Hype Health Clubs Information Security Policy

Version: 0.1

Date: 03/01/2020

Table of Contents

1 Purpose

The purpose of this Policy is to safeguard information belonging to Hype Health Clubs and its stakeholder (third parties, clients or customers and the general public), within a secure environment.

This Policy informs Hype Health Clubs staff, members, and other individuals entitled to use Hype Health Clubs facilities, of the principles governing the holding, use and disposal of information.

1.1 Goals

It is the goal of Hype Health Clubs that:

- Information will be protected against unauthorised access or misuse.
- Confidentiality of information will be secured.
- Integrity of information will be maintained.
- Availability of information / information systems is maintained for service delivery.
- Business continuity planning processes will be maintained.
- Regulatory, contractual and legal requirements will be complied with.
- Physical, logical, environmental and communications security will be maintained.
- Infringement of this Policy may result in disciplinary action or criminal prosecution.
- When information is no longer of use, it is disposed of in a suitable manner.
- All information security incidents will be reported to the Hype Health Clubs management and investigated through the appropriate channels.

1.2 Definition of Information

Information relates to:

- Electronic information systems (software, computers, and peripherals) owned by Hype Health Clubs whether deployed or accessed on or off Hype Health Clubs sites.
- Hype Health Clubs computer network used either directly or indirectly.
- Hardware, software and data owned by Hype Health Clubs.
- Paper-based materials.
- Electronic recording devices (video, audio, CCTV systems).

2 The Policy

Hype Health Clubs requires all users to exercise a duty of care in relation to the operation and use of its information systems.

2.1 Authorised users of information systems

With the exception of information published for public consumption, all users of Hype Health Clubs information systems must be formally authorised by appointment as a member of staff, by enrolment as a gym member, or by other process specifically authorised by the Hype Health Clubs management. Authorised users will be in possession of a unique user identity. Any password associated with a user identity must not be disclosed to any other person. The *Network password policy* in *section 5.2* below describes these principles in greater detail.

Authorised users will pay due care and attention to protect Hype Health Clubs information in their personal possession. Confidential, personal or private information must not be copied or transported without consideration of:

- permission of the information owner
- the risks associated with loss or falling into the wrong hands
- how the information will be secured during transport and at its destination.

2.2 Acceptable use of information systems

Use of Hype Health Clubs information systems by authorised users will be lawful, honest and decent and shall have regard to the rights and sensitivities of other people. The detail of acceptable use in specific areas may be found in the list of *Subsidiary Policies* detailed in *section 5*.

2.3 Information System Owners

Hype Health Clubs management who are responsible for information systems are required to ensure that:

1. Systems are adequately protected from unauthorised access.
2. Systems are secured against theft and damage to a level that is cost-effective.
3. Adequate steps are taken to ensure the availability of the information system, commensurate with its importance (e.g. Business Continuity).
4. Electronic data can be recovered in the event of loss of the primary source, i.e. failure or loss of a computer system. It is incumbent on all system owners to backup data and to be able to restore data to a level commensurate with its importance (e.g. Disaster Recovery).
5. Data is maintained with a high degree of accuracy.
6. Systems are used for their intended purpose and that procedures are in place to rectify discovered or notified misuse.
7. Any electronic access logs are only retained for a justifiable period to ensure compliance with the data protection, investigatory powers and freedom of information acts.
8. Any third parties entrusted with Hype Health Clubs data understand their responsibilities with respect to maintaining its security.

2.4 Personal Information

Authorised users of information systems are not given rights of privacy in relation to their use of Hype Health Clubs information systems. Duly authorised staff of Hype Health Clubs may access or monitor personal data contained in any Hype Health Clubs information system (e.g. mailboxes, web access logs, file-store, etc.).

2.5 Breach of Policy

Individuals in breach of this policy are subject to disciplinary procedures (staff or member) at the instigation of Hype Health Clubs management with responsibility for the relevant information system, including referral to the Police where appropriate.

Hype Health Clubs will take legal action to ensure that its information systems are not used by unauthorised persons.

3 Physical Security

Hype Health Clubs will ensure that all paper-based information is protected as follows:

- Equipment and paper records are located in secure areas.
- Disposal policies and procedures are in place, e.g. shredding documents before disposing of them.
- Print rules and follow me printing restricts access to documents on MFPs.

4 Ownership

Hype Health Clubs management has direct responsibility for maintaining this policy and providing guidance and advice on its implementation.

Information system owners are responsible for the implementation of this Policy within their area, and to ensure adherence.

5 Subsidiary Policies

The detail of acceptable use in specific areas may be found in the following subsidiary polices.

5.1 ICT Acceptable use policy

- Users must use Hype Health Clubs ICT resources professionally and appropriately at all times.
- Users should remember that Hype Health Clubs ICT resources are provided to staff for business purposes and to enhance effectiveness and efficiency at work.
- Hype Health Clubs ICT resources must not be used for unlawful, offensive or otherwise improper activities. For example, they must not be used:
  - for material that is pornographic, hateful, racist, sexist, abusive, obscene, discriminatory, offensive or threatening
  - to stalk, bully, harass, defame or breach copyright.
- ICT resources can be used for personal use during breaks if it is not excessive and is within the acceptable use policy.

- An authorised person (e.g. a Hype Health Clubs gym manager) can monitor your use of the Hype Health Clubs ICT resources if they have a valid reason for doing so.
- If you discover inappropriate content on a Hype Health Clubs computer, you should report it to the Hype Health Clubs manager.
- A breach of the policy is regarded seriously. Depending on the seriousness of the breach, termination of employment is a possible outcome.

5.2 Network password policy

Hype Health Clubs password policies and best practices are detailed below.

5.2.1 Enforce Password History policy

The Enforce Password History policy **will set how often an old password can be reused**. It should be implemented with a minimum of 10 previous passwords remembered. This policy will discourage users from reusing a previous password, thus preventing them from alternating between several common passwords. Some tech-savvy users might try to work around the Enforce Password History policy, to prevent that from happening use the Minimum Password Age policy.

5.2.2 Minimum Password Age policy

This policy determines **how long users must keep a password before they can change it**. The Minimum Password Age will prevent a user from dodging the password system by using a new password and then changing it back to their old one. To prevent this, the specific minimum age should be set from three to seven days, making sure that users are less prone to switch back to an old password, but are still able to change it in a reasonable amount of time. As a system administrator you must keep in mind that **this policy could also prevent a user from immediately changing a compromised password**, so if the user can't change it, it will be up to you to make the change.

5.2.3 Maximum Password Age policy

The Maximum Password Age policy **determines how long users can keep a password before they are required to change it**. This policy forces the user to change their passwords regularly. To ensure a network's security you should set the value to 90 days for passwords and 180 days for passphrases.

5.2.4 Minimum Password Length policy

This policy determines the minimum number of characters needed to create a password. You would generally want to **set the Minimum Password Length to at least eight characters since long passwords are harder to crack than short ones**. For even greater security, you could set the minimum password length to 14 characters. A word of advice: if you haven't changed the default setting, you should change it immediately since sometimes the default is set to zero characters, meaning that it allows empty passwords.

5.2.5 Passwords Must Meet Complexity Requirements policy

By enabling the Passwords Must Meet Complexity Requirements policy, you'll go beyond the basic password and account policies and ensure that every password is secured following these guidelines:

- Passwords **can't contain the user name** or parts of the user's full name, such as their first name.

- Passwords must use **at least three of the four available character types**: lowercase letters, uppercase letters, numbers, and symbols.

5.2.6 Reset Password

The local **administrator password should be reset every 180 days for greater security** and the service account password should be reset at least once a year during maintenance time.

5.2.7 Use Strong Passphrases

Strong passphrases with a minimum of 15 characters should always be used to protect domain administrator accounts. While passwords and passphrases serve the same purpose, passwords are usually short, hard to remember and easy to crack, while passphrases are easier to remember and type but much harder to crack due to length.

5.2.8 Password Audit policy

Enabling the Password Audit policy **allows you to track all password changes**. By monitoring the modifications that are made it is easier to track potential security problems. This helps to ensure user accountability and provides evidence in the event of a security breach.

5.2.9 E-Mail Notifications

Create **e-mail notifications prior to password expiry to remind your users when it's time to change their passwords** before they actually expire.

5.2.10 Store Password Using Reversible Encryption for All Users policy

This policy should only be enabled on a per-user basis and then only to meet the user's actual needs. Passwords in the password database are all encrypted, and this encryption can't normally be reversed. If Hype Health Clubs uses an application that needs to read a password, then that is the only time you would want to enable this setting. Keep in mind that when enabling the Store Password Using Reversible Encryption for All Users policy, it's like your passwords are stored as plain text, representing the same security risks. Always be cautious when enabling this policy.

5.3 Network connection policy

5.3.1 Appropriate Connection Methods

Users may connect devices to Hype Health Clubs network at appropriate connectivity points.

Modifications or extensions to the network can cause undesired effects, including loss of connectivity. These effects are not always immediate, nor are they always located at the site of modifications. Therefore, extending or modifying Hype Health Clubs network (e.g. through the addition of switching equipment or routers) must only be done by, or with the guidance of, Hype Health Clubs management.

5.3.2 Network Registration

Users of Hype Health Clubs network may be required to register a device before connecting it. Users may also be required to install a software agent on their device before they are allowed on the network. The role of such an agent would be to ensure that the device complies with current standards.

5.3.3 Responsibility for Security

Users are responsible for ensuring that their computing devices meet all relevant security standards (see *section 5.3.4* below) and for managing the security of the equipment and the services that run on it. Some Hype Health Clubs may assign the responsibility for computer security and maintenance to dedicated IT staff. Therefore, it is possible that one user manages multiple devices plus their own

computing devices. Every user should know who is responsible for maintaining their computing device(s).

5.3.4 Security Standards

Users must ensure that all computing devices capable of running anti-virus/anti-malware software have licensed anti-virus software (or other appropriate virus protection products) installed and running. Owners should update definition files at least once per week.

Users must install the most recent security patches on the system as soon as practical or as directed by IT staff. Where computing devices cannot be patched, other actions may need to be taken to secure the computing devices appropriately.

Users must ensure that they have password, pin code, or biometric access enabled on their devices. Additionally, users who regularly handle research data or sensitive data such as member biographic and registration information must encrypt their devices.

5.3.5 Centrally-Provided Network-Based Services

IT staff is responsible for providing reliable network services for the entire Hype Health Clubs. As such, users may not run any service which disrupts or interferes with IT provided services. These services include, but are not limited to, email, DNS, DHCP, and Domain Registration. Exceptions may be made by IT staff for approved personnel in Hype Health Clubs who can demonstrate competence with managing such services.

5.3.6 Protection of the Network

IT uses multiple methods to protect the Hype Health Clubs network, including:

- monitoring for external intrusion
- scanning hosts on the network for suspicious anomalies
- blocking harmful traffic, both inbound and outbound

Traffic of computing devices connected to Hype health Clubs network may be scanned for signs of compromise.

IT reserves the right to take necessary steps to contain security exposures to Hype Health Clubs. IT will act to contain devices that exhibit the behaviours indicated below, and allow normal traffic and central services to resume:

- imposing an exceptional load on a Hype Health Clubs service
- exhibiting a pattern of network traffic that disrupts centrally provided services
- exhibiting a pattern of malicious network traffic associated with scanning or attacking others
- exhibiting behaviour consistent with a host compromise

IT reserves the right to restrict certain types of traffic coming into and across the Hype Health Clubs network. Computing devices exhibiting any of the behaviours listed above are in violation of this policy and will be removed from the network until they meet compliancy standards.

5.4 Software licensing policy

Hype Health Clubs employs Software as a Service (SaaS) software licensing and delivery model in which software is licensed on a subscription basis and is centrally hosted.

5.5 E-mail usage policy

5.5.1 Purpose

Hype Health Clubs email usage policy helps employees use their company email addresses appropriately. Email is essential to our everyday jobs. Hype Health Clubs want to ensure that its employees understand the limitations of using their company email accounts.

5.5.2 Goal

Hype Health Clubs goal is to protect its confidential data from breaches and safeguard its reputation and technological property.

5.5.3 Scope

This policy applies to all employees, vendors and partners who are assigned (or given access to) a company email. This email may be assigned to an individual (e.g. firstname.lastname@hypehealhtclubs.com.au) or group (e.g. management@hypehealthclubs.com.au)

5.5.4 Policy elements

Company emails are powerful tools that help employees in their jobs. Employees should use their company email primarily for work-related purposes. However, Hype Health Clubs want to provide employees with some freedom to use their emails for personal reasons.

Hype Health Clubs management will define what constitutes appropriate and inappropriate use.

5.5.4.1 Inappropriate use of company email

Our employees represent our company whenever they use their company email address. They must not:

- Sign up for illegal, unreliable, disreputable or suspect websites and services.
- Send unauthorised marketing content or solicitation emails.
- Register for a competitor's services unless authorised.
- Send insulting or discriminatory messages and content.
- Intentionally spam other people's emails, including their coworkers.

Hype Health Clubs has the right to monitor and archive company emails.

5.5.4.2 Appropriate use of company email

Employees are allowed to use their company email for work-related purposes without limitations. For example, employees can use their email to:

- Communicate with current or prospective customers and partners.
- Log in to purchased software they have legitimate access to.
- Give their email address to people they meet at conferences, career fairs or other corporate events for business purposes.
- Sign up for newsletters, platforms and other online services that will help them with their jobs or professional growth.

5.5.4.3 Personal use

Employees are allowed to use their company email for some personal reasons. For example, employees can use their company email to:

- Register for classes or meetups.
- Send emails to friends and family as long as they don't spam or disclose confidential information.
- Download eBooks, guides and other content for their personal use as long as it is safe and appropriate.

Employees must adhere to this policy at all times, in addition to the *Privacy Act 1988*.

5.5.4.4 Email security

Email is often the medium of hacker attacks, confidentiality breaches, viruses and other malware. These issues can compromise Hype Health Clubs reputation, legality and security of its equipment.

Employees must:

- Select strong passwords with at least eight characters (capital and lower-case letters, symbols and numbers) without using personal information (e.g. birthdays).
- Remember passwords instead of writing them down and keep them secret.
- Change their email password in accordance with *section 5.2.3* above.

Also, employees should always be vigilant to catch emails that carry malware or phishing attempts. Hype Health Clubs instruct employees to:

- Avoid opening attachments and clicking on links when content is not adequately explained (e.g. "Watch this video, it's amazing.")
- Be suspicious of clickbait titles.
- Check email and names of unknown senders to ensure they are legitimate.
- Look for inconsistencies or style red flags (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 ask Hype Health Clubs management.

Hype Health Clubs remind employees to keep their anti-malware programs updated.

5.5.4.5 Email signature

Hype Health Clubs encourage employees to create an email signature that exudes professionalism and represents our company well. Salespeople and executives, who represent Hype Health Clubs to customers and stakeholders, should pay special attention to how they close emails. An acceptable email signature block is shown below:

[Click here to insert signature block]

Employees may also include professional images, company logos and work-related videos and links in email signatures. If they are unsure how to do so, they can ask for help from Hype Health Clubs management.

5.5.5 Disciplinary action

Employees who don't adhere to the present policy will face disciplinary action up to and including termination. Example reasons for termination are:

- Using a company email address to send confidential data without authorisation.
- Sending offensive or inappropriate emails to our customers, colleagues or partners.
- Using a company email for an illegal activity.

6 References

Title	Hyperlink
Privacy Act 1988	https://www.legislation.gov.au/Details/C2019C00241

7 Abbreviations and Terminology

Abbreviation/Term	Meaning
CCTV	Closed Circuit Television
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
ICT	Information and Communications Technology
IT	Information Technology
MFP	Multi-function Printer
SaaS	Software as a Service
VPN	Virtual Private Network

8 Document History

Version	Date	Author/Editor	Comments
0.1	03/01/2020	David Murr	Initial draft