Cyber Security Policy

1 Introduction and Scope

1.1 This Cyber Security Policy provides the basis of cybersecurity management within H&M Security Services.

1.2 This policy applies to all of H&M Security Services employees, contractors, volunteers, vendors and anyone else who may have any type of access to H&M Security Services systems, software and hardware.

1.3 Effective protection of business information creates a competitive advantage, both in the ability to preserve the reputation of H&M Security Services and in reducing the risk of the occurrence of negative events and incidents.

2 Password Requirements

To avoid employees' work account passwords being compromised, these best practices are advised for setting up passwords:

(a) Use at least 8 characters (must contain capital and lower-case letters, numbers and symbols).
(b) Do not write down password and leave it unprotected
(c) Do not exchange credentials when not requested or approved by supervisor.
(d) Change passwords every 3 months.

2.2 Email Security

Emails can contain malicious content and malware. In order to reduce harm, employees should employ the following strategies:

(a) Do not open attachments or click any links where content is not well explained.
(b) Check the email addresses and names of senders
(c) Search for inconsistencies
(d) Block junk spam and scam emails.
(e) Avoid emails that contain common scam subject lines such as prizes, products and money transfer

If an employee is not sure that an email, or any type of data is safe, the employee should contact the manager of the company.

2.3 Device Security and Using Personal Devices

Logging in to any work accounts for personal devices such as mobile phones, tablets or laptops, can put H&M Security Services data at risk. H&M Security Services does not recommend accessing any H&M Security Services data from personal devices. However, if this cannot be avoided, employees are obliged to keep their devices in a safe place and not exposed to anyone else.

Employees are recommended to follow these best practices steps:

(a) Keep all electronic devices' passwords secure and protected.

(b) Logging into accounts should only be performed through safe networks.
(c) Install security updates on a regular basis.
(d) Never leave devices unprotected and exposed.
(e) Lock computers when leaving the desk.

3 Transferring Data

Data transfer is a common cause of cybercrime. Employees should follow these best practices when transferring data:

(a) Avoid transferring personal information such as customer data and employee information.
(b) Adhere to the relevant personal information legislation.
(c) Data should only be shared over authorised networks.
(d) If applicable, destroy any sensitive data when it is no longer needed.

4 Working Remotely

Remote employees are also obligated to follow all aspects of this cybersecurity policy as they also will be using company's systems, equipment, and confidential data.

5 Acceptable Use

User accounts on work systems are only to be used for the business purposes of H&M Security Services and not to be used for personal activities.

Employees are responsible for protecting all confidential information used and/or stored on their accounts. This includes their user logins and passwords. Employees are prohibited from making unauthorised copies of such confidential information and/or distributing it to unauthorised person outside of H&M Security Services.

Employees must not purposely engage in any 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 H&M Security Services systems for which they do not have authorisation.

6 Security Requirements

6.1 Employees must not install unauthorised software. The company may at any time introduce a whitelist of approved/trusted programs. If this occurs then only these programs may be used by employees.

6.2 Employees should perform daily backups of important new/changed data, software and configuration settings.

6.3 Employees must not use unauthorised devices on their workstations, unless they have received specific authorisation from the Managing Director Ian Henderson.

6.4 Employees must not attempt to turn off or circumvent any security measures.

6.5 Employees must report any security breaches, suspicious activities or issues that may cause a cyber security breach to the Managing Director Ian Henderson.

7 Disciplinary Action

If this policy is breached, one or more of the following disciplinary actions will take place:

(a) Incidents will be assessed on a case-by-case basis

(b) In case of breaches that are intentional or repeated or cases that cause direct harm to H&M Security Services, employees may face serious disciplinary action.

(c) Subject to the gravity of the breach, formal warnings may be issued to the offending employee.

(d) employee's childcare arrangements to assist with flexible working, or contact in emergency situations.

Employee Name: _____ Date: _____

Signature: _____

The ultimate responsibility for this policy lies with the Managing Director who ensures that it is given and retains the highest of priorities. This policy and its implementation will be reviewed at least annually and updated as required.

Signed by:

Ian Henderson
Managing Director
H & M Security Services