IT Security Policy

Introduction

Information Technology (IT) is an integral and critical component of The Simple Pharma Company's ("SP") daily business. This policy seeks to ensure that the IT infrastructure efficiently serves the primary business functions of SP, provides security for the organisation and members' electronic data, and complies with National Cyber Security Centre (NCSC) and other relevant regulations. IT resources include hardware (computers, servers, peripherals), software (licensed applications, operating systems), network equipment (routers, firewalls, wiring), and IT personnel. The integrity of all IT resources is critical to the successful operation of SP's business. All computer equipment, peripherals, and software are Simple Pharma's property and are provided for business purposes. Proper use and control of computer resources is the responsibility of all employees. Intentional or reckless violation of established policies or improper use of Simple Pharma's computers will result in corrective action up to and including termination.

Aim

This policy helps us:

1. Reduce the risk of IT problems
2. Plan for problems and deal with them when they happen
3. Keep working if something does go wrong
4. Protect company, client and employee data
5. Keep valuable company information, such as plans and product designs, secret
6. Meet our legal obligations under the General Data Protection Regulation (GDPR) and other laws
7. Meet our professional commitments towards our clients and customers

Responsibilities

- Head of IT – is responsible for the overall IT security strategy and will also act as the data protection officer.
- IT Consultants – help plan and deliver SP's IT infrastructure.

Information Classification

We will only classify information which is necessary for the completion of our duties. We will also limit access to personal data to only those that need it for processing. We classify information into different categories so that we can ensure that it is adequately protected and that we allocate security resources appropriately:

- **Unclassified**: This type of data is freely accessible to the public (i.e. all employees/company personnel). It can be freely used, reused, and redistributed without repercussions. Examples might be first and last names, job descriptions, or press releases.
- **Internal-only**: This type of data is strictly accessible to internal company personnel or employees who are granted access. This might include internal-only memos or other communications, business plans, etc.
- **Confidential Information**: Access to confidential data requires specific authorisation and/or clearance. There are three main types:
    - **Employee confidential**: includes information such as medical records, compensation, etc.
    - **Company Confidential**: includes information such as contracts, business plans, passwords for critical IT systems, client contact records, accounts etc.
    - **Client confidential**: This includes personally identifiable information such as name or address, passwords to client systems, client business plans, new product information, market-sensitive information etc.
- **Restricted data**: Restricted data includes data that, if compromised or accessed without authorisation, could lead to criminal charges and massive legal fines or cause irreparable damage to the company. Restricted data might include proprietary information or research and data protected by state and federal regulations.

Access Controls

SP operates a transparent culture where reasonably possible. A 'need to share' rather than a 'need to know' basis with respect to company confidential information. This means our bias and intention is to share information to help people do their jobs rather than raise barriers to access needlessly.

As for client information, we comply with the GDPR' Right to Access'. This is the right of data subjects to confirm whether we are processing their data, where we are processing it and for what purpose. However, in general, to protect confidential information, we implement the following access controls:

- To access confidential information, all employees must go through the multi-factor authenticator process (more info below in the password management guidelines section).
- If the information is strictly confidential, it will be stored in an area with limited access.

Security Software

To protect our data, systems, users, and customers, we use the following systems:

Firewalls

Firewalls are in place between the office network and the internet. All devices that access company information have firewalls enabled using the default settings. 1Password's random password generator and the secure vault are also used to ensure that the firewall password is safe from brute-force password guessing.

Malware

Windows Defender is used to ensure sufficient malware protection is provided.

Employees Joining and Leaving

Joining

When a new employee joins the company, we will add them to the following systems:

- Microsoft 365 (Office, Emails, Teams, Teams telephony, Sharepoint)
- GitHub
- HubSpot
- BackHub (GitHub backup solution)
- Freshdesk
- 1password

Access levels will be varied by Job role. New joiners will also be required to attend mandatory IT security training.

Leaving

Under SP's offboarding process, employees leaving will have their access privileges to the computer system revoked promptly.

Password Management Guidelines

At SP, we use 1Password to store and create strong passwords securely. Even though 1Password provides the user with the tool to manage passwords, the following guidelines should be followed to ensure good housekeeping of passwords.

- Change default passwords and PINs on computers, phones and all network devices
- Don't share your password with other people or disclose it to anyone else
- Don't write down PINs and passwords next to computers and phones
- Use 1Password's random password generator to ensure passwords are suitably strong
- Change them regularly
- Don't use the same password for multiple critical systems

Be alert to other security risks

While technology can prevent many security incidents, your actions and habits are also necessary.

The following things (among others) are, in general, prohibited on company systems and while carrying out your duties for the company and may result in disciplinary action:

- Anything that contradicts our equality and diversity policy, including harassment.
- Circumventing user authentication or security of any system, network or account.
- Downloading or installing pirated software.
- Disclosure of confidential information at any time.

Backup, disaster recovery and continuity

SP uses GitHub to store the majority of its business-critical information. SP use Backhub (authorised software by GitHub) to back up all data stored in GitHub every 24 hours. As an additional safety measure, we back up information stored in Backhub quarterly.

In the case of a disaster, business-critical information can be recovered and restored from either Backhub or SharePoint to ensure the business continues.