Executive Officer) that device / equipment is empty
- Do not throw any device / equipment into the waste bin directly.
- Return all device / equipment to the CEO (Chief Executive Officer)
- The CEO (Chief Executive Officer) will perform full formatting or use specialised software to ensure data are securely deleted and non-recoverable and store such devices/equipment in a locked cabinet.
- Approved third-party IT equipment disposal service providers will be engaged by the CEO (Chief Executive Officer) to destroy the device / equipment.
- The Company will perform its due diligence on such service providers before any prior engagement. At this point in time there is not yet any use for engaging any document disposal/destruction service provider.
- Upon collection, receipt of the explicit device/equipment will be issued by the service provider and upon destruction, a destruction certificate. The CEO (Chief Executive Officer) is to maintain the destruction certificates for as long as the company is in operation.

19. REVIEW

The CEO (Chief Executive Officer) shall be responsible for conducting a regular review (at least once a year) on the effectiveness of security measures in the Security Policy to keep up to date with emerging security threats by considering the current IT infrastructure, relevant IT information relating to IT security and updates received from third parties (e.g., authorities, PDPC, service provider, vendor, industry regulator, etc.) and implement necessary implementation to protect company information.

Other than the above periodic review, below are also situations which will trigger an immediate review of the effectiveness of the current security measures in the Security Policy:

- Data breach incident
- Critical IT threat
- Major upgrading or new implementation of IT system (e.g., new server, etc.) or protection system (e.g., new CCTV system, etc.)
- Relevant regulatory update pertaining to IT security

Any revision of the security measures in the Security Policy will require a review by the Data Protection Officer and final approval from the management.

The CEO (Chief Executive Officer) or their designees shall review the active user accounts for both network and application access annually to ensure that any inactive account removal lapses are identified and such accounts are removed from the system. IT will document and inform the accounts identified and made inactive to the management.

Where applicable, the CEO (Chief Executive Officer) shall engage IT/application developers to assess the IT security risk prior to any commencement of IT development works. Otherwise by default, the CEO (Chief Executive Officer) shall engage an external service provider to conduct a greybox vulnerability assessment and penetration to ensure company systems, inclusive but not limited to the hardware (e.g., firewall, security devices, computer endpoints, etc.), software (e.g., company owned web application and mobile applications), and network have sufficient protection measures and security in place.

Any vulnerabilities discovered during the Vulnerability Assessment and Penetration Testing (VAPT) exercise will be remediated as soon as practicable, in a priority order starting with the highest vulnerability risk rating based on the VAPT report. The CEO (Chief Executive Officer) will work with the respective involved parties to close the identified gaps accordingly and third parties (e.g., application developer, IT specialists/consultants, etc.) might be engaged for assistance.

The outcome of the VAPT testing, any critical threats, the need to upgrade the system or recommendations must be reported to the management. An action plan by the CEO (Chief Executive Officer) for upgrading the systems or implementing fixes will be established and can only be implemented upon **management approval.**

A revalidation VAPT will be conducted to ensure that the identified gaps have been resolved and no longer exist.

20. VISITOR HOSTING POLICY

As part of the physical security measures to prevent security or data breaches, all visitors to any permanent or temporary office space (e.g., dedicated office, co-working space, etc) that employees may be working from or located in, will need to be hosted/escorted. The objective is to ensure we do not leave our visitors unattended and inadvertently allow any possible unauthorised access to sensitive/confidential data.

Below are guidelines for visitor hosting:

- Before visitor arrival, ensure the meeting room is cleared, ensure that any documents containing company confidential information or Personal Data are securely kept and stored away from view.
- If sharing of Confidential data is required in the meeting, ensure that this vendor or third-party has already signed the necessary confidentiality agreement and Data Protection Notice for the third-party vendor with the company.
- If the laptop is needed as part of the meeting, ensure it is compliant to the laptop security guidelines.
- Upon the arrival of a visitor, employees are to receive the visitor at the entrance and escort the visitor directly into the meeting room.
- During meetings or events, the host is to escort the visitor if he/she needs to navigate around the office. If employees need to leave the meeting room halfway, they will lock their laptop (if present) and bring along with them any printed confidential/sensitive documents out of the room.
- At the end of the meeting or event, the host is to escort the visitor to the exit.
- If any employees happen to see any unescorted visitor, they are to identify and verify the purpose of the visit and host them till the relevant employee is here to take over.
- If employees are late for a meeting with any visitor, they are to contact a colleague as a temporary replacement as host.

21. PRINTER PASSWORD REQUIREMENT

Secured printing is recommended as part of our secured business processes. All employees are to update their respective office / home printer settings in their desktop / laptop so that it will operate on secured printing mode, which prevents any printing task from executing until a passcode is keyed into the printer directly.

Below is a list of the step by step instructions for setting up secure printing and employees are to set this function as the print default configuration.

1. click on Search icon beside the Windows Start button;
2. Enter Control Panel;
3. Select View Devices and Printers
4. Right click the Printer Driver, select Printer Properties;
5. Select Advance Tab;
6. Click on Printing Defaults
7. Change the Job Type from Normal Print to Secure Print;
8. Click on Setup and Enter the User ID and Password accordingly
9. Select OK, Apply and OK

Note that the above steps to configure secure printing may differ slightly across different Windows Operating System versions.

22. COMPLETION / TERMINATION OF EMPLOYMENT

Upon termination or completion of employment, HR will inform the CEO (Chief Executive Officer) through email providing the employee's name, email and date of termination or completion of employment.

- The CEO (Chief Executive Officer) shall promptly remove, suspend or revoke the access right to work related online accounts (e.g., work email and company shared file storage drive access) or configure the account to expire for the employee on the last day of employment.
- The employee's manager shall ensure all access (e.g., keys to cabinets, access card, badge, etc.) and Company's devices/equipment and assets, where applicable, are returned to the Company by the last day of employment and utilize the employee offboarding checklist for efficient governance.

23. COMPANY RIGHT

The Company reserves the right, at its discretion, to review any employee's files or electronic communications to the extent necessary to ensure all electronic media and services are used in compliance with all applicable laws and regulations as well as Company policies.

24. REPORTING

Any personnel member (e.g., employee, visitor, vendor, etc.) who suspects a company device/equipment (ex. desktop, laptop, mobile, etc.) has been infected with virus or malware, or compromised to any extent should take the following steps immediately:

- Stop using the computer;
- disconnect device from the network/internet.
- note down the issue and if possible take screenshots or picture
- Inform the direct supervisor or CEO (Chief Executive Officer)

It is the responsibility of each personnel to report any security incidents or violations of the security policy immediately to the direct supervisor and CEO (Chief Executive Officer)/DPO.

25. DISCIPLINARY ACTION

Employees are expected to follow this policy strictly and those who are found in violation due to negligence, regardless of any security breach as an outcome, will face disciplinary action:

First-time, unintentional
Issue a verbal warning and provide further training to the employee on security.

Intentional, repeated or large-scale breaches (as determined by the Company at the point of such incident at the Company's sole discretion)
Invoke more severe disciplinary consequences which may include termination and filing of a report with the relevant law authorities or regulators. We will investigate each incident on a case-by-case basis.

Additionally, employees who are observed to disregard this IT Security Policy will face progressive disciplinary consequences, even if their behaviour had not resulted in a security breach.