Information Security Policy

IOCOM's statement of Information Security Compliance

Date: Thursday, April 19, 2018

Contents

1 Introduction

The confidentiality, integrity and availability of information, in all its forms, are critical to the on-going functioning and good governance of IOCOM.

This information security policy outlines IOCOM's approach to information security management. It provides the guiding principles and responsibilities necessary to safeguard the security of the company's information systems. Supporting policies, codes of practice, procedures and guidelines provide further details.

IOCOM is committed to a robust implementation of Information Security Management. It aims to ensure the appropriate confidentiality, integrity and availability of its data. The principles defined in this policy will be applied to all of the physical and electronic information assets for which the IOCOM is responsible.

IOCOM is specifically committed to preserving the confidentiality, integrity and availability of documentation and data supplied by, generated by and held on behalf of third parties pursuant to the carrying out of work agreed by contract in accordance with the requirements of data security standard ISO 27001.

1.1 Objectives

The objectives of this policy are to:

1. Provide a framework for establishing suitable levels of information security for all IOCOM information systems (including but not limited to all Cloud environments commissioned or run by IOCOM, computers, storage, mobile devices, networking equipment, software and data) and to mitigate the risks associated with the theft, loss, misuse, damage or abuse of these systems.
    a. This explicitly includes any ISO27001-certified Information Security Management Systems the company may run.
    b. The resources required to manage such systems will be made available

c. Continuous improvement of any ISMS will be undertaken in accordance with *Plan Do Check Act* principles

2. Make certain that users are aware of and comply with all current and relevant UK and EU legislation.
3. Provide the principles by which a safe and secure information systems working environment can be established for staff and any other authorized users.
4. Ensure that all users understand their own responsibilities for protecting the confidentiality and integrity of the data that they handle.
5. Protect IOCOM from liability or damage through the misuse of its IT facilities.
6. Maintain research data and other confidential information provided by suppliers at a level of security commensurate with its classification, including upholding any legal and contractual requirements around information security.
7. Respond to changes in the context of the organization as appropriate, initiating a cycle of continuous improvement.

1.2 Scope

This policy is applicable to, and will be communicated to, all staff and third parties who interact with information held by the IOCOM and the information systems used to store and process it.

This includes, but is not limited to: Cloud systems developed or commissioned by IOCOM, any systems or data attached to the IOCOM data or telephone networks, systems managed by IOCOM, mobile devices used to connect to IOCOM networks or hold IOCOM data, data over which IOCOM holds the intellectual property rights, data over which IOCOM is the data controller or data processor, electronic communications sent from the IOCOM.

2 Policy

2.1 Information security principles

The following information security principles provide overarching governance for the security and management of information at IOCOM.

1. Information should be classified according to an appropriate level of confidentiality, integrity and availability (see *Section 2.3. Information Classification*) and in accordance with relevant legislative, regulatory and contractual requirements (see *Section 2.2. Legal and Regulatory Obligations*).
2. Staff with particular responsibilities for information (see *Section 3. Responsibilities*) must ensure the classification of that information; must handle that information in accordance with its classification level; and must abide by any contractual requirements, policies, procedures or systems for meeting those responsibilities.
3. All users covered by the scope of this policy (see *Section 1.2. Scope*) must handle information appropriately and in accordance with its classification level.
4. Information should be both secure and available to those with a legitimate need for access in accordance with its classification level.
    a. On this basis, access to information will be on the basis of *least privilege* and *need to know*.
5. Information will be protected against unauthorized access and processing in accordance with its classification level.
6. Breaches of this policy must be reported (see Sections *2.4. Compliance* and *2.5. Incident Handling*).
7. Information security provision and the policies that guide it will be regularly reviewed, including through the use of annual internal audits and penetration testing.
8. Any explicit Information Security Management Systems (ISMSs) run within the company will be appraised and adjusted through the principles of continuous improvement, as laid out in ISO27001 clause 10.

2.2 Legal & Regulatory Obligations

IOCOM has a responsibility to abide by and adhere to all current UK and EU legislation as well as a variety of regulatory and contractual requirements.

A non-exhaustive summary of the legislation and regulatory and contractual obligations that contribute to the form and content of this policy is provided in *Appendix A*.

Related policies will detail other applicable legislative requirements or provide further detail on the obligations arising from the legislation summarized below.

2.3 Information Classification

The following table provides a summary of the information classification levels that have been adopted by IOCOM and which underpin the 8 principles of information security defined in this policy.

These classification levels explicitly incorporate the General Data Protection Regulation's definitions of *Personal Data* and *Special Categories of Personal Data*, as laid out in IOCOM's *Data Protection Policy*, and are designed to cover both primary and secondary research data.

Detailed information on defining information classification levels and providing appropriate levels of security and access is provided in the *Data Classification Standard*.

Information may change classification levels over its lifetime, or due to its volume – for instance:

- NHS patient data aggregated to a higher level (so that, for instance, there is one observation for each GP Practice, or Hospital) is considered Confidential if any observations created using 5 or fewer patient-level observations are present, but is *not* considered confidential if any such observations are either not present, or are dropped from the dataset.

Security Level	Definition	Examples	FOIA2000 status
1. Confidential	Normally accessible only to specified members of IOCOM staff. Should be held in an encrypted state outside IOCOM systems; may have encryption at rest requirements from providers.	GDPR-defined *Special Categories* of personal data (racial/ethnic origin, political opinion, religious beliefs, trade union membership, physical/mental health condition, sexual life, criminal record) including as used as part of primary or secondary research data; patient-level observations; aggregated patient data containing observations created using 5 or fewer patient-level observations; passwords; large aggregates of personally identifying data (>1000 records) including elements such as name, address, telephone number.	Subject to significant scrutiny in relation to appropriate exemptions/ public interest and legal considerations.
2. Restricted	Normally accessible only to specified members of IOCOM staff	GDPR-defined *Personal Data* (information that identifies living individuals including home / work address, age, telephone number, photographs); reserved committee business; draft reports, papers and minutes; systems.	Subject to significant scrutiny in relation to appropriate exemptions/ public interest and legal considerations.
3. Internal Use	Normally accessible only to members of IOCOM staf	Internal correspondence, final working group papers and minutes, committee papers, information held under license	Subject to scrutiny in relation to appropriate exemptions/ public interest and legal considerations

4. Public	Accessible to all members of the public	Annual accounts, minutes of statutory and other formal committees, pay scales etc. Information available on the IOCOM website or through the IOCOM's Publications Scheme.	Freely available on the website or through the IOCOM's Publication Scheme.

2.4 Suppliers

All IOCOM's suppliers will abide by IOCOM's Information Security Policy, or otherwise be able to demonstrate corporate security policies providing equivalent assurance.

This includes:

- when accessing or processing IOCOM assets, whether on site or remotely
- when subcontracting to other suppliers.

2.5 Cloud Providers

Under the GDPR, a breach of personal data can lead to a fine of up to 4% of global turnover. Where IOCOM user Cloud services, IOCOM retains responsibility as the data controller for any data it puts into the service, and can consequently be fined for any data breach, even if this is the fault of the Cloud service provider. IOCOM will also bear the responsibility for contacting Information Commissioner's Office concerning the breach, as well as any affected individual. It will also be exposed to any lawsuits for damages as a result of the breach. It is extremely important, as a consequence, that IOCOM is able to judge the appropriateness of a Cloud service provider's information security provision. This leads to the following stipulations:

1. All providers of Cloud services to IOCOM must respond to IOCOM's Cloud Assurance Questionnaire prior to a service being commissioned, in order for IOCOM to understand the provider's information security provision.

2. Cloud services used to process personal data will be expected to have ISO27001 certification, with adherence to the standard considered the best way of a supplier proving that it has met the GDPR principle of privacy by design, and that it has considered information security throughout its service model.
3. Any request for exceptions will be considered by the Risk Manager and the Chief Operating Officer.

2.6 Compliance, Policy Awareness and Disciplinary Procedures

Any security breach of IOCOM's information systems could lead to the possible loss of confidentiality, integrity and availability of personal or other confidential data stored on these information systems. The loss or breach of confidentiality of personal data is an infringement of the General Data Protection Regulation, contravenes IOCOM's Data Protection Policy, and may result in criminal or civil action against IOCOM.

The loss or breach of confidentiality of contractually assured information may result in the loss of business, financial penalties or criminal or civil action against IOCOM. Therefore it is crucial that all users of the company's information systems adhere to the Information Security Policy and its supporting policies as well as the Information Classification Standards.

All current staff and other authorized users will be informed of the existence of this policy and the availability of supporting policies, codes of practice and guidelines.

Any security breach will be handled in accordance with all relevant company policies, including the *Conditions of Use of IT Facilities at the IOCOM* and the appropriate disciplinary policies.

2.7 Incident Handling

If a member of staff is aware of an information security incident then they must report it to the Information Management and Technology Service Desk.

2.8 Supporting Policies, Codes of Practice, Procedures and Guidelines

Supporting policies have been developed to strengthen and reinforce this policy statement. These, along with associated codes of practice, procedures and guidelines are published together and are available on IOCOM's website.

All staff and any third parties authorized to access IOCOM's network or computing facilities are required to familiarize themselves with these supporting documents and to adhere to them in the working environment.

2.9 Review and Development

This policy, and its subsidiaries, shall be reviewed by the Information Security Advisory Board (ISAB) and updated regularly to ensure that they remain appropriate in the light of any relevant changes to the law, organizational policies or contractual obligations.

Additional regulations may be created to cover specific areas.

ISAB comprises representatives from all relevant parts of the organization. It shall oversee the creation of information security and subsidiary policies.

The Information Security Manager will determine the appropriate levels of security measures applied to all new information systems.

3 Responsibilities

Members of IOCOM:

All members of IOCOM, IOCOM associates, agency staff working for IOCOM, third parties and collaborators on IOCOM projects will be users of IOCOM information. This carries with it the responsibility to abide by this policy and its principles and relevant legislation, supporting policies, procedures and guidance. No individual should be able to access information to which they do not have a legitimate access right. Notwithstanding systems in place to prevent this, no individual should knowingly contravene this policy, nor allow others to do so. To report policy contraventions, please see *Section 2.5: Incident Handling*

Data Controllers:

Many members of IOCOM will have specific or overarching responsibilities for preserving the confidentiality, integrity and availability of information. These include:

Principal Investigators / Project administrators:

Responsible for the security of information produced, provided or held in the course of carrying out research, consultancy or knowledge transfer activities. This includes ensuring that data is appropriately stored, that the risks to data are appropriately understood and either mitigated or explicitly accepted, that the correct access rights have been put in place, with data only accessible to the right people, and ensuring there are appropriate backup, retention, disaster recovery and disposal mechanisms in place.

***Heads of Departments, Divisions, Centers*:**

Responsible for the information systems (e.g. HR/ Registry/ Finance) both manual and electronic that support IOCOM's work. Responsibilities as above (for *Principal Investigators / Project administrators*).

***Departmental managers / Line managers*:**

Responsible for specific area of IOCOM work, including all the supporting information and documentation that may include working documents/ contracts or staff information.

Head of Research Division

Signs off IOCOM research contracts and is responsible for providing the assurance that any mandated security measures for research data are met.

Records Manager / Data Protection Officer

Responsible for IOCOM's Data Protection Policy, data protection and records retention issues. Breach reporting to ICO.

Head of Security:

Responsible for physical aspects of security and will provide specialist advice throughout the IOCOM on physical security issues.

Information Security Team:

Responsible for this and subsequent information security policies and will provide specialist advice throughout the company on information security issues.

Information Security Advisory Board

Responsible for the advising on and recommending information security policies to the Information Technology Committee, assessing information security risks, identifying and implementing controls to risks.

Information Technology Committee

Responsible for approving information security policies.

4 Appendix A: Summary of relevant legislation

4.1 The Computer Misuse Act 1990

Defines offences in relation to the misuse of computers as:

1. Unauthorized access to computer material.
2. Unauthorized access with intent to commit or facilitate commission of further offences.
3. Unauthorized modification of computer material.

4.2 The Freedom of Information Act 2000

The Freedom of Information Act 2000 (FOIA2000) is a general right of public access to all types of recorded information held by public authorities in order to promote a culture of openness and accountability.

4.3 Regulation of Investigatory Powers Act 2000

The Regulation of Investigatory Powers Act 2000 regulates the powers of public bodies to carry out surveillance and investigation. It covers the interception and use of communications data and can be invoked in the cases of national security, and for the purposes of detecting crime, preventing disorder, public safety and protecting public health.

4.4 Defamation Act 1996

“Defamation is a false accusation of an offence or a malicious misrepresentation of someone's words or actions. The defamation laws exist to protect a person or an organization’s reputation from harm.”

4.5 Obscene Publications Act 1959 and 1964

The law makes it an offence to publish, whether for gain or not, any content whose effect will tend to "deprave and corrupt" those likely to read, see or hear the matter contained or embodied in it. This could include images of extreme sexual activity such as bestiality, necrophilia, rape or torture.

4.6 Protection of Children Act 1978, Criminal Justice Act 1988, Criminal Justice and Immigration Act 2008

The Protection of Children Act 1978 *prevents the exploitation of children by making indecent photographs of them and penalizes the distribution and showing of such indecent photographs.* Organizations must take appropriate steps to prevent such illegal activities by their workers using their digital systems and networks. The definition of 'photographs' include data stored on a computer disc or by other electronic means which is capable of conversion into an image.

It is an offence for a person to distribute or show such indecent photographs; or to possess such indecent photographs, with a view to their being distributed or shown by himself or others.

Section 160 of the Criminal Justice Act 1988 made the simple possession of indecent photographs of children an offence. Making an indecent image of a child is a serious arrestable offence carrying a maximum sentence of 10 years imprisonment. Note: The term "make" includes downloading images from the Internet and storing or printing them out.

4.7 Terrorism Act 2006

The Terrorism Act 2006 makes it an offence to write, publish or circulate any material that could be seen by any one or more of the persons to whom it has or may become available, as a direct or indirect encouragement or other inducement to the commission, preparation or instigation of acts of terrorism.

It also prohibits the writing, publication or circulation of information which is likely to be useful to any one or more persons in the commission or preparation of terrorist acts or is in a form or context in which it is likely to be understood by any one or more of those persons as being wholly or mainly for the purpose of being so useful.

In addition, it prohibits the glorification of the commission or preparation (whether in the past, in the future or generally) of terrorist acts or such offences; and the suggestion that what is being glorified is being glorified as conduct that should be emulated in existing circumstances.

4.8 Counter-Terrorism and Security Act 2015 – Statutory Guidance

The statutory guidance accompanying the Counter-Terrorism and Security Act 2015 (Prevent duty guidance for higher education institutions in England and Wales https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/445916/Prevent_Duty_ Guidance_For_Higher_Education__England__Wales_.pdf) requires IOCOM to have "due regard to the need to prevent people from being drawn into terrorism." The Act imposes certain duties under the *Prevent* programme, which is aimed at responding to "the ideological challenge we face from and aspects of extremism, and the threat we face from those who promote these views." The Prevent programme also aims to provide "practical help to prevent people from being drawn into terrorism and ensure they are given appropriate advice and support". IOCOM must balance its existing legal commitments to uphold freedom of speech within the law against the new Prevent duty, and seek to ensure that its IT facilities are not used to draw people into terrorism

4.9 General Data Protection Regulation

The GDPR will apply in the UK from 25 May 2018. The government has confirmed that the UK's decision to leave the EU will not affect implementation of the GDPR. The GDPR reinforces and extends data subjects' rights as laid out in the Data Protection Act (1998), and provides additional stipulations around accountability and governance, breach notification and transfer of data. It also extends the maximum penalties liable due to a data breach, from £500,000 to 4% global turnover.

The GDPR requires IOCOM to maintain an Information Asset Register, to ensure where personal data is voluntarily gathered people are required to explicitly opt in, and can also easily opt out. It requires data breaches to be reported to the Information Commissioner's Office within 72hrs of IOCOM becoming aware of their existence.