HAVi Security Policy

1. Overview

Protection of company assets is vital to the success of our business. To this end, a security policy is necessary in order to consider the processes required to identify the information we need to protect and how we must protect it.

Because the needs of our business change, we recognise that our management system must be continually improved to meet our needs. To this effect, the policy will be continually assessed and improved upon.

It is the responsibility of everyone within the business to ensure that HAVi Information Security is of the standard outlined in this document.

Security strategy is carried out internally but also through the company who provide us with our server capabilities. Mick Callum, Company Secretary and Andrew Mee Technical Director are therefore responsible for the overall information security.

2. Purpose

This document describes HAVi employees' requirements when dealing with anything in the line of the business that could compromise company or customer information security.

3. Scope

This policy applies to any HAVi employee handling the elements discussed.

4. Target

This policy is intended for HAVi staff in order to understand expected behaviour as well as for HAVi customers to assess the security of HAVi operations when considering supplier relations.

5. Policies

5.1 Acceptable Use Policy

5.1.1 General Requirements

HAVi staff are responsible for exercising good judgment regarding appropriate use of HAVi resources in accordance with HAVi policies, standards, and guidelines. HAVi resources may not be used for any unlawful or prohibited purpose.

For security, compliance, and maintenance purposes, authorised personnel may monitor and audit equipment, systems, and network traffic. Devices that interfere with other devices or users on the HAVi network may be disconnected.

5.1.2 System Accounts

HAVi staff are responsible for the security of data, accounts, and systems under their control.

Passwords must be kept secure and not shared with anyone, including other personnel, family, or friends. Providing access to another individual, either deliberately or through failure to secure its access, is a violation of this policy.

HAVi staff must maintain system-level and user-level passwords in accordance with the Password Policy.

You must ensure through legal or technical means that proprietary information remains within the control of HAVi at all times. Conducting HAVi business that results in the storage of proprietary information on personal or non-HAVi controlled environments, including devices maintained by a third party with whom HAVi does not have a contractual agreement, is prohibited. This specifically prohibits the use of an e-mail account that is not provided by HAVi, or its customer and partners, for company business.

5.1.3 Computing Assets

You are responsible for ensuring the protection of assigned HAVi assets that include the use of computer cable locks and other security devices. Laptops left at HAVi overnight must be properly secured or placed in a locked drawer or cabinet. Promptly report any theft of HAVi assets to HAVi.

All PCs, mobile phones, laptops, and workstations must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended.

5.1.4 Network Use

HAVi staff are responsible for the security and appropriate use of HAVi network resources. Using HAVi resources for the following is strictly prohibited:

- Causing a security breach to either HAVi or other network resources, including, but not limited to, accessing data, servers, or accounts to which you are not authorised; circumventing user authentication on any device; or sniffing network traffic.
- Causing a disruption of service to either HAVi or other network resources, including, but not limited to, ICMP floods, packet spoofing, denial of service, heap or buffer overflows, and forged routing information for malicious purposes.
- Introducing honeypots, honeynets, or similar technology on the HAVi network.
- Violating copyright law, including, but not limited to, illegally duplicating or transmitting copyrighted pictures, music, video, and software.
- Exporting or importing software, technical information, encryption software, or technology in violation of international or regional export control laws.
- Use of the Internet or HAVi network that violates the HAVi, HAVi policies, or local laws.
- Intentionally introducing malicious code, including, but not limited to, viruses, worms, Trojan horses, e-mail bombs, spyware, adware, and key loggers.

5.1.5 Electronic Communications

The following are strictly prohibited:

- Inappropriate use of communication vehicles and equipment, including, but not limited to, supporting illegal activities, and procuring or transmitting material that violates HAVi policies against harassment or the safeguarding of confidential or proprietary information.
- Sending Spam via e-mail, text messages, pages, instant messages, voice mail, or other forms of electronic communication.
- Forging, misrepresenting, obscuring, suppressing, or replacing a user identity on any electronic communication to mislead the recipient about the sender.
- Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).
- Use of a HAVi e-mail or IP address to engage in conduct that violates HAVi policies or guidelines. Posting to a public newsgroup, bulletin board, or listserv with a HAVi e-mail or IP address represents HAVi to the public; therefore, you must exercise good judgment to avoid misrepresenting or exceeding your authority in representing the opinion of the company.

5.2 Authentication Policy

Access to all HAVi data and systems not intended for unrestricted public access requires authentication.

Passwords and other authenticators must be constructed to have a resistance to attack commensurate with the level of system or data access granted to the account.

Systems must be designed and configured to protect passwords during storage and transmission.

No one may require another to share the password to an individually assigned university account, for example as a condition of employment or in order to provide technical support.

5.3 Backup Policy

HAVi IT administrators are responsible for providing system support and data backup tasks and must ensure that adequate backup and system recovery practices, processes and procedures are followed.

All IT backup and recovery procedures must be documented, regularly reviewed and made available to trained personnel who are responsible for performing data and IT system backup and recovery.

All data, operating systems/domain infrastructure state data and supporting system configuration files must be systematically backed up - including patches, fixes and updates which may be required in the event of system re-installation and/or configuration.

All backup media must be encrypted and appropriately labeled with date/s and codes/markings, which enable easy identification of the original source of the data and type of backup used on the media. All encryption keys should be kept securely at all times with clear procedures in place to ensure that backup media can be promptly decrypted in the event of a disaster.

A recording mechanism must be in place and maintained to record all backup information such as department, data location, date, type of backup (e.g. Incremental, Full etc…) including any failures or other issues relating to the backup job.

Copies of backup media must be removed from devices as soon as possible when a backup or restore has been completed.

Backup media which is retained on-site prior to being sent for storage at a remote location must be stored securely in a locked safe and at a sufficient distance away from the original data to ensure both the original and backup copies are not compromised.

Access to the on-site backup location and storage safe must be restricted to authorised personnel only.

All backups identified for long-term storage must be stored at a remote secure location with appropriate environmental control and protection to ensure the integrity of all backup media.

Hard copy paper files containing important information and data should be scanned and stored electronically to ensure digital copies are created which can be backed up by the HAVi's ICT systems. Where this may not be possible, photocopies of paper files must be made and stored in a secure storage location.

Regular tests must be carried out to establish the effectiveness of the HAVi's backup and restore procedures by restoring data/software from backup copies and analysing the results.

Backup data/media no longer required must be clearly marked and recorded for secure disposal and with due environmental consideration (Waste, Electrical and Electronic Equipment - WEEE Directive)

5.4 Confidential Data Policy

Confidential data is stored on the HAVi Total system only and at no point is it held outside of the HAVi Total System.

The data is only to be accessed by users who have authorisation to access the HAVi Total system and the security level that is allocated to their usage.

The personal data stored consists of personnel numbers, names and what exposure risk to vibration that they each employee is subject to. Alongside side this information are training records based on hand arm vibration

There is no medical information kept within the HAVi Total system.

All HAVi employees that have access to the data are vetted and security checked accordingly.

5.5 Data Classification Policy

Company managers or information 'owners' are responsible for assigning classifications to information assets according to the standard information classification system presented below.

Where practicable, the information category shall be embedded in the information itself.

All HAVi associates will be guided by the information category in their security-related handling of HAVi information.

All company information and all information entrusted to HAVi from third parties falls into the one of four classifications in the table below, presented in order of increasing sensitivity.

HAVi classifies its information based on the following structure:

Information Category	**Description**	**Examples**
Unclassified Public	Information is not confidential and can be made public without any implications for HAVi. Loss of availability due to system downtime is an acceptable risk. Integrity is important but not vital	Information widely available to the public such as external marketing materials
Proprietary	Information is restricted to management-approved internal access and protected from external access. Unauthorised access could influence HAVi's operational effectiveness, cause an important financial loss, provide a significant gain to a competitor, or cause a major drop in customer confidence. Information integrity is vital.	HAVi Passwords or information on HAVi security procedures. HAVi TOTAL Software code.
Client Confidential Data	Information received from clients in any form for processing in production by HAVi. The original copy of such information must not be changed in any way without written permission from the client. The highest possible levels of integrity, confidentiality, and restricted	Customer employee training and exposure records. Customer groups and processes.

	availability are vital.	
Company Confidential Data	Information collected and used by HAVi in the conduct of its business to employ people, to log and fulfil client orders, and to manage all aspects of corporate finance. Access to this information is very restricted within the company. The highest possible levels of integrity, confidentiality, and restricted availability are vital.	Personal health surveillance outcomes and actions. Company business plans.

5.6 Encryption Policy

5.6.1 Algorithm Requirements

Ciphers in use must meet or exceed the set defined as "AES-compatible" or "partially AES-compatible" according to the IETF/IRTF Cipher Catalogue, or the set defined for use in the United States National Institute of Standards and Technology (NIST) publication FIPS 140-2, or any superseding documents according to the date of implementation. The use of the Advanced Encryption Standard (AES) is strongly recommended for symmetric encryption.

Algorithms in use must meet the standards defined for use in NIST publication FIPS 140-2 or any superseding document, according to date of implementation. The use of the RSA and Elliptic Curve Cryptography (ECC) algorithms is strongly recommended for asymmetric encryption.

5.6.2 Signature Algorithms

Algorithm	Key Length (min)	Additional Comment
ECDSA	P-256	Cisco Legal recommends RFC6090 compliance to avoid patent infringement.
RSA	2048	Must use a secure padding scheme. PKCS#7 padding scheme is recommended. Message hashing required.
LDWM	SHA256	Refer to LDWM Hash-based Signatures Draft

5.6.3 Hash Function Requirements

In general, HAVi adheres to the NIST Policy on Hash Functions.

5.6.4 Key Agreement and Authentication

Key exchanges must use one of the following cryptographic protocols: Diffie-Hellman, IKE, or Elliptic curve Diffie-Hellman (ECDH).

End points must be authenticated prior to the exchange or derivation of session keys.

Public keys used to establish trust must be authenticated prior to use. Examples of authentication include transmission via cryptographically signed message or manual verification of the public key hash.

All servers used for authentication (for example, RADIUS or TACACS) must have installed a valid certificate signed by a known trusted provider.

All servers and applications using SSL or TLS must have the certificates signed by a known, trusted provider.

5.6.5 Key Generation

Cryptographic keys must be generated and stored in a secure manner that prevents loss, theft, or compromise.

Key generation must be seeded from an industry standard random number generator (RNG). For examples, see NIST Annex C: Approved Random Number Generators for FIPS PUB 140-2.

5.7 Email Policy

All use of email must be consistent with HAVi policies and procedures of ethical conduct, safety, compliance with applicable laws and proper business practices.

HAVi email accounts should be used primarily for HAVi business-related purposes; personal communication is permitted on a limited basis, but non-HAVi related commercial uses are prohibited.

Email should be retained only if it qualifies as a HAVi business record. Email is a HAVi business record if there exists a legitimate and ongoing business reason to preserve the information contained in the email.

The HAVi email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair colour, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any HAVi employee should report the matter to their supervisor immediately.

Users are prohibited from automatically forwarding HAVi email to a third party email system individual messages which are forwarded by the user must not contain HAVi confidential information.

Users are prohibited from using third-party email systems and storage servers such as Google, Yahoo, and MSN Hotmail etc. to conduct HAVi business.

Using a reasonable amount of HAVi resources for personal emails is acceptable, but non-work related email will be saved in a separate folder from work related email. Sending chain letters or joke emails from a HAVi email account is prohibited.

HAVi employees shall have no expectation of privacy in anything they store, send or receive on the company's email system.

HAVi may monitor messages without prior notice. HAVi is not obliged to monitor email messages.

5.8 Guest Access Policy

HAVi allows access when approved, to the HAVi total system.

Guests are set up on a standalone demo account for a set period of time after which the account expires. This account can be used for training and sales purposes.

Software users can allow their own access to the software via there own portal this is out side of HAVi control.

5.9 Incident Response Policy

5.9.1 Incident Reporting

HAVi staff are required to provide a rapid response to incidents that threaten the confidentiality, integrity and availability or information assets, information systems, and the networks that deliver the information.

Incidents will be reported immediately via email and recorded and logged in house.

5.9.2 Penetration Testing

Penetration testing is carried out on an ad-hoc basis by the server house.

5.10 Mobile Device Policy

5.10.1 Technical Requirements

Devices must use the following Operating Systems: IOS 4 or later.

Devices must store all user-saved passwords in an encrypted password store.

Devices must be configured with a secure password that complies with HAVi’s password policy. This password must not be the same as any other credentials used within the organisation.

5.10.2 User Requirements

Users must only load data essential to their role onto their mobile device(s).

Users must report all lost or stolen devices to HAVi IT immediately.

If a user suspects that unauthorised access to company data has taken place via a mobile device the user must report the incident in alignment with HAVi’s incident reporting process.

Devices must not be “jailbroken” or have any software/firmware installed, which is designed to gain access to functionality not intended to be exposed to the user.

Users must not load pirated software or illegal content onto their devices.

Devices must not be connected to a computer which does not have up-to-date and enabled anti-malware protection and which does not comply with corporate policy.

5.11 Network Access Policy

Users are permitted to use only those network addresses issued to them by HAVi.

Users inside the HAVi firewall may not be connected to the HAVi network at the same time a modem is being used to connect to an external network.

Users must not extend or re-transmit network services in any way. This means staff must not install a router, switch, hub, or wireless access point to the HAVi network without HAVi approval.

Users must not install network hardware or software that provides network services without HAVi approval.

Non-HAVi computer systems that require network connectivity must conform to HAVi Standards.

Users must not download, install or run security programs or utilities that reveal weaknesses in the security of a system. For example, HAVi users must not run password cracking programs, packet sniffers, network mapping tools, or port scanners while connected in any manner to the HAVi network infrastructure.

Users are not permitted to alter network hardware in any way.

5.12 Network Security Policy

5.12.1 Network Security

The HAVi information network will be available when needed, can be accessed only by legitimate users and will contain complete and accurate information. The network must also be able to withstand or recover from threats to its availability, integrity and confidentiality. To satisfy this, HAVi will undertake to the following:

- Protect all hardware, software and information assets under its control. This will be achieved by implementing a set of well-balanced technical and non-technical measures.
- Provide both effective and cost-effective protection that is commensurate with the risks to its network assets.
- Implement the Network Security Policy in a consistent, timely and cost effective manner.

5.12.2 Physical & Environmental Security

Network computer equipment will be housed in a controlled and secure environment. Critical or sensitive network equipment will be housed in an environment that is monitored for temperature, humidity and power supply quality.

Critical or sensitive network equipment will be housed in secure areas, protected by a secure perimeter, with appropriate security barriers and entry controls.

Critical or sensitive network equipment will be protected from power supply failures.

Critical or sensitive network equipment will be protected by intruder alarms and fire suppression systems.

Smoking, eating and drinking is forbidden in areas housing critical or sensitive network equipment.

All visitors to secure network areas must be made aware of network security requirements.

All visitors to secure network areas must be logged in and out. The log will contain name, organisation, purpose of visit, date, and time in and out.

5.13 Password Policy

5.13.1 Password Complexity Rules

Strong passwords have the following characteristics:

- Contain at least 12 alphanumeric characters.
- Contain both upper and lower case letters.
- Contain at least one number (for example, 0-9).
- Contain at least one special character (for example,!$%^&*()_+|~-=\`{}[]:";'<>?,/).

Poor, or weak, passwords have the following characteristics:

- Contain less than eight characters.
- Can be found in a dictionary, including foreign language, or exist in a language slang, dialect, or jargon.
- Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.

- Contain work-related information such as building names, system commands, sites, companies, hardware, or software.
- Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.
- Contain common words spelled backward, or preceded or followed by a number (for example, terces, secret1 or 1secret).
- Are some version of “Welcome123” “Password123” “Changeme123”

5.13.3 Password Creation

Users must not use the same password for HAVi accounts as for other non-HAVi access

Where possible, users must not use the same password for various HAVi access needs.

5.13.5 Password Protection

Passwords must not be shared with anyone. All passwords are to be treated as sensitive, Confidential HAVi information.

Passwords must not be inserted into email messages or other forms of electronic communication.

Passwords must not be revealed over the phone to anyone.

Do not reveal a password on questionnaires or security forms.

Do not hint at the format of a password (for example, "my family name").

Do not share HAVi passwords with anyone, including administrative assistants, secretaries, managers, co-workers while on vacation, and family members.

Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption.

Do not use the "Remember Password" feature of applications (for example, web browsers).

Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.

5.12 Remote Access Policy

5.12.1 Access Protocols

Unencrypted protocols (notably FTP and Telnet) must not be used for access from offsite to HAVi systems.

5.12.2 VPN and Firewall Access

All connections from offsite to HAVi computers must be made via a VPN.

5.12.3 Access to PC’s from offsite

Access will not be provided to desktop PC’s from offsite.

6. Definitions

Jailbreak - To jailbreak a mobile device is to remove the limitations imposed by the manufacturer. This gives access to the operating system, thereby unlocking all its features and enabling the installation of unauthorised software.

7. Appendices

Appendix 1 – DBS Procedure

Group 1: Primary identity documents

Document	Notes
Passport	Any current and valid passport
Biometric residence permit	UK
Current driving licence – photocard with paper counterpart	UK, Isle of Man, Channel Islands and EU (full or provisional)
Birth certificate - issued at time of birth	UK and Channel Islands – including those issued by UK authorities overseas, eg embassies, High Commissions and HM Forces
Adoption certificate	UK and Channel Islands

Group 2a: Trusted government documents

Document	Notes
Current driving licence – photocard (if you were issued a paper counterpart but don’t give it to your checker)	All countries (full or provisional)
Current driving licence – paper version	UK, Isle of Man, Channel Islands and EU (full

	or provisional)
Birth certificate – issued after time of birth	UK and Channel Islands
Marriage/civil partnership certificate	UK and Channel Islands
HM Forces ID card	UK
Firearms licence	UK, Channel Islands and Isle of Man

Group 2b: Financial and social history documents

Document	Notes	Issue date and validity
Mortgage statement	UK or EEA	Issued in last 12 months
Bank or building society statement	UK and Channel Islands or EEA	Issued in last 3 months
Bank or building society account opening confirmation letter	UK	Issued in last 3 months
Credit card statement	UK or EEA	Issued in last 3 months
Financial statement, eg pension or endowment	UK	Issued in last 12 months
P45 or P60 statement	UK and Channel Islands	Issued in last 12 months
Council Tax statement	UK and Channel Islands	Issued in last 12 months
Work permit or visa	UK	Valid up to expiry date
Letter of sponsorship from future employment provider	Non-UK or non-EEA only - valid only for applicants residing outside of the UK at time of application	Must still be valid
Utility bill	UK – not mobile telephone bill	Issued in last 3 months
Benefit statement, e.g. Child Benefit, Pension	UK	Issued in last 3 months
Central or local government, government agency, or local council document giving entitlement, e.g. from the Department for Work and Pensions, the Employment Service, HMRC	UK and Channel Islands	Issued in last 3 months
EU National ID card		Must still be valid
Cards carrying the PASS accreditation logo	UK and Channel Islands	Must still be valid
Letter from head teacher or college principal	UK - for 16 to 19 year olds in full time education - only used in exceptional circumstances if other documents cannot be provided	Must still be valid