Security Management Plan

Prepared for Cabinet Office as part of the CCS (Crown Commercial Services) Civil Service Pensions contract

16th June 2017
Security Management Plan for CCS Framework – Civil Service Pensions

This document has been prepared based upon our understanding of the requirements of the Crown Commercial Service – Civil Service Pensions contract - Government Security Policy Framework (SPF) available from www.gov.uk) and with consideration for compliance with HMRC policies and procedures.

Health Management Ltd (HML) is providing Software as a Service (SaaS) services from its own offices and datacentres.

There is no requirement for HML to connect to the Public Services Network (PSN).

Information Security Policy

The purpose of this plan is to detail HML’s security stance toward protecting Customer information assets from internal and external threats, whether deliberate or accidental.

It is HML’s policy to ensure that:
- Information is protected against unauthorised access
- Confidentiality of information is assured
- Integrity of information is maintained (3)
- Regulatory and legislative requirements is met (4)
- Business continuity plans is produced, maintained and tested (5)
- Information security training is undertaken by all staff
- All breaches of information security, actual or suspected, is reported to, and investigated by the Information Security Manager

Standards have been produced to support this policy. These include virus control, access control, passwords and encryption.

Business requirements for the availability of information and information systems is met.

On behalf of the HML Board, HML’s Managing Director; Patrick Birchall, has approved the Information Security Policy.

HNL’s Information Security Manager; Peter Saul, has direct responsibility for day to day management of HNL’s ISO27001 certified ISMS (Information Security Management System) and providing security related advice and guidance on its implementation.

Directors, employees and business partners are responsible for implementing the Information Security Policy within their defined areas.

NOTES:
1. Information takes many forms and includes data stored on computers, transmitted across networks, printed out or written on paper, sent by fax, stored on tapes and diskettes, or spoken in conversations and over the telephone.

2. The protection of valuable or sensitive information from unauthorised disclosure or intelligible interruption.

3. Safeguarding the accuracy and completeness of information by protecting against unauthorised modification.

4. This applies to record keeping it includes the requirements of legislation such as the Companies Act and the Data Protection Act as well as regulations such as Lawful Business Practices and the Combined Code.

5. This will ensure that information and vital services are available to users when they need them.

6. This may be a part or full-time role for the allocated person

**Compliance Policy**

It is the responsibility of each of the above to adhere to this Policy.

Any breach of this policy must be reported and escalated promptly as described in the Security Incident Management Policy (see appendix 1)

**Personal data**

Health Management ensure compliance with the requirements of the Data Protection Act by having appropriate audited controls in place.

Employees are contractually obligated to adhere to the DPA and to the Information Security and IT policies. These policies contain controls designed to ensure compliance.

**Personnel Security**

**Staff handling sensitive/personal/MO data**

Personnel engaged by Health Management are subject to a BPSS style vetting which includes:

- Identity Check
- Employment and Academic history
- Nationality and right to work in the UK
- Unspent criminal records (Disclosure Scotland)
- In the case of clinicians current registration and insurance check

CRB checks are not carried out because HML employees do not work with vulnerable people nor children.
All employees and embedded contractors are required to undertake mandatory training at both
induction and then as part of an annual programme. This includes
- Data protection/information security training
- Conduct and business ethics training
- (for specific roles) Annual refresher training in anticorruption and authority matrix is required.

The responsibilities of contractors with respect to confidentiality are be stated in the requisite
contractual documentation. In addition a risk review is carried out as part of the standard ISMS
procedures for the on boarding of Third Parties.

**Physical Security**

**Physical protection of information**

There is a secured perimeter around the data centre consisting of 7ft high Palisade fencing. Access is
via a gated compound monitored by intrusion detection alarms, managed by an approved supplier
ISO 9001 and 27001.

Security locks are installed on all external doors. Access for HML staff to HML areas is controlled by
individually attributable key fobs and a door access system.

Datacentres and IT cabinets are in dedicated secure areas controlled with two factor access control.
Physical access is controlled electronically and via key access to which only permitted key holders
are allowed.

All visitors are required to report to a manned reception for their escort and to sign confidentiality
paperwork and are not permitted onsite unless escorted. These visitors would not be permitted
access to any of HML’s sensitive areas unless there was a business need and that they were escorted
by a HML member of staff. These visitors are required to wear a ID card at all times. Further access
to the data centre is governed through a regularly audited electronic access fob system. In addition,
the CCTV cameras record every entry and egress and all logs are retained for 90 days.

**System Based Security**

**Outsourcing and Third Party Access**

A risk review is carried out as part of the standard ISMS procedures for the on boarding of Third
Parties, the level of due diligence depends upon the services that are being provided by the Third
Party. The responsibilities of contractors with respect to confidentiality are be stated in the requisite
contractual documentation. Further information is detailed in the Data Protection Policy

In order to proceed these third parties requesting access to Health Management systems must agree
to follow the Health Management information security policy. They will also be required to sign a
confidentiality agreement to protect Health Management and their customers information assets.
As part of the contract HML reserve the right to audit suppliers for compliance.
There is no transfer of any HMRC asset to third parties (any individual or group other than the main
Contractor) without prior written consent from HMRC.

There is no transfer or processing of any HMRC assets outside of the United Kingdom without prior
written consent from HMRC.
Information Handling

All information is handled in accordance with legislation including the Data Protection Act.

HML’s Data Protection registration number: Z8503898, expires: 21 March 2018

The IT policy (see appendix 1) specifically prohibits the use of removable media for storage and transport of customer or company data. Printed material is controlled within workflow processes and with respect to its classification, it is disposed of by on-site shredding as soon as is practicable.

Archive paper records are stored in a controlled environment for their legal or medical lifespan.

A backup and recovery process exists to safeguard against loss of data. HML utilise the DR features of our storage arrays to ensure a robust recovery process. DR tests are performed on a schedule dictated by risk assessment.

These backups are created and encrypted under AES256 which are then managed through an approved supplier Iron Mountain, tape libraries are not organisation identifiable with Iron Mountain barcoded model of management with all tapes being encrypted to AES256. All backups are encrypted and hosted with the ISO certified Iron Mountain facility within the UK.

Our storage arrangements allow high availability and rollback to file level.

Users of Health Management Information systems are subject to controls established through risk assessment, risk treatment plans, audit and management review. Acceptable use of information assets are covered in the HML IT Policy and the Internet Acceptable Use Policy.

All HML assets are inventoried in the Asset Register which is part of the Helpdesk system. All assets are marked and logged in the system and have defined owners. Access to the system is restricted by group policy to only staff that require access as part of their role.

Data is classified to ensure correct handling but we do not use the protective marking system. Our data classification system ensures very clear physical partitions between data types.

Health Management undertakes to preserve any Protective Marking on HMRC data and to educate staff as to the meaning and appropriate treatment of such data.

HMRC data is stored as part of the HML Online database. This database is access controlled utilising the principle of least privilege and has been hardened using vendor best practice. It undergoes an annual IT Security Health Check (pen test) by a certified CREST/CHECK Team.

HMRC data will not be transmitted across networks outside of Health Management without confirming that the recipient is authorised to receive the information and agreeing a method of encryption.

All parties is notified in advance if recording are to be made of telephone conversations or video conferences.

Emails is checked for correct addressing and due care taken when revealing other peoples email addresses when using cc instead of bcc.
Email should only be used for business purposes and in accordance with the Health Management IT Policy (see appendix 1). Due care is taken with email attachments with regard to their classification. Incoming and outgoing attachments is automatically scanned for viruses or other malicious code.

Care is taken when acting upon information received by email due to its inherent information security risks.

Access to HMRC data is on the following basis:

- Access granted on a need to know basis.
- HMRC data is clearly identified as such.
- HMRC data will not be taken or stored overseas.

Equipment and media disposal is controlled by policy, specifically the Data Protection Policy P009 and IT Policy P011 and approved by the HML IA Manager. Whereby any magnetic media is first purged using the Blanco product prior to being securely destroyed by an approved contractor as stated in the Information Security Policy PO11. HML data governance provides a High level process for client data deletion.

HML are ISO27001 & Cyber Essential Plus. Certified and are also SEQOHS certified (Safe, Effective, Quality Occupational Health Service)

**User Management Policy**

As part of the ISO27001 certified ISMS HML maintain an access control policy which is part of the overarching IT Policy PO11

A starters and leavers process is in place. A record is kept of requests for access. These are authorised by the appropriate line manager or other authorised person. They are aligned to the role.

Allocation of rights are determined by the least privilege model. Application rights are allocated on a least privilege basis with staff only being permitted to access data that they have a legitimate business need to access. Local administrative permissions are only granted to HML administrators to enable troubleshooting and maintenance. Standard users do not have any escalated privileges

In addition access rights may be granted only by a competent and authorised systems administrator. A change in rights must be authorised by a line manager or other authorised person. A regular audit of users and rights is performed.

Users ID’s are unique and policy dictates that passwords must not be shared. Use of a user id is restricted solely to the person to whom it was issued

A password complexity policy is automatically enforced by Active Directory and passwords changed on an interval specified in the Health Management IT policy (see appendix 1)

Microsoft Active Directory, operating system and application access controls are used to ensure users have the least privileges required to perform their duties. Each sub-component of the system
has an associated detailed design which details any elevated privileges required for system management duties. Specifically, ICT management and IA security management (e.g. protective monitoring) privileges are segregated to reduce the risk to security log tampering.

Event logging is enabled at all times and Netwrix Auditor software is employed which produces regular reports that are reviewed by the Information Security Manager.

IDS is present on the edge network and monitors for intrusion. A form of IPS is provided by Mailmarshall screens all incoming and outgoing attachments on email.

Staff role changes are performed with an access request, authorised by the new line manager or other authorised person, which will supersede and replace all previous access rights.

**Use of Computers for processing HMRC Information**

All users of the Health Management computer system have signed agreement to comply with the IT policy (see appendix 1).

A password complexity policy is automatically enforced and passwords changed on an interval specified in the Health Management IT policy (see appendix 1).

All computers must be locked when left unattended and will automatically lock out after 20 mins.

Files originating outside of the Health Management computer network and all email attachments should be treated with due care to safeguard against malicious code and inappropriate material, this is carried out by Mailmarshal for email and anti-virus is installed on all servers and end user device images.

Emails is checked for correct addressing. email containing sensitive data must be sent using an encryption method agreed beforehand with the HMRC.

Email containing sensitive data must only be transmitted to persons identified as authorised by the HMRC.

HML utilises a Citrix based desktop ensuring that no HMRC data is stored on laptops or on local PC drives.

Usage of portable media to transport and store HMRC information is prohibited by policy.

**System Planning**

New hardware systems are subject to risk assessment and thorough review before deployment. This may involve consultation with the HMRC where the change is significant and affects HMRC data processing systems directly or as necessary as identified by a risk assessment.

As part of the overarching architectural process, security impact assessment and resulting requirements have been input at the design stage. There is a set of specific security requirements to meet that have been defined by the HML Security Manager and reviewed and agreed by ICT, these include information assurance and business continuity. These have been addressed as part of all designs including the Service Management design. External suppliers have had to address these
Security requirements as part of their design as shown in the system High Level Designs and Low Level Designs.

Software upgrades are subject to careful planning, impact and risk assessment and thorough review before deployment. This may involve consultation with the HMRC where the change is significant and affects HMRC data processing facilities directly or as necessary as identified by a risk assessment.

To ensure secure code development HML operate a Secure System Development Process which aligns with industry practice for staged development, test, release and monitoring. Security testing includes methods automated and procedural such as code scanning and peer code review. We manage the process through Policy P032 IT Secure Service Development Policy and aligns to NIST 800-160 (System Security Engineering).

Capacity management is performed on all systems. All systems is correctly maintained.

A computing ‘terms of use’ is documented in the Health Management IT policy (see appendix 1).

**Network Management**

The Health Management Network is managed only by authorised and suitably qualified staff.

These staff have the responsibility for overseeing day to day running and the integrity and security of the network. All network management staff are given training on information security issues by the HML Security Manager.

A domain security model is employed. All networks used for processing data are protected by a firewall configured appropriately for that data based upon its classification.

All access externally to the HML fixed offices to the HML network uses RSA multi factor for authentication and citrix sessions to ensure no data at rest. All external connections are via encrypted VPNs, multifactor authentication is provided by RSA hard tokens

Users are to be denied access to the network resources unless explicitly allowed to access a specific resource.

Network segregation, connection control and routing control is configured in accordance with guidelines detailed in ISO 18028.

VLANS are not used as a security boundary to separate areas of differing trust levels (e.g they are not used to separate the DMZ and Internal network traffic) but are used to separate traffic within zones.

Dedicated management VLAN/subnets have implemented in both the internal network and the DMZ.

Within the internal network functions are separated

From a procedural perspective groups of information services, user and information systems are segregated in networks in accordance with ISMS 11.07 Network Access and ISMS 11.08 Access Control
Access control procedures ensure that access is strictly controlled and users are denied access by default to network resources. Access is by explicit consent only.

All external connections are via encrypted VPNs, multifactor authentication is provided by RSA hard tokens. A policy is defined within HML Teleworking Policy P037 & IT Policy P011

A Security patch management process is in place that defines the process that is implemented through processes which include the use of IBM IEM (End Point Manager). This ensures that all servers are patched in accordance with software / OS practice on a 6 weekly basis unless there is a critical vulnerability that needs to be addressed. A test before deploy method is adopted. Desktop and Server anti-virus are updated daily as per the ISMS. The patching policy is described in the IT policy (see appendix 1)

Boundary firewalls are be used to protect systems processing HMRC data from external and other networks. They is correctly configured and maintained.

As part of system hardening all unnecessary services are disabled, HML Online undergoes an annual IT Security Health Check by a CREST/CHECK certified team to ensure that minimal risk is presented to the application

Ongoing internal vulnerability scanning is undertaken by Qualsys.

Ongoing website vulnerability scanning is undertaken by White HAT. Both of these products produce real time information on the current vulnerability status of the environment

In addition the network proactively monitored to ensure integrity, confidentiality and availability of data

**Software Management**

Applications used to process HMRC data are managed by suitably trained and qualified staff to oversee their day to day running and to preserve security and integrity in collaboration with nominated individual application owners. All such staff shall be given relevant training in information security issues.

Software upgrades are subject to careful planning, impact and security risk assessment and thorough review before deployment. The HMRC may be consulted before such changes are made where the change is significant or otherwise as revealed by a risk assessment.

Modifications to Vendor supplied software packages is avoided.

The use of Mobile Code is avoided for processing HMRC data.

Change control (see appendix 1) is implemented and will apply to all software changes

**Incident Handling**

Security incidents is handled in line with the Health Management Incident Management Policy (see appendix 1). This policy is widely advertised on a regular basis to all employees.

All incidents must be reported to their respective manager and a call raised on the IT Helpdesk System where an incident is raised. The Data Protection Officer, Information Security Manager and
IT Director will then be informed that the incident has occurred. An initial incident response plan will then be implemented.

Where weaknesses have been identified as part of the Security Incident report or other form of report (ITSHC) these are assessed for the level of risk presented to the information and then a suitable mitigation plan is implemented. Depending upon the weakness will depend upon the action undertaken however as examples this could be implementation of new technical controls or enhancements to current policies.

Upon any security event that occurs, this is either presented at the next account management meeting as part of a to be agreed set of security reporting metrics or is reported immediately by the HML Information Security Manager depending upon the severity of the event.

HML have a Forensic Readiness Policy that outlines the requirements for the correct procedures to follow in the event of an investigation.

**Mobile Computing**

The HML ISMS outlines the requirements to control HML Assets whilst off premises.

Mobile computing users are subject to the restrictions and notes relating to mobile computing contained within the IT Policy (see appendix 1).

In summary mobile computers must be encrypted

No data may be stored on the hard drives of mobile computers

Mobile access to the HML network is restricted to access via Citrix

Extra care and attention must be used when using a mobile computing device with due consideration given to the surrounding environment and risks that it may pose.

For 3rd Parties this is covered in contractual agreements and it is mandated that all data at rest must be encrypted to ensure privacy if the data is lost.

There is currently no BYOD mobile or laptop solution permitted for the HML corporate infrastructure.

**Teleworking**

Persons who do part or all of their work using dedicated equipment in a fixed location HML premises (teleworking) must be authorised to do so by an appropriate Supplier authority. A risk assessment based on the criticality of the information assets or software application being accessed and the appropriateness of the proposed telework location should be carried out.

Teleworkers who contribute to HML’s services for the HMRC is provided with appropriate computing and communications equipment and must use this equipment only for teleworking. The equipment provided may only be modified or replaced if this has been authorised. All equipment must be returned at the end of the teleworking arrangement, or when the teleworker leaves the company.
All teleworking agreements will include appropriate measures, based on a risk assessment, to protect the security of HMRC information assets. Teleworkers must follow the agreed security procedures at all times.

All external connections are via encrypted VPNs, multifactor authentication is provided by RSA hard tokens. A policy is defined within HML Teleworking Policy P037 & IT Policy P011

Cryptography

Any HMRC Protectively Marked data that leaves the HML processing environment must be encrypted.

A risk assessment is carried out before any data is removed from HML premises

Cryptographic keys is stored with due consideration for their highly sensitive nature.

Business Continuity and Disaster Recovery Provisions (BCDR)

HML Operate an IT Disaster Recovery Plan which is governed by the P005 Disaster Recover & Contingency Policy which is tested periodically.

These plans are tested on a schedule identified by risk assessment but not less than once every 12 months

A communication strategy forms part of the BCDR plans.

The HML Disaster Recovery & Contingency Policy states RTO and ROP as 24 hours

1 TOPIC-SPECIFIC POLICIES

Paragraphs in italics are excerpts from ISO 27001 controls

Security of third party access

Objective: To maintain the security of organisational information processing facilities and information assets accessed by third parties.

Access to data processing systems by outside organisations and the transfer of data between Health Management and outside organisations is restricted for reasons of security and in accordance with requirements of Data Protection Act 1998. The Information Systems Security Group receives and considers requests for such access, and gives appropriate advice to management.

The list of organisations with access is maintained by the Information Security Officer in conjunction with the operations team. Access to the organisation’s information processing facilities by third parties should be controlled.

Where there is a business need for such third party access, a risk assessment should be carried out to determine security implications and control requirements. Controls should be agreed and defined in a contract with the third party.

Third party access may also involve other participants. Contracts conferring third party access should include allowance for designation of other eligible participants and conditions for their access.

This standard could be used as a basis for such contracts and when considering the outsourcing of information processing.

Outsourcing

Objective: To maintain the security of information when the responsibility for information processing has been outsourced to another organisation.

Staff involved in arranging contracts for the outsourcing of information processing are required to include procedures for the maintenance of information security and compliance with the Data Protection Act 1998 in the contract. The Information Security Officer must be informed, who will give advice to management.

Outsourcing arrangements should address the risks, security controls, and procedures for information systems, networks and/or desktop environments in the contract between the parties.

Accountability for assets

Objective: To maintain appropriate protection of organisational assets.
The Information Security Officer shall maintain a list of all Information Databases along with the designated member of staff responsible for implementing controls.

All organisational assets are required to be registered in the Health Management Asset Register.

All major information assets should be accounted for and have a nominated owner.

Accountability for assets helps to ensure that appropriate protection is maintained.

Owners should be identified for all major assets and the responsibility for the maintenance of appropriate controls should be assigned.

Responsibility for implementing controls may be delegated. Accountability should remain with the nominated owner of the asset.

**Information classification**

Objective: To ensure that information assets receive an appropriate level of protection.

Owners of information assets are required to record details of the requirements for protection of the information, and to take appropriate action.

Information should be classified to indicate the need, priorities, and degree of protection.

Information has varying degrees of sensitivity and criticality; some items may require an additional level of protection or special handling. An information classification system should be used to define an appropriate set of protection levels, and communicate the need for special handling measures.

**Personnel security**

**Security in job definition and resourcing**

Objective: To reduce the risks of human error, theft, fraud or misuse of facilities.

All staff should be made aware of their responsibilities with regard to information security.

This includes both specific job-related responsibilities and those contained within the Information Systems Security Manual and Guidelines. Access to information will only be granted once this requirement has been satisfied.

HR should identify staff with responsibility for handling sensitive data, who should be appropriately screened during the recruitment process and monitored periodically during employment.

All staff are responsible for complying with the Policy and Guidelines.

Security responsibilities should be addressed at the recruitment stage, included in contracts, and monitored during an individual’s employment. Potential recruits should be adequately screened, especially for sensitive jobs.

All employees and third party users of information processing facilities should sign a confidentiality (nondisclosure) agreement.
User Awareness

Objective: To ensure that users are aware of information security threats and concerns, and are equipped to support organisational security policy in the course of their normal work.

The Information Systems Security Group shall determine what is required to make users aware of the need for information security, and make appropriate arrangements, including the production of Information Systems Security Guidelines documentation. This would include examples of security incidents.

Users should be trained in security procedures and the correct use of information processing facilities to minimise possible security risks.

Incident Response: Responding To Security Incidents And Malfunctions

Objective: To minimise the damage from security incidents and malfunctions, and to monitor and learn from such incidents.

All users must report any security incidents that they become aware of. Users should report incidents via the IT Help Desk (xxxx)

The Information Systems Security Incident Report Form, (see Appendix 2) is completed by IT and submitted to the Information Security Officer.

The Information Security Officer may call an emergency meeting of the Information Systems Security Group who will consider these reports, and organise appropriate dissemination to stakeholders.

Individuals who commit security breaches are subject to the Staff Disciplinary Procedures Incidents affecting security should be reported through appropriate management channels as quickly as possible.

All employees and contractors should be made aware of the procedures for reporting the different types of incident (security breach, threat, weakness or malfunction) that might have an impact on the security of organisational assets.

They should be required to report any observed or suspected incidents as quickly as possible to the designated point of contact The organisation should establish a formal disciplinary process for dealing with employees who commit security breaches. To be able to address incidents properly it is necessary to collect evidence as soon as possible after the occurrence.

Physical and Environmental Security

Secure areas

Objective: To prevent unauthorised access, damage and interference to business premises and information.

Physical Protection – Ringmer Server Room and Network Wiring Closets

The server room at Ringmer and all network wiring closets are regarded as secure areas. They are kept physically secure through the use of appropriate locks and other security measures. Staff are instructed to keep these areas locked when not occupied.
Further details are kept confidential.

The responsibilities of IT regarding the physical protection of servers are listed in Appendix 7: Responsibility of IT Operating Servers.

Critical or sensitive business information processing facilities should be housed in secure areas, protected by a defined security perimeter, with appropriate security barriers and entry controls.

They should be physically protected from unauthorised access, damage, and interference.

The protection provided should be commensurate with the identified risks. A clear desk and clear screen policy is recommended to reduce the risk of unauthorised access or damage to papers, media and information processing facilities.

**Equipment Security**

Objective: To prevent loss, damage or compromise of assets and interruption to business activities.

The equipment in the server room is kept at the correct temperature and humidity by the use of air conditioning systems. The performance of these is recorded on a paper chart.

The power-supply in main computer rooms is protected by UPS systems which are subject to regular periodic test.

Staff users of computers or any related hand-held device are required to protect their own computer or hand-held device from loss or damage and to take appropriate measures to keep information secure. In addition, before any computer or device is disposed of, steps must be taken to erase all data stored internally.

Equipment should be physically protected from security threats and environmental hazards.

Protection of equipment (including that used off-site) is necessary to reduce the risk of unauthorised access to data and to protect against loss or damage. This should also consider equipment siting and disposal. Special controls may be required to protect against hazards or unauthorised access, and to safeguard supporting facilities, such as the electrical supply and cabling infrastructure.

**General Controls**

Objective: To prevent compromise or theft of information and information processing facilities.

Only authorised people are allowed access to areas containing sensitive information systems.

It is the responsibility of individual members of staff to keep their offices and personal computer secure. IT ensure that computers in common areas, e.g. staff room, areas are secure.

Information and information processing facilities should be protected from disclosure to, odification of or theft by unauthorised persons, and controls should be in place to minimise loss or damage.

**Communications and operations management**

**Operational procedures and responsibilities**
Objective: To ensure the correct and secure operation of information processing facilities.

Appropriate training is provided for all staff who are required to operate information processing systems.

Responsibilities and procedures for the management and operation of all information-processing facilities should be established.

This includes the development of appropriate operating instructions and incident response procedures.

Segregation of duties should be implemented, where appropriate, to reduce the risk of negligent or deliberate system misuse.

Health Management IT Policy

Purpose

The purpose of the IT Policy is to ensure the effective protection and proper usage of the computer systems within Health Management.

The IT investment of the organisation is considerable, and the dependency on computer technology in the delivery of Health Management services is high. The IT Policy will assist in maintaining systems at operational level.

Contraventions of the IT Policy could seriously disrupt the operation of Health Management and any breaches is treated seriously.

Legislation That Applies

- Data Protection Act
- Computer Misuse Act
- Copyright Design and Patents Act
- Health and Safety at Work Act
- Related Policies, Procedures or Reference Points
- Training and Development Policy
- Disciplinary and Grievance Policy
- Employee Handbook
- Internal Procedures
- Disaster Contingency Plan
- ISO27001 procedures and manual

Health Management Policy

HML’s policy is divided into five key sections covering the Computer Systems; Computer Users; Email, Internet and Remote Access; Data Security and the Contravention terms of the IT Policy.

Section 1 – Computer Systems

Network
Network management, administration and maintenance within Health Management are the responsibility of the IT Department. Access to and administrative operation of the:

- Servers and other network infrastructure equipment is restricted to authorised staff.
- Hardware (PCs, Laptops, Printers, Modems, etc.)
- The requirement for IT equipment will normally be identified within the context of an IT strategy for Health Management or within the context of staff expansion.
- The purchase, installation, configuration and maintenance of computer equipment are the responsibility of the IT Department.
- Computer equipment registers is maintained by the IT Department to ensure full tracking of equipment.
- Requirements for new hardware should be discussed in advance with the IT Director/Manager to assess the detailed specification.
- The deployment of new equipment or re-deployment of existing equipment is undertaken by the IT Department after consultation with Department Managers.
- The relocation of hardware within, or outside of, Health Management premises should be discussed with the IT Director / Manager in advance to ensure good reason for relocation, determine the most appropriate means of relocation and to ensure computer equipment registers and insurance policies are updated.
- The security and safekeeping of portable and other equipment used outside Health Management offices is the responsibility of the member of staff using it.
- All members of staff are responsible for the proper usage, care and cleanliness of the computer equipment they use. Managers should ensure that staff maintain the cleanliness of their machines.
- Problems with hardware should be promptly reported to the IT Department in accordance with established IT Help Desk procedures.

Software & Software Applications

- The requirement for software will normally be identified within the context of an IT strategy for Health Management and more specifically within a planned software upgrade programme.
- The purchase, installation, configuration and support of all software and software applications used within Health Management are the responsibility of the IT Department.
- Software, including screensavers, must not be installed by users without prior authorisation from the IT Department. This includes programs downloaded from the Internet.
● Health Management will treat the installation of unlicensed software by users as a serious breach of the IT Policy.

● Original software media is kept securely by the IT Department.

● Requirements for new software/software applications should be discussed in advance with the IT Director / Manager to assess the detailed specification and implications.

● Problems with software should be reported promptly to the IT Department.

● Requests for modifications, enhancements and upgrades of existing software applications should be discussed with the IT Director / Manager.

Data/Electronic Information

● Data Management should be in accordance with the Data Security section of this policy.

● Managers are responsible for maintaining the quality of the computer-held data processed by their staff.

● The individual user is responsible to their line manager for the quality of the computer data they have personally processed.

● Managers are responsible for ensuring compliance with Data Protection legislation with regards to data processed within their teams.

● In conjunction with the nominated Data Protection Officer the IT Director will keep abreast of data protection legislation, advise accordingly and ensure applications and databases are registered if appropriate in accordance with the legislation.

● All information/data held on Health Management systems is deemed the property of Health Management

● As a condition of employment, staff consent to the examination of the use and content of all data/information processed and/or stored by the staff member on Health Management systems as required.

Back Up

● The IT Department is responsible for ensuring the production and implementation of an effective Back-up Strategy for server-held software and data. This forms part of the Disaster Contingency Plan

● Backups is regularly inspected for consistency and a restore test carried out on a schedule agreed by the IT Director

● Due reference to the Data Security section of this policy should be made when moving or storing backups.

● Users of networked desktop PCs should avoid storing data on their local hard drives. Data so stored may be lost if a problem develops with the PC, and the IT Department may not be able
to assist in its recovery. Data should be stored within the file directory (folder) structure used by the office or within your “My Documents” folder.

**Anti-Virus and Perimeter Protection**

- The IT Department is responsible for the implementation of an effective Anti Virus and Anti Malware solution as part of the IT Security Strategy.
- The IT Department is responsible for the implementation of an effective management and monitoring system for firewalls and VPNs.
- The installation of anti-virus software on all machines is the responsibility of the IT Department.
- The IT Department will ensure the upgrade of the anti-virus software on networked desktop PCs.
- Remote users and users of portable machines will assist in the upgrade of anti-virus software in accordance with specified mechanisms agreed with the IT Department, e.g. internet updates.
- Staff should present all media (including USB drives, floppy disks, zip disks, CDs and DVDs) to the IT department before first use for virus scanning and approval.
- On detection of a virus staff should notify the IT Department who will provide assistance in accordance with the Incident Management Policy.
- Under no circumstances should staff attempt to disable or interfere with the virus scanning software.
- Computers or devices which are not the property of Health Management must be authorised by the IT Department in accordance with the IT Security Strategy before connecting to the network.

**Change Management**

All changes to Health Management IT equipment must take the IT Security Policy into consideration, such as changes to:

- Network Configuration
- Firewall and VPN configuration
- Backup Configuration

must first be authorised by the IT Director or other such nominated competent person in their absence.

Changes to;
- Server configuration
- Live Database schema or configuration
- Live Application configuration
- File Security and Group Policy
- Telephone System

must first be authorised by the IT Director or other such nominated competent person in their absence, except when the change is a common minor maintenance or management task. All server logins must be recorded in the Server Activity Log web application and include a plan and justification.

Consumables (Toner / Paper / Batteries etc)

It is the responsibility of Managers to ensure that they have an adequate system to maintain a small stock of consumables for the IT equipment that their team uses.

Section 2 – Computer Users

Health & Safety

- Health and safety with regards to computer equipment and computer work stations should be managed within the context of the general and any specific Health & Safety policies and procedures within Health Management.

- Managers are responsible for ensuring health & safety legislation and procedures with regards to computer equipment are implemented within their Departments.

Training

- It is the responsibility of Managers to ensure appropriate computer training for their staff is identified. The IT Department can advise on, and often directly provide, computer related training.

User Accounts

- The HR Manager should notify the IT Department of new members of staff in advance to allow the creation of network and e-mail accounts and system permissions.

- The HR Manager should notify the IT Department of the departure of staff to allow the deletion of network accounts and redirection or cancellation of e-mail accounts.

Passwords

- The IT Department will ensure a secure password system is part of the IT Security Strategy

- Users should change their passwords when prompted by the system in the case of networked machines or on a regular basis for standalone machines.
• Staff are responsible for the security of their password which they should not divulge, even to colleagues. If you need access to a colleague’s inbox or other mail folders or calendars this should be provided through the email system security mechanism– the IT Department can advise on this.

• Problems with passwords or breaches/suspected breaches of password security should be reported promptly to the IT Department.

System Usage

• The IT Department is responsible for automatically hibernating or turning off computers overnight as required to minimise power consumption. Users should turn off their screens at the end of the day.

• Computers should be locked or logged off when left unattended for any significant period of time and should be used in accordance with the Data Security section of this policy.

• All faults must be reported promptly through the IT Help Desks, no attempt must be made to repair equipment, software or configuration yourself.

Section 3 - e-mail, Internet and Remote Access

Email

• The Health Management e-mail system is a core business application. It should not be used for political, business or commercial purposes not related to Health Management.

• The Health Management e-mail system must not be used to send illegal or inappropriate material.

• The Health Management e-mail system must be used in accordance with the Data Security section of this policy

• Limited personal use of email is permitted. Managers should ensure there is no abuse of this privilege.

• It is a condition of employment that all staff consent to the examination of the use and content of their email accounts as required

• Global distribution lists should be used appropriately. Email to all staff (spamming) should be used only when appropriate.

• Staff should minimise the number of messages in their email in-box to ensure maximum efficiency of the delivery system. Folders should be set up and messages filed accordingly.

• Staff should utilise the archiving facility within the email system in accordance with current guidelines

• Confidential material sent by email should be so marked but sent only with caution and due reference to the Data Security section of this policy.
Caution should be exercised when opening unsolicited attachments or emails.

To help fight junk mail staff should avoid providing their email addresses in online forms/registrations unless absolutely necessary to carry out their duties.

The IT Department will also provide measures to reduce junk mail as appropriate and in accordance with the IT Security Strategy.

Health Management retains the right to access and view all emails sent and received by the email system. This right is exercised solely through the IT Director or other nominated competent person on the instructions of the Managing Director.

Webmail

Webmail access is granted on a discretionary basis by managers.

Whilst using Webmail to access your email account, extra precautions must be taken to ensure the security of Health Management information. The IT Department will provide advice on this.

Internet

Access to the Internet is provided for business purposes. Limited personal use is permitted and is to be restricted to lunch breaks and periods outside working time.

Staff should not make inappropriate use of their access to the Internet. They must not use Health Management systems to access pornographic, illegal or other improper material.

Staff should not subscribe to chat rooms, dating agencies, messaging services or other online subscription Internet sites unless they pertain to work duties.

The IT Department may deploy content filtering and packet management to control or manage internet access as appropriate in accordance with the IT Security Strategy.

Programs, including screensavers, must not be downloaded from the Internet without authorisation from the IT Department.

No instant messenger software (eg msn messenger / yahoo messenger/ AIM) is to be installed or used except in the course of legitimate company business and where it has been approved by the IT Director.

Web requests which use an unusually large amount of bandwidth e.g. streaming video/audio should only be made when necessary to carry out work duties or otherwise at the discretion of the IT Director.

Staff must not use peer to peer file sharing networks such as BittTorrent, Kazaa, eDonkey etc. The IT Department may block this traffic in accordance with the IT Security Strategy.

Strategy
Health Management retains the right to monitor Internet usage by staff. This right is exercised solely through the IT Director or other nominated competent person and, where relating to a specific member of staff, only on instructions from the Managing Director.

It is a condition of employment that all staff consent to the examination of the use and content of their Internet activity as required.

Abuse of Internet access is dealt with severely relative to seriousness.

Remote Access

- Remote access to the Health Management network is granted on a discretionary basis by managers.

- A Remote Access facility should always be used in accordance with the Data Security section of this policy.

- It is the employee’s responsibility to ensure that the computer they use is protected by an adequate password, an updated anti-virus system, has an appropriate firewall and is physically secure. The IT Department will advise on this.

- Remote access is provided by the IT department in the form of a Citrix desktop and, where appropriate, an IP telephone which would require a VPN connection to head Office.

- Only hardware or software supplied by the IT Department for that purpose may be used to establish the VPN.

- Mobile Citrix users must be extra vigilant whilst accessing their desktop when out of the office.

Section 4 – Data Security

Introduction

Data is considered a primary asset and as such must be protected in a manner commensurate to its value. Data security is necessary in today’s environment because dataprocessing represents a concentration of valuable assets in the form of information, equipment, and staff. Dependence on information systems creates a unique vulnerability for our organisation.

Security and privacy must focus on controlling unauthorised access to data.

Security compromises or privacy violations could jeopardize our ability to provide service; lose revenue through fraud or destruction of proprietary or confidential data; violate business contracts and customer privacy; or reduce credibility and reputation with our customers and partners.

The main objective of this section of the policy is to ensure that data is protected in all of its forms, on all media, during all phases of its life cycle, from unauthorized or inappropriate access, use, modification, disclosure, or destruction. This policy applies to all of our data assets and all customer data assets that exist, in any of our processing environments. The processing environment is considered to be, collectively, all applications, systems, and networks that we own or operate.
Data Classification

Data classification is necessary to enable the allocation of resources to the protection of data assets, as well as determining the potential loss or damage from the corruption, loss or disclosure of data.

- To ensure the security and integrity of all data the default data classification for any data asset is either Confidential Customer Data or Proprietary Company Data.

- Managers are responsible for evaluating the data classification schema and reconciling it with new data types as they enter usage. It may be necessary, as the business develops, to create additional data classifications.

- All data found in the processing environment must fall into one of the following categories:

  - **Public Company Data** – Public company data is defined as data that any entity either internal or external to Health Management can access. The disclosure, use or destruction of Public company data will have limited or no adverse affects on Health Management nor carry any significant liability.

  - **Proprietary Company Data** – Proprietary company data is any information that derives its economic value from not being publicly disclosed. It includes information that Health Management is under legal or contractual obligation to protect. The value of proprietary company information to Health Management would be destroyed or diminished if such information were disclosed to others. Most Health Management sensitive information should fall into this category. Proprietary company information may be copied and distributed within Health Management only to authorised users. Proprietary company information disclosed to authorised external users must be done so under a non-disclosure agreement. (Examples of Proprietary company data include company policies, sales plans, and application source code)

  - **Confidential Company Data** – Confidential Company Data is information that is not to be publicly disclosed, regardless of its economic value. The disclosure, use, or destruction of Confidential Company Data can have adverse affects on Health Management and possibly carry significant civil, fiscal, or criminal liability. This designation is used much less frequently. It is used for highly sensitive information whose access is restricted to selected, authorised employees. The recipients of confidential information have an obligation not to reveal the contents to another individual unless that person has a valid need to know for the information. Company confidential information must not be copied without authorisation from the identified owner. (Examples of Confidential Company Data include company strategic plans, certain HR information or cryptographic keys.)

  - **Confidential Customer Data** – Confidential customer data is defined as data that only authorised internal Health Management entities or specific authorised external entities can access. The disclosure, use, or destruction of confidential customer data can have adverse affects on Health Management and their relationship with their customers, and possibly carry significant liability for both. Confidential customer data is entrusted to and may transit or is stored by Health Management (and others) over which they have custodial
responsibility but do not have ownership. (Examples of Confidential customer data including employee information, customer bank account information, cryptographic keys, or other data considered private.)

- **Public Customer Data** – Public customer data is defined as data that any entity either internal or external to Health Management can access. The disclosure, use, or destruction of Public customer data will have limited or no adverse affects on Health Management or the customer, and carry no significant liability. Public customer data is entrusted to, and may transit or be stored by Health Management (and others) over which they have custodial responsibility but do not have ownership. (Examples of Public customer data include emails, public key certificates or other customer data that is readily available through other public channels or records.)

**Ownership & Management**

- In order to classify data it is necessary that an owner be identified for all data assets.

- The owner of data is responsible for classifying their data according to the classification schema outlined in this policy. If an owner cannot be determined for a Health Management data asset, the IT Department will act as its custodian.

- The IT Department is responsible for developing, implementing, and maintaining procedures for identifying all data assets and associated owners

- Staff must be familiar with the data classification scheme and implications of disclosure or loss as outlined in part 3 of this policy section and understand how to identify different classes of data. Training is provided by the IT Department as necessary.

- Data must be processed, transmitted or stored with due regard for its classification.

- Data classed as Confidential or Proprietary is encrypted in accordance with the IT Security Strategy.

- All reasonable efforts must be made to maintain the security of Health management data assets at all times.

- The IT Department is responsible for ensuring the technical security of the computer network by maintaining an IT Security Strategy which details specific measures and procedures which must be noted or followed by the IT Department.

- The physical security of Servers and Backup devices which contain Health Management data assets should be regularly reviewed.

- Deployment of new equipment such as servers, web servers, and storage devices must be made in accordance with this policy and comply with the current IT Security Strategy.
Staff leaving the company will have their accounts suspended promptly prior to authorisation from the IT Director to delete them.

Printed data should be treated as having the same security classification as its source data. Anything other than data classed as Public must be shredded at the end of its life cycle.

Backup data is treated as Confidential Company Data.

Any suspected breach in security must be escalated immediately to the IT Director or other nominated competent person.

**Security**

The security and safekeeping of portable and other equipment used outside Health Management offices is the responsibility of the member of staff using it.

- The use of USB and other portable electronic storage devices is prohibited except for use at sales presentations and storing only sales material or standard documents. Devices must be returned to IT for inspection before being plugged into an HML computing device.

- Storage of medical or client specific data or files (HML or client) on any computer other than HML desktop PC’s joined to the security domain or core networking infrastructure is prohibited.

- Storage of medical or client specific data on laptops is prohibited. Laptops may be used to process such data when either directly connected to the security domain in Head Office and using central files (such as the x drive) or via citrix if off site or at a client’s location.

- Laptop hard drives and other portable storage media are to be encrypted before use.

- Users of HML web applications must not download and store data on devices other than as specified in point 1.

- Users of HML webmail must not download and permanently store medical or client specific data on devices other than as specified in point 1.

- Data must be processed, transmitted or stored with due regard for its classification.

- Data classed as Confidential or Proprietary is encrypted in accordance with the IT Security Strategy.

- All reasonable efforts must be made to maintain the security of Health management data assets at all times.

**Section 5 - Contravention of the IT Policy**

- Staff should be aware of their responsibilities under the Data Protection Act, Computer Misuse Act1 and the Copyright Design and Patents Act. The IT Department will provide guidance where required.
• Contravention of the Health Management IT Policy or any act of deliberate sabotage to Health Management computer systems may be considered a disciplinary offence or gross misconduct.

• Computer Users shall not, by any wilful or deliberate act, jeopardize the integrity of the computing equipment, its systems programs or any other stored information to which they have access. Under the Terms of the Computer Misuse Act (1990), unauthorized access to a computer (sometimes called "hacking") or other unauthorized modification to the contents of a computer (such as the deliberate introduction of viruses) are criminal offences punishable by unlimited fines and up to 5 years imprisonment.