

## **Information security policy**

### **Policy objectives**

- 1 This policy is intended to establish the necessary policies, procedures and an organisational structure that will protect NMC's 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**

4. This policy applies to:
  - 4.1. All directorates and the information processed by those directorates.
  - 4.2. All NMC's operations run out of the offices in London and Edinburgh.
  - 4.3. All information processed by NMC in pursuit of all its operational activities, regardless of whether it is processed electronically or in paper form.
  - 4.4. All information transferred or exchanged with third parties, or held by third parties on behalf of the NMC, regardless of whether it is processed electronically or in paper form.

### **Communication**

5. This policy will be made available to all those working for or on behalf of the NMC and made available on the NMC website to NMC's suppliers, customers and stakeholders.

### **Policy Statement**

5. It is the policy of NMC to ensure that:
  - 5.1. Information assets and information processing facilities will be protected against unauthorised access

- 5.2. Information will be protected from unauthorised disclosure
- 5.3. Confidentiality of information assets will be a high priority
- 5.4. Integrity of information will be maintained.
- 5.5. NMC's requirements, as identified by information asset owners, for the availability of information assets and information processing facilities required for operational activities will 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.
- 5.7. Any supplier engaged by NMC to handle payment card data will comply with the Payment Card Industry Data Security Standard (PCI).
- 5.8. Business continuity plans will be produced, maintained and tested.
- 5.9. Unauthorised use of information assets and information processing facilities will be prohibited.
6. All breaches of information security, actual or suspected, will be reported and investigated in line with NMC's policies.
7. Controls will be commensurate with the risks faced by the NMC.
8. In support of this Information security policy, more detailed security policies and processes will be developed for those working for or on behalf of the NMC, 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 NMC's 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.
  12. To preserve the appropriate level of confidentiality, integrity and availability of NMC's information assets and critical activities.

1643317

Updated August 2023  
Next review: September 2024

## Responsibilities

- 9 The NMC's Chief Executive and Registrar and NMC's directors will be accountable for ensuring that appropriate and effective information security controls are implemented, monitored and reviewed to ensure compliance with the NMC's legal regulatory or contractual obligations.
- 10 NMC's directors will be responsible for ensuring that the NMC's information security objectives are aligned with the organisation's objectives.
- 11 NMC's directors will be accountable for ensuring that appropriate security, legal and regulatory controls are identified, implemented and maintained by information owners. They will be supported in this task by all colleagues.
- 12 Information asset owners within the NMC will be responsible for the identification, implementation and maintenance of controls for the information assets they own and the risks to which they are exposed. A list of information assets and their owners is set out in the *Information Asset register*.
- 13 NMC's directors will ensure continuous compliance monitoring within their area of jurisdiction. Compliance will be a matter for periodic review by the Information Governance and Security Board (IGSB).
- 14 The IGSB is responsible for setting the priorities for the information security work programme. A programme of reviews and assessments of security effectiveness will form part of this programme, and will establish an agenda for security improvements.
- 15 The role and responsibility for facilitating information security at an operational level shall be performed by Head of Information Compliance and Data Protection officer, including convening the IGSB.
- 16 Managers within every business areas 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.
- 17 All colleagues whether permanent or temporary are responsible for the protection of the NMC's information assets, enabling the confidentiality, integrity and availability of these assets to be maintained.
- 18 All third party suppliers to the NMC are to conform to this policy.
- 19 Specific roles in respect of responsibility and accountability for information governance activities including information security, records management, data governance, technical security and business continuity are set out in the *Information Security Roles and Responsibilities RACI chart*.

- 20 All colleagues must adhere to all policies relating to Information Security and Data Protection. Non-compliance will be subject to investigation and may result in disciplinary action under NMC's disciplinary procedure. Disciplinary action will be consistent with the severity of the incident, as determined by an investigation and may include, but not be limited to:
  19. Loss of access privileges to information assets or information processing facilities
  20. Disciplinary action including termination of employment and legal prosecution
  21. Other actions as deemed appropriate by management, the People and Organisational Effectiveness directorate and legal advice.

## **Governance**

- 23 Information Security will be governed and the effectiveness measured by the following methods:
  - 23.1 Internal audit
  - 23.2 External audit, e.g. Regulator (The Professional Standards Authority), ISO 27001 International Standard for Information Security, Payment Card Industry Standard (PCI DSS)
  - 23.3 Business continuity and service continuity exercises
  - 23.4 Management review e.g. risk assessments, results of awareness training, lessons learnt from security incidents and identified improvement opportunities.
  - 23.5 The results from these processes will enable the business to review the effectiveness of the controls and continually develop the Management System.
- 24 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**

- 26 All colleagues with access to information assets and information processing facilities will be educated on their information security responsibilities. Education shall be provided as part of the induction process so that new colleagues understand their responsibilities in the protection of information assets and information processing facilities.
- 27 Colleagues will be provided with on-going security education and supporting reference materials to regularly remind staff about their obligations with respect to information security.
- 28 The security responsibilities of third parties will be made clear at an early stage of the contract by the person responsible for engaging the third party.

## **Risk Management**

- 29 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.
- 30 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 NMC's services there are a number of instances where risk assessment is necessary.
- 31 The implementation of the information risk strategy will be based on formal methods for risk assessment, risk management and risk acceptance and independent of technology or software.

## **Continual improvement**

- 32 The Chief Executive and Registrar and directors will ensure continual improvement of the information security management system.

## Legislation and standards

33 The list below contains some of the legislative and regulatory requirements NMC must comply with:

Data Protection Act 2018

UK General Data Protection Regulation

Privacy and Electronic Communications (EC Directive) Regulations 2003

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

The Payment Card Industry Data Security Standard

## Glossary

<b>Asset</b>	Anything of value to the organisation. There are many types of assets including information, software, hardware and intangible assets such as reputation.
<b>Availability</b>	The property of being accessible and usable upon demand by an authorised entity.
<b>Business continuity management</b>	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.
<b>Confidentiality</b>	The property that information is not made available, or disclosed to unauthorised individuals, entities or processes.
<b>Information security</b>	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.
<b>Information security management system</b>	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.
<b>Integrity</b>	The property of protecting the accuracy and completeness of assets.
<b>Physical security</b>	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.