HealthMatters
Specialists in Employee Benefits

# Information security policy

## Policy objectives

1 This policy is intended to establish the necessary policies, procedures and an organisational structure that will protect Health Matters (UK) Ltd and its customers, information assets and critical activities from all appropriate threats and to ensure regulatory, statutory, contractual and legislative requirements are met.

2 Compliance with this policy is necessary to ensure business continuity, and to minimise business damage by preventing and minimising the impact of security incidents.

## Scope

3 This policy applies to:

3.1. All departments and the information processed by those departments.

3.2. All Health Matters (UK) Ltd operations run out of the offices in Coventry.

3.3. All information processed by Health Matters (UK) Ltd in pursuit of all its operational activities, regardless of whether it is processed electronically or in paper form.

3.4. All information transferred or exchanged with third parties or held by third parties on behalf of the Health Matters (UK) Ltd, regardless of whether it is processed electronically or in paper form.

## Communication

4. This policy will be made available to all those working for or on behalf of the Health Matters (UK) Ltd and made available on the Health Matters (UK) Ltd website to Health Matters (UK) Ltd suppliers, customers and stakeholders.

## Policy Statement

5. It is the policy of Health Matters (UK) Ltd to ensure that:

5.1. Information assets and information processing facilities shall be protected against unauthorised access

5.2. Information shall be protected from unauthorised disclosure

5.3. Confidentiality of information assets shall be a high priority

5.4. Integrity of information shall be maintained.

5.5. Health Matters (UK) Ltd requirements, as identified by information asset owners, for the availability of information assets and information processing facilities required for operational activities shall be met.

5.6. The management of the supply chain requires those negotiating contracts to ensure appropriate information security and business continuity measures are included in contracts, where possible, so that the service provider is able to deliver acceptable levels of service.

5.8. Business continuity plans shall be produced, maintained and tested.

5.9. Unauthorised use of information assets and information processing facilities shall be prohibited; the use of obscene or otherwise offensive statements shall be dealt with in accordance with other policies published by Health Matters (UK) Ltd.

6. All breaches of information security, actual or suspected, shall be reported and investigated in line with Health Matters (UK) Ltd policies.

7. Controls shall be commensurate with the risks faced by Health Matters (UK) Ltd.

8. In support of this Information security policy, more detailed security policies and processes shall be developed for those working for or on behalf of Health Matters (UK) Ltd, information assets and information processing facilities.

## Information security objectives

9. The objectives of the Information security management system are:

10. To provide the necessary policies, procedures and an organisational structure that will protect Health Matters (UK) Ltd information assets and critical activities from all appropriate threats and to ensure regulatory, statutory, contractual and legislative requirements are met.

11. To ensure business continuity, and to minimise business damage by preventing and minimising the impact of security incidents.

11.1. To preserve the appropriate level of confidentiality, integrity and availability of Health Matters (UK) Ltd information assets and critical activities.

## Responsibilities

12. Health Matters (UK) Ltd directors shall be accountable for ensuring that appropriate and effective information security controls are implemented, monitored and reviewed to ensure compliance with the Health Matters (UK) Ltd legal regulatory or contractual obligations.
13. Health Matters (UK) Ltd directors shall be responsible for ensuring that Health Matters (UK) Ltd information security objectives are aligned with the organisation's objectives.

14. Health Matters (UK) Ltd directors shall be accountable for ensuring that appropriate security, legal and regulatory controls are identified, implemented and maintained by information owners. They shall be supported in this task by all staff.

15. Information asset owners within Health Matters (UK) Ltd shall be responsible for the identification, implementation and maintenance of controls for the information assets they own and the risks to which they are exposed.

16. The role and responsibility for facilitating information security at an operational level shall be performed by the Managing Director.

17. Managers within every business area are responsible for implementing security policies and procedures in their areas including with the third parties that they manage. As part of the formal assessment of security effectiveness, they will be required to account for security problems, breaches, and the security performance of their areas.

18. All staff whether permanent or temporary are responsible for the protection of the Health Matters (UK) Ltd information assets, enabling the confidentiality, integrity and availability of these assets to be maintained.

19. All third-party suppliers to Health Matters (UK) Ltd are to conform to this policy.

20. All staff must adhere to all policies relating to Information Security. Non-compliance will be subject to investigation and may result in disciplinary action under Health Matters (UK) Ltd disciplinary procedure. Disciplinary action shall be consistent with the severity of the incident, as determined by an investigation and may include, but not be limited to:

    - Loss of access privileges to information assets or information processing facilities

    - Disciplinary action including termination of employment and legal prosecution

    - Other actions as deemed appropriate by management, the Human Resources Department and legal advice.

## Governance

21. Information Security will be governed, and the effectiveness measured by the following methods:

21.1 Internal audit

21.2 Business continuity and service continuity exercises

21.3 Management review e.g. risk assessments, results of awareness training, lessons learnt from security incidents and identified improvement opportunities.

21.4 The results from these processes will enable the business to review the effectiveness of the controls and continually develop the Management System.

22. The Directors will review and approve the prioritisation of information security aspects of the internal audit schedule on an annual basis, ensuring that every business process is audited at least once in a 3-year period.

23. The Information Security policy will be reviewed every 12 months or when there are significant changes to ensure it is being implemented correctly and consistently and that quality is maintained.

## Security awareness and training

24. Staff with access to information assets and information processing facilities shall be educated on their information security responsibilities. Education shall be provided as part of the induction process so that new staff completely understand their responsibilities in the protection of information assets and information processing facilities.

25. Staff shall be provided with on-going security education and supporting reference materials. Human Resources and/or the Data Protection Officer shall provide refresher courses and other security related materials to regularly remind staff about their obligations with respect to information security

26. The security responsibilities of third parties shall be made clear at an early stage of the contract by the person responsible for engaging the third party

## Risk Management

27. A systematic approach to information security risk management has been adopted to identify business needs regarding information security requirements (including legal, contractual and regulatory) and to create an effective operational information security framework.

29. Information security risk management is not a one-off exercise with a single set of control recommendations which remain static in time but a continual process.

During the operational delivery and maintenance of Health Matters (UK) Ltd services there are several instances where risk assessment is necessary.

30. The implementation of the information risk strategy shall be based on formal methods for risk assessment, risk management and risk acceptance and independent of technology or software.

## Continual improvement

31. The Directors shall ensure continual improvement of the information security management system.

## Legislation and standards

32. The list below contains some of the legislative and regulatory requirements Health Matters (UK) Ltd must comply with:

Data Protection Act 1998

The General Data Protection Regulation (from 25 May 2018)

Freedom of Information Act 2000

Human Rights Act 1998

Computer Misuse Act 1990

Companies Act 2006

Health & Safety at Work Act

Employment Legislation

Bribery Act 2010

Fraud Act 2006

Regulation of Investigatory Powers Act 2000

## Glossary

| | |
|---|---|
| **Asset** | Anything of value to the organisation. There are many types of assets including information, software, hardware and intangible assets such as reputation. |
| **Availability** | The property of being accessible and usable upon demand by an authorise entity. |
| **Business continuity management** | A process that identifies potential threats to an organisation and the impacts to operations that those threats, if realised, might cause. It provides a framework for building the capability for an effective response that safeguards the interests of its key stakeholders and the organisation's reputation. |
| **Confidentiality** | The property that information is not made available, or disclosed to unauthorised individuals, entities or processes. |
| **Information security** | Information security is the protection of information from a wide range of threats in order to minimise business risk. Information security is the preservation of confidentiality, integrity, and availability of information. |
| **Information security management system** | Part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve the organisation's information security. |
| **Integrity** | The property of protecting the accuracy and completeness of assets. |
| **Personal information** | Any information that relates to one specific person. It can be their name, address, or telephone number. It can also be the type of job they do, their preferences, records of attendance, qualifications, and so on. |
| **Physical security** | This covers the assets, and the way those assets are used, to restrict physical access and the presence of people in certain locations to stop theft of, or damage to, assets and property. This may include guards, locked doors, identity checks and movement controls. |