medicash a positive approach to health	Reference:	Information Security Policy.doc
	Issue Date:	15th April 2024
	Review Date:	15th April 2025
INFORMATION SECURITY POLICY	Author:	Paul Marley
	Approver:	Andrew Roberts
	Issue Number:	6.1

POLICY AREA:

Organisational

POLICY STATEMENT:

Introduction

This information security policy is a key component of Medicash Health Benefits Limited ("Medicash") overall information security management framework and will be considered alongside other security documentation.

Aim of Policy

The aim of the Medicash information security policy is to preserve:

- **Confidentiality**
  Access to Data shall be confined to those with appropriate authority.

- **Integrity**
  Information shall be complete and accurate. All systems, assets and networks shall operate correctly, according to specification.

- **Availability**
  Information shall be available and delivered to the right person, at the time when it is needed.

1. Organisational Responsibilities

.

Medicash fosters a culture of shared accountability and proactive commitment to safeguarding information security at every level of the organisation. Medicash shall ensure that all staff fully understand their responsibilities to information security and data protection. Medicash shall provide staff with annual training and ongoing updates, awareness sessions and educational resources to ensure information is always handled securely.

Leadership and commitment

Management shall demonstrate leadership and commitment of the Information Security Management System (ISMS) by;

- ensuring this information security policy and its objectives are established, monitored and compatible with the strategic direction of the business.
- ensuring the integration of the ISMS within the businesses processes and procedures.
- ensuring that suitable resources needed for the ISMS are available.
- communicating the importance of effective information security and meeting the requirements of the ISMS.
- ensuring the ISMS achieves its intended outcomes.
- encouraging others to contribute to the effectiveness of the ISMS.
- promoting continual improvements to processes, procedures and service delivery.
- supporting relevant management and team leaders to demonstrate leadership within their areas of responsibility.

2. Information Security Objectives

Training

Information security awareness shall be included in the staff induction process. An ongoing awareness programme shall be maintained in order to ensure that staff awareness is refreshed and updated as necessary.

Contracts of Employment

Employee security requirements shall be addressed at the recruitment stage and all contracts of employment shall contain a confidentiality clause. Information security expectations of staff shall be included within the staff handbook. All staff shall be vetted through the Disclosure and Barring Service (“DBS”).

Access Controls

Access to information shall be restricted to authorised users who have a bona-fide business need to access the information.

Computer Access Controls

Access to information shall be restricted to authorised users who have a bona-fide business need to access the information.

Application Access Controls

Access to data, system utilities and program source libraries shall be controlled and restricted to those authorised users who have a legitimate business need e.g. systems or database administrators. Authorisation to use an application shall depend on the availability of a licence from the supplier.

Equipment Security
To minimise loss of, or damage to, all assets, equipment shall be physically protected from threats and environmental hazards.

Information Risk Assessment
Once identified, information security risks shall be managed on a formal basis by the Risk Group Committee ("RGC"). They shall be recorded within the information security risk register and relevant action shall be put in place to effectively manage those risks.

Information Security Events and Weaknesses
All information security events, and suspected weaknesses are to be reported using the Medicash Help Desk and escalated to the IT Manager. All information security events shall be investigated to establish their cause and impacts with a view to avoiding similar events. The IT Manager shall ensure that appropriate events and weaknesses are escalated to the Information Governance Group as and when required.

Logging of events
Microsoft Defender for Endpoint shall be enabled for endpoint detection and response (EDR).
All log files (e.g., application, system, network) shall be retained for 12 months in accordance with compliance requirements.
Firewall logs (Dimension) shall be retained to separate storage and retained for a minimum of 12 months.

Protection from Malicious Software
Medicash shall use software countermeasures and management procedures to protect itself against the threat of malicious software. All staff shall be expected to co-operate fully with this policy. Users shall not install software on the organisation's property without permission from the IT Department.

User Media
Removable media of all types that contain software or data from external sources, or that have been used on external equipment, require the approval of the IT Department before they may be used on Medicash systems.

System Change Control
Changes to information systems, applications or networks shall be reviewed and approved by following the Change Management Policy.

Intellectual Property Rights
Medicash shall ensure that all information products are properly licensed. Users shall not install software on the organisation's property without permission from the IT Department.

. **Business Continuity and Disaster Recovery Plans**
Medicash shall ensure that business impact assessment, business continuity and disaster recovery plans are produced for all mission critical information, applications, systems and networks.

Remote Working
Remote workers must ensure that company data and systems remain secure when working offsite. Medicash requires all remote employees to use company-approved devices, encrypted connections (VPN), and multi-factor authentication for accessing company resources. Confidential information must not be stored on personal devices

or shared via unauthorised channels. Employees are responsible for maintaining a secure working environment and must report any security incidents immediately.

3. Person Identifiable Information (PII)

Handling paper-based information

When paper-based personal identifiable information is received it will be stored securely, as soon as practical, for example:

- Inbound correspondence will be delivered to the mail sorting area promptly
- Any policy specific information received by post will be scanned and attached to the associated policy record, stored securely for 30 days and the paperwork securely destroyed.

Printing or Copying PII from the Policy database

There may be occasions when PII is required to be printed or copied to alternate media, however before transferring data, consider whether the media will remain within the confines of the Medicash office and if not, that such information can be secured appropriately and if possible to limit those details necessary in order for the recipient to carry out their role.

By Post

- Ensure envelopes are marked “Private & Confidential”
- Double check the full postal address of the recipient.
- Carefully consider the method for sending confidential information based on risk of loss.
- When necessary, ask the recipient to confirm receipt or send via recorded delivery.

Communication by email

When information is to be transmitted by email, the sender must ensure;

- The correct email address of the recipient.
- The subject line of the email is prefixed ‘Encrypted –‘ followed by the message subject or the Encrypt email option is taken within Outlook using Egress.
- The minimum amount of information is being transmitted.

Removable media

Confidential, Sensitive and Personal Identifiable Information must not be stored or carried on non-encrypted memory sticks. Confidential, sensitive or PII carried on encrypted memory sticks must not under any circumstance be placed on non-Medicash issued computers. Such information must always remain on the encrypted device and be immediately transferred onto user’s departmental Network drive and deleted from the encrypted memory stick once no longer required to be on the device.

4. User Account Management

The creation, suspension and deletion of user accounts are the responsibility of the IT department. User accounts must not be requested by the individual user but can be requested by HR and\or a company director using the Helpdesk.

When a user’s contract ends, the HR Department must raise a Helpdesk request.

Account Housekeeping

The CTO will periodically check that all user accounts are still in use. If an account has not been accessed for 28 days then the account may be suspended until either HR or the user’s departmental head has been contacted.

. **Password Resets**

Users will inevitably forget their passwords, when this occurs the user must request a new password from IT.

Compromised Accounts

If an account or password is suspected to have been compromised, immediately report the incident to the IT Department, such passwords must be changed.

. **Password Security**

All users will be provided with a unique User Name and password in order to access the Medicash servers and applications

- A password must be at least eight characters long and not relate to the user's name or system account. The password must not be one of the previous 12, will remain valid for 180 days and must contain a mix of case, a number and a non-alphanumeric character.
- Passwords must not be written down or inserted into email messages or other forms of electronic communication.
- All passwords must be changed after the initial network login
- Network (Domain) passwords will lockout following 3 failed attempts and can only be reinstated by the IT department.
- Passwords must not be shared across different accounts or services
- USB MFA devices must be used for all domain related logins

Unattended Equipment and Clear Screens

Users must ensure that they protect the network from unauthorised access.

- Users must lock their screen when leaving their desk area
- Users must log off the network when they have finished working. .
- If a PC is left unattended for a short time the user will be required to re-input their password to reactivate the session.
- Desktop computers must be shut down at the end of each day

Clear Desk policy

Employees are required to ensure that all sensitive/confidential information in hardcopy or electronic form is secure in their work area .and desks are cleared at the end of each day

- Restricted or Sensitive information must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the work day.
- Filing cabinets containing Restricted or Sensitive information must be kept closed and locked when not in use or when not attended.
- Keys used for access to Restricted or Sensitive information must not be left at an unattended desk

5. Reporting of Security Incidents

Any security incident, including an active data breach or breach of credentials, must be reported to the IT team urgently, either in person or by calling **0151 702 0306**. Examples of security incidents that must be reported immediately include, but are not limited to:

- Suspected or confirmed data breaches (e.g., accidental sharing of personal data, loss of confidential information).

- Compromised user accounts (e.g., suspected hacking, unauthorised access to business systems).
- Lost or stolen company devices (e.g., laptop, mobile phone)
- Suspicious emails or phishing exploits
- Unauthorised access to secure areas or tampering with company IT infrastructure.

Timely reporting is critical to mitigating risks and ensuring the security of company data. The incident management policy must be adhered to following notification of an incident.

6. Hardware and Software

- Staff with non-Medicash provided portable devices are not allowed to connect them to the Network.
- Software downloaded from the Internet must not be loaded onto systems managed and supported by the IT Department.
- Software obtained illegally must not be loaded onto any devices.
- Upon termination of employment or contract, the user is required to return all Medicash owned properties as soon as possible.
- The user will exercise care in using and housing Medicash equipment.
- The IT Department may recall laptops and portables devices at any time to audit their use.
- All devices, software purchases or associated licenses must be registered using your Medicash email address only.
- All Devices must be enrolled within Microsoft Intune\Entra

Protection of Portable equipment

- The user is responsible for safeguarding of the portable device hardware. In this case, it means: When not in use, portable devices must be kept in a locked drawer.
- While in transit, portable devices will be in a suitable carrying case and must be kept out of view wherever possible.
- Portable device security is always the responsibility of the user.
- Do not leave the portable device unattended in a public place e.g. car park. Do not keep password credentials in the same location as the portable device.
- Avoid leaving the portable device within sight of ground floor windows or within easy access of external doors.

Security of Data

- Confidential data must only be installed on portable devices which have been supplied by the IT Department and must be protected with BitLocker and decryption keys stored within Intune\Entra
- If work is being carried out in public places, meeting rooms and other unprotected areas care will be taken to avoid the unauthorised access to or disclosure of the information stored and processed by the portable device
- Care will be taken by the staff using the portable device to minimise the risk of unauthorised persons overlooking the screen
- Confidentiality Policies apply equally to information whether in the office or at home. Failure to maintain confidentiality may result in a disciplinary action

- Data backup solution is provided centrally on the Medicash data network and not on each portable device. It is the user's responsibility to ensure that their data is frequently copied to the data network, for backup purposes
- The use of the portable device and the data on it must not be shared with family members

Backup of Information
Medicash shall ensure that critical business information is regularly backed up and recoverable in the event of data loss or system failure.

- Backup procedures shall be documented, tested, and reviewed periodically.
- Backups shall be encrypted and stored securely in multiple locations.
- Retention periods for backups shall align with regulatory and business requirements.
- Restore tests shall be conducted at regularly to verify data integrity.

Accounting/Audit
The software and information held on portable devices are subject to the same audit procedures as the Medicash desktop computer systems. This also covers information and data stored on removable media e.g. memory sticks, CDs, DVDs.

7. Disposal of Equipment
This policy applies to any and all items that are recorded on the Medicash Asset Register held within Navision and controlled by the Finance Department.
This policy details the process that must be followed for the disposal of any computer related equipment within Medicash. This includes Personal Computer's (desktop or laptop), Tablets, Smartphones, printers, scanners and any other peripheral device.

Any Personal Computer or device for storing data which is managed and supported by the IT Department is considered as a confidentiality risk, and has the potential for unlawful disclosure.

- All hard disk drives are considered likely to contain information that either relates to staff or policyholders (or both), which will not be available to unauthorised individuals.
- No disk will be disposed of before any data that is held on it is erased, in such a way that it cannot be recovered by anyone with sufficient technical skill.
- Appropriate disposal of all Medicash equipment will be undertaken by the IT Department or by their approved contractors.

. Departments are responsible for advising the IT Department when an item of equipment is no longer required.

IT Department Responsibilities

- The IT Department is responsible for assessing whether the equipment could be suitably redeployed.
- Before disposal, the IT Department will confirm with the user that no data is held locally which needs to be retained. All data will be copied to the users network drive.
- In the event of such data being discovered then the data will be copied for safe storage and security onto a data network file server and the user notified.
- The equipment maybe dismantled and used for spare part purposes. In this case the hard disk will be erased to a complete and unrecoverable state or physically destroyed.

- In the event that any equipment is un-repairable or has no other useful life it will be disposed of, and the hard disk will be physically destroyed.
- After disposal, the IT Department will inform the Finance department to record the disposal on the relevant Asset Register, including the reason and method of disposal and which person undertook the task.
- All IT systems, network devices, and applications shall be synchronised to a reliable, approved time source using Network Time Protocol (NTP) to ensure accurate logging, event correlation, and compliance with security and audit requirements.

8. Virus and Malware Control

Medicash shall implement proactive measures to detect, prevent, and mitigate malware threats across IT systems, applications, and user endpoints.

- All workstations, servers, and cloud environments shall have Microsoft Defender for Endpoint enabled for real-time malware detection and response.
- Microsoft Defender for Office 365, DarkTrace Antigena and Egress Defend shall scan all inbound/outbound emails for phishing, ransomware, and malicious attachments/links.
- Only approved applications shall be installed on company devices, enforced through Microsoft Intune and Windows Defender Application Control (WDAC).
- Antivirus definitions and security patches for endpoint protection software shall be updated daily.
- Employees shall receive quarterly phishing and malware awareness training, with simulated phishing campaigns to test and improve awareness.
- Suspected malware infections shall trigger an automated isolation and forensic analysis process using Defender for Endpoint.
- The Medicash domain has Anti-Virus software packages installed and monitored by IT Department
- These packages are installed to prevent attacks from malicious software and to prevent loss of data and corruption of programs/files on the desktop system.
- Medicash users are not permitted to change the Anti-Virus application settings and access to the configuration page will be password protected.
- The IT Manager is responsible for reporting and checking the daily reporting logs and acting appropriately to resolve any issues.

9. Asset Management

Assets Recorded – Hardware

The following hardware items are recorded by the IT Department.

- File Servers
- Network Devices (including Switches & Routers)
- Desktop PCs
- Laptops
- Tablets
- Monitors
- Printers, Scanners or other Peripherals
- Network Attached Storage
- Telephony hardware
- Mobile Phones

. **Assets Tags**

All hardware assets must retain an asset tag; this asset tag serves as the key identifier within the asset database.

All desktop\laptop devices are enrolled within Microsoft Intune to monitor their usage, compliance and

10. Management of Technical Vulnerabilities

Medicash shall proactively identify, assess, and mitigate technical vulnerabilities in IT systems to minimize security risks.

- Automated scans shall be conducted using Microsoft Defender for Cloud and Qualys to detect system vulnerabilities.
- All security patches shall be applied within 7 days for critical vulnerabilities and 30 days for moderate risks, managed via Azure Update Management.
- Emerging threats shall be monitored through Microsoft Threat Intelligence and mitigation strategies implemented within 48 hours.
- A real-time asset inventory shall be maintained in Microsoft Purview to track systems and prioritise remediation efforts.
- All security patches shall be tested in a controlled environment before deployment to production.
- External security assessments shall be conducted annually to identify exploitable vulnerabilities in Medicash's infrastructure and applications.

11. Third Party Providers

Appointing a Third Party

All third parties are subject to signing the Medicash Non-Disclosure agreement ("NDA") prior to any information being released. A copy of the signed NDA must be stored within the relevant project folder and a scanned copy distributed to a company director.

The Third Party Engagement process must be completed.

Site and System Access

- All third Parties are prohibited from accessing company systems or associated networks. A secure Guest network is provided for visitor use which is subject to terms and conditions.
- All third parties are required to be accompanied at all times during their visit
- Under no circumstance is any information, albeit Paper based, electronic or any other media be permitted to be removed from the premises without the approval of a company director and such information be transported in a secure manner.
- In the event that a third party requires access to restricted or sensitive information, a Risk assessment must be completed and actions resolved prior to its release and that such information can be secured appropriately and if possible, to limit those details necessary in order for the recipient to carry out their role.

Service Review

The services provided by established Third Parties will be reviewed on a regular basis and at least twelve-monthly intervals. A record of these reviews must be stored within the ISMS Operation folder.

12. Cloud Services

To ensure continuity of Cloud services, Medicash have considered factors such as reputation, security practices, compliance certifications, and pricing. Microsoft Azure

services align with our requirements and therefore all business cloud services shall be deployed using the UK region of Microsoft Azure only. Adoption of Microsoft Azure ensures ongoing compliance with our ISO27001 requirements. Medicash will monitor our cloud service provider(s) for security incidents, performance, and compliance with a regular review of access controls, permissions, and user activity. Medicash will address any identified vulnerabilities promptly.

High-availability architectures shall be designed for key IT infrastructure.

Medicash shall implement redundancy measures to ensure the availability and resilience of critical information systems.

13. Information Retention, Integrity and Destruction

- Data retention periods shall be defined and documented for all systems and data types within the Document Retention Policy.
- Secure deletion methods (e.g., cryptographic erasure, data shredding) shall be used for digital assets.
- Physical media (e.g., hard drives, USBs) shall be physically destroyed using approved disposal methods.
- Deletion activities shall be logged and audited periodically.

14. Data Loss Prevention

Medicash shall deploy Data Leakage Prevention (DLP) measures to prevent unauthorised transmission of sensitive information outside the organisation using Microsoft 365 services, Watchguard Firewalls and Darktrace Antigena.

- DLP solutions shall monitor and restrict the transfer of sensitive data via email, cloud storage, and external devices.
- Alerts and automatic blocking shall be configured for unauthorized data transfers.
- Employees shall receive training on secure data handling and the risks of data leaks.
- Automated reports shall be reviewed and actioned as appropriate.

15. Cryptography

Medicash shall implement cryptographic controls to protect sensitive data and ensure confidentiality, integrity, and authenticity in accordance with legal, regulatory, and business requirements.

- All sensitive data, including personally identifiable information (PII) and financial data, shall be encrypted in transit and at rest using industry-recognised cryptographic algorithms (e.g., AES-256, RSA-2048, SHA-256)
- All external and internal communications involving sensitive data shall use secure transmission protocols (e.g., TLS 1.2 or higher, HTTPS, VPN, IPsec)
- Access to encryption tools and cryptographic keys shall be restricted based on the principle of least privilege.
- Cryptographic controls shall align with applicable regulatory requirements, including GDPR and UK Data Protection Act.

16. Capacity Management

Medicash shall ensure that IT resources within Microsoft Azure and Microsoft 365 are monitored and scaled effectively to maintain performance, availability, and cost efficiency.

- Azure Monitor, Log Analytics, and Microsoft 365 Admin Centre shall be used to track resource utilization, performance trends, and capacity thresholds.

- Azure Auto scale shall be enabled for virtual machines, databases, and applications to prevent performance degradation.
- Azure Cost Management & Billing shall be used to analyse and optimise resource consumption to prevent unnecessary expenditures.
- Workloads shall be reviewed annually to ensure that storage, compute, and network resources are right sized according to business demands.

17. Configuration Management

Medicash shall enforce secure and standardised configuration management practices for Microsoft Azure and Microsoft 365 to reduce security risks and ensure compliance.

- All cloud resources shall follow predefined configuration baselines, enforced through Azure Policy and Microsoft Defender for Cloud.
- Azure Security Centre and Microsoft Purview Compliance Manager shall be used to detect deviations from approved configurations.
- Any modifications to system configurations shall follow a documented Change Management Process, requiring approval through Microsoft Intune or Azure DevOps Pipelines.
- Updates and security patches for Azure VMs, Microsoft 365 applications, and other managed services shall be deployed using Windows Update for Business and Microsoft Endpoint Manager.
- Role-Based Access Control (RBAC) shall be applied within Azure AD and Microsoft 365 Admin Centre to restrict configuration changes to authorised personnel only.

18. Validity of this Policy

This policy will be reviewed annually, unless any significant impact or changes to legislation, under the authority of the Information Governance Group. Associated information security standards will be subject to an ongoing development and review programme.