Information Security Roles and Responsibilities

Brunel University London

An ISO/IEC 27001:2013: *Aligned Document - Implementing Cyber and Information Security Best Practice*

Internal Use Only

Mick Jenkins
Chief Information Security Officer

Document History

Version	Author	Comments	Date
V 0.1	Andrew Clarke	Initial Draft	09/12/2016
V 0.2	Mick Jenkins	Re-Org Draft	09/08/2017
V1.0	Mick Jenkins	First release for approvals	11/10/2017
V1.1	Mick Jenkins	Approved Exec	26/01/2018

Document Approval

This document requires the approval from BUL as defined in the ISMS Compliance document.

MG Jenkins	
Document Owner: Michael Jenkins	Document Approver: Pekka Kahkipuro
Chief Information Security Officer	Chief Information Officer

Document Distribution

Name	Title	Version	Date of Issue
	All Directors for Cascade		
	DCO's / DRO		
	COO		
	CIO		
	CFO		
	University secretary		

Contents

1. Purpose of Document

The purpose of this document is to define roles and responsibilities that are essential to the implementation of the University's Information Security Management System (ISMS) and Information Security (INFOSEC) Policy.

Please refer to Brunel University London ISMS Document BUL-GLOS-000 - SyOPs Glossary of Terms for the glossary of terms, acronyms and their definitions for the suite of Brunel University (BUL) London ISMS documentations.

The University's **Information Security Policy** states that:

> "*Brunel University London will maintain an Information Security Management System (ISMS) to preserve its competitive edge, educational excellence, cash-flow, data protection, customer confidence and reputational image.*
>
> *Brunel University will ensure that the individuals, roles, bodies and governing frameworks are in place to maintain security ownership and responsibilities*."

This document formally establishes these governing bodies and roles and responsibilities for the University Information Security management and the ISMS framework. An organisational schematic is at Annex A.

2. ISO 27001 - Conformance

This section indicates the University Conformance to ISO27001:2013.

University ISMS Control Number	SOA – Number A.6 – Organisation of Information Security
ISO 27001:2013 Conformance Control	Information Classification Objective A.6.1.1 Information Security Roles and Responsibilities

3. Principles

From ISO 27001 & ISO 27014[1], the principles of information security governance are to:

- Establish an organisational wide information security policy.
- Adopt a risk based approach.
- Set the direction of investment for INFOSEC.
- Ensure conformance with security requirements.
- Foster a security-positive environment.
- Review performance in relation to business outcomes.

[1] Information Security Governance

- The organisation should define accountabilities and responsibilities at a high level, making top management explicitly accountable for information security but ensuring that personal roles and responsibilities are also defined.

Within BUL, information security governance has been approached holistically and covers people, processes and technology – it is not an IT issue. The security controls that form part of the ISMS take account of human, environmental and physical factors and cover information in all its forms including paper records. The BUL information security governance framework encompasses policies, processes, procedures, tools and training that are all joined up and designed in relation to each other in order to achieve BUL information security objectives.

4. Committees and Governance

Council

Council has ultimate accountability for information security activities within the University. More specifically, it protects institutional reputation by being assured that clear regulations, policies and procedures that adhere to legislative and regulatory requirements are in place, ethical in nature, and followed. Council needs to be assured that there are effective systems of control and risk management, and that governance structures and processes are fit for purpose by referencing them against recognised standards of good practice.

Executive Board

The University Executive Board is responsible via the Vice-Chancellor to Council for:

- Leading and fostering a culture that values, protects and uses information for the success of the University and benefit of its members.
- Defining the University's information security risk appetite in the context of the prevailing legal, political, socio-economic and technological environment and external standards.
- Ensuring that a fit for purpose and adequately resourced information security framework is in place including this policy document as a reference document.

The Executive Board is ultimately accountable for information security governance and INFOSEC risk as a whole. The management and control of information security risks is an integral part of Executive Board governance. The Executive Board provides overall strategic direction by approving and mandating the information security principles and axioms but delegates operational responsibilities for physical and information security to the COO, CIO and CISO.

The Executive Board is responsible for achieving the Cyber & INFOSEC vision set out in the Strategy paper[2] and ensuring the appropriate levels of investment are made to meet the desired goals of the Cyber & INFOSEC Strategy.

Infrastructure Strategy Committee

The Infrastructure Strategy Committee (ISC) is a forum for operational and executive consideration of University-wide digital and information services strategy. This and its information subcommittee have specific oversight responsibilities related to implementation of the Information Security Policy and ISMS security controls including the following:

- Approving and reviewing the Cyber & INFOSEC strategy to ensure the implementation of the Information Security Policy and associated ISMS.
- Analysing the business impact of proposed Cyber & INFOSEC strategies on the University.
- Approving proposed policies of the ISMS.
- Serving as the executive champion for accepted strategies and policies within respective business units and colleges.

Cyber and Information Security and Applications Steering Group (CISA)

The Cyber, Information Security and Applications Steering Group purpose is to drive the programme of Cyber & INFOSEC strategic projects forward and deliver the capability development outcomes and benefits as set out in the Cyber & INFOSEC strategy paper. It has the following responsibilities:

- Confirming the scope and mandate for each cyber security project.
- Recommending investment decisions for Cyber & INFOSEC capability development.
- Providing visible leadership and commitment, championing and supporting the programmes of cyber security development.
- Promoting awareness of security initiatives within colleges and business units.
- Considering security risks, ideas, policies and procedures and how they may impact the organisation.
- Ensuring that cyber and information security is considered and built into systems and applications development life cycles.

5. Roles and Responsibilities

Chief Information Officer (CIO) & SIRO

[2] A 5 year University Strategy published in June 2017 – see cyber 365 webpages https://intra.brunel.ac.uk/s/cc/security/Pages/default.aspx

The CIO undertakes the role of Senior Information Risk Owner (SIRO) for the organisation. The role of the SIRO is to take ownership of the organisation's information risk, act as an advocate for information risk on the Executive Board, and provide advice to the board and Council on the Information risk governance and risk exposure. The SIRO's responsibilities can be summarised as:

- Leading and fostering a culture that values, protects and uses information for the success of the organisation and benefit of its clients and stakeholders.
- Owning the organisation's overall information risk policy and risk assessment processes ensuring they are implemented consistently.
- Advising the VC & COO or relevant accounting officer on the information risk aspects of internal controls.

Information Asset Owners

Information Asset Owners (IAOs) are Directors and Heads of Departments held accountable for the protection of particular Information Assets[3]. IAOs may delegate information security tasks to managers or other individuals but remain accountable for the proper implementation of the tasks. IAOs are responsible for:

- Ensuring compliance with BUL ISMS policies and all regulatory requirements as they relate to the information assets.
- The appropriate classification and protection of the information assets.
- Ensuring all staff managing information assets are appropriately trained in INFOSEC.
- Determining appropriate criteria for obtaining access to information assets[4].
- Authorising access to information assets in accordance with the classification and business need.
- Undertaking or commissioning information security risk assessments to ensure that the information security requirements are properly defined and documented.
- Monitoring compliance with protection requirements affecting their assets.

A number of senior staff will have de facto responsibility for the information assets under their control. For example, the HR Director will have responsibility for all the personnel information held within the organisation and will, in part, be responsible for determining how it is used, accessed and stored. The responsibility may be implicit, for example the post holder will be the senior business owner of processes relating to the given asset. Alternatively, it may be explicitly outlined, for example in the terms and conditions associated with research grant awards and information management.

Secretary to Council and University Secretary

[3] The named asset owners are aligned to the ISMS information asset registers that have been completed within BUL.
[4] A Data Owner is accountable for who has access to information assets within their functional areas

The Secretary to Council and University Secretary is a legal and governance role responsible for reporting issues of concern to Council and the Executive and:

- Oversee reviews of legal effectiveness of policy and contractual documents used as information security safeguards and controls.

- Provide legal information and counsel to executive officers and council related to information security breaches, incidents and risk management.

Chief Information Security Officer (CISO)

The Chief Information Security Officer is a security leadership role with a core responsibility to drive and deliver the University's Cyber & Information Security Strategy and implement the Information Security Management System (ISMS). Responsibilities are summarised as:

- Developing and implementing a University-wide cyber and information security programme.
- Documenting and disseminating information security policies and procedures.
- Coordinating the development and implementation of a University-wide information security training and awareness programme.
- Coordinating a response to actual or suspected breaches in the confidentiality, integrity or availability of University Data.
- Supporting and advising information asset owners on security matters and information security risk.

Data Protection Officer (DPO)

The Data Protection Officer (DPO) is a leadership role required by the General Data Protection Regulations (GDPR)[5]. The Data Protection Officer is responsible for overseeing the data protection strategy and its implementation to ensure compliance with GDPR. As outlined in the GDPR Article 39, the DPO's responsibilities include, but are not limited to, the following:

- Educating the University and employees on important compliance requirements.
- Training staff involved in data processing.
- Conducting audits to ensure compliance and address potential issues proactively.
- Serving as the point of contact between the university and GDPR Supervisory Authorities.
- Monitoring performance and providing advice on the impact of data protection efforts.
- Maintaining comprehensive records of all data processing activities conducted by the University, including the purpose of all processing activities, which must be made public on request.

[5] GDPR legislation comes into force in May 18

Cyber & Information Security Manager

The Cyber & Information Security Manager is an operational role responsible for day to day cyber and information security incident reporting, investigations, due diligence and intelligence collection. The role includes but is not restricted to:

- The project management and delivery of the University Cyber and Information Security 'action plan'.
- Delivery of projects associated with the strategic aim of achieving Cyber Essentials accreditation and alignment to ISO 27001 controls.
- Leading on cyber and information security audits, testing, and documenting vulnerability assessments alongside the technical IT teams.
- Cyber security advice and support to all areas of the University and its business units.
- Delivery of training and awareness packages to improve end user awareness and protection.

Cyber Officer

This position is responsible for operational coordination of cyber security intelligence collection, security incident responses, and technical protections aligned to ISO 27001 and Cyber security best practice. The cyber officer, reporting to the Cyber & INFOSEC manager has the following high level roles:

- Ensure the development and promotion of a positive Cyber and Information Security culture that incorporates an increased awareness of security threats, vulnerabilities and cyber-crime prevention measures.
- Advise clients (either verbally or in writing) on various aspects of Cyber security, ICT technical controls, risk, threats, cyber intelligence and compliance.
- Delivery of policy, process and procedures to support the 20 Cyber controls and sub controls within the ICT arena.
- The delivery of Cyber Security audits and reviews in alignment with the Cyber & INFOSEC Manager leading the strategic programme and action plan.
- Coordinate investigation and responses to external and internal IT security threats or compromises.
- Consult with University departments on maintenance of Disaster Recovery Plans and align them with the risk management strategy.

Head of Security & Emergency Planning

The Head of Security & Emergency planning is responsible for the University incident management plan (IMP) and providing guidance on the physical and procedural security for securing information assets. The role works closely with the CISO and cyber security team to ensure criminal acts are correctly reported and investigated. The core responsibilities for INFOSEC are:

- Conducting joint criminal investigations with the support of the campus police officer.
- Reporting crime to the relevant fraud or cyber-crime departments.
- Maintaining an incident and cyber-criminal database to generate reports.
- Conducting ISMS audits aligned to physical and procedural controls for information assets alongside the Cyber officer.

Head of IT Infrastructure and Operations & Head of Development and Application Services

These roles lead and champion the requirements for embedding cyber and information security good practice within the centralised IT teams. Both roles within the ISMS act as Data Custodians[6] and are responsible for:

- Implementing appropriate physical and technical controls[7], to protect the confidentiality, integrity and availability of University data.
- Applying the 5 cyber security controls specified by the Cyber Essentials scheme[8].
- Understanding and reporting on security risks and how they impact the confidentiality, integrity and availability of University Data.
- Ensuring the relevant ISMS patching and configuration policy is adopted within the centralised IT teams and reported on regularly to provide risk exposure status.
- Ensuring comprehensive disaster recovery architecture is maintained and operations are in place for such.
- Investigating and resolving information security incidents in conjunction with the Cyber & INFOSEC Manager and CISO.
- Supporting appropriately authorised forensic investigations overseen by Governance, Information, & Legal Services, the CIO or CISO.
- Ensuring compliance with required RPOs and RTOs during business continuity events.
- Motivating, organising, mentoring, and directing department managers and staff regarding the security of information assets and cyber risks.
- The corrective action plans and remediation activity from internal and external audits, and other observed vulnerabilities.

College and Department IT officers

College and department IT officers, responsible for specific business unit IT systems, also act within the ISMS as Data Custodians. They are responsible for:

[6] Data Custodians are IT services and / or locally appointed persons responsible for the technical environments. This may also be a person who has technical control over an information asset dataset with administrator level of access.
[7] Aligned to the Statement of Applicability and the development of ISMS technical controls
[8] Aligned to the Statement of Applicability and the development of ISMS technical controls

- Applying appropriate physical and technical safeguards to protect the confidentiality, integrity, and availability of information asset datasets.
- Leading and championing the requirements for embedding cyber and information security good practice within College and departmental teams.
- Applying IT technical controls within the ISMS policies and controls.
- Implementing the 5 cyber security controls specified by the Cyber Essentials Scheme.
- Understanding and reporting on security risks and how they impact the confidentiality, integrity and availability of University Data.
- Ensuring the relevant ISMS patching and configuration policy is adopted within the business unit.

University Department Heads and Managers

Heads of Departments and Managers are responsible for:

- Day-to-day conformance with the University information security policies and college policy.
- Ensuring that security controls are in place in accordance with information security policy and in particular, they should take measures to ensure that staff:

    - Are informed of their information security obligations in adherence to relevant policy by means of appropriate awareness, training and education activities.
    - Comply with the information security policies and undertake good information security practice.
    - Providing the direction, support, and management necessary to ensure that information assets are appropriately protected within their area of responsibility.

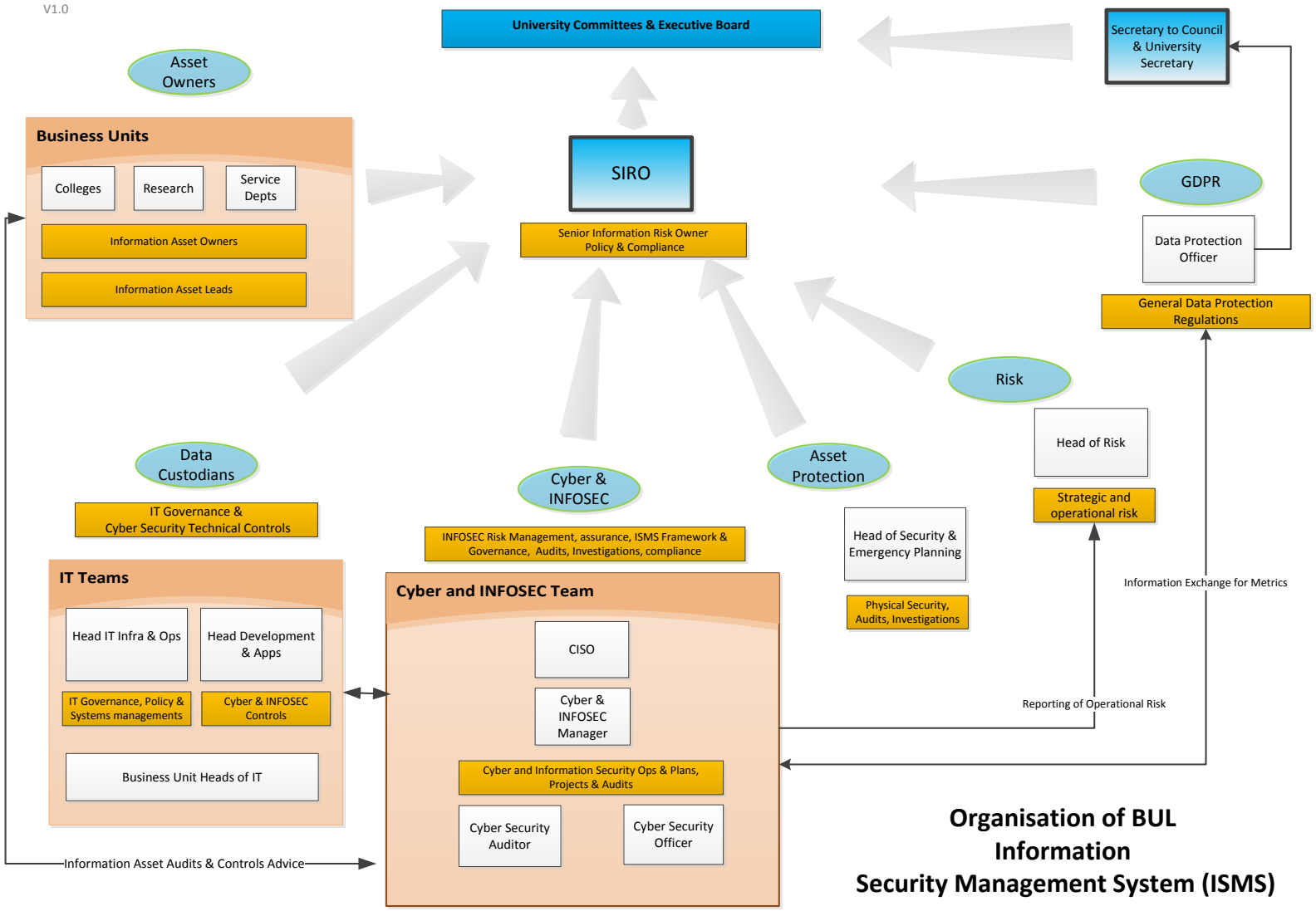
All Users

All individual users of University information systems and those handling or having access to University information outside of those systems shall be responsible for:

- Complying with all relevant information security, policies, practices and procedures including any external accountability.
- Ensuring that they undertake, or request where necessary, relevant information security awareness training to enable them to undertake their roles.
- Reporting information security incidents via the defined and approved channels.
- Ensuring that the University Data Protection Officer is informed of all potential breaches of privacy laws in accordance with the Data Protection Policy.

-End-

Annex A


V1.0
University Committees & Executive Board
Secretary to Council & University Secretary
Asset Owners
Business Units
Colleges
Research
Service Depts
Information Asset Owners
Information Asset Leads
SIRO
Senior Information Risk Owner
Policy & Compliance
GDPR
Data Protection Officer
General Data Protection Regulations
Risk
Head of Risk
Strategic and operational risk
Data Custodians
IT Governance & Cyber Security Technical Controls
Cyber & INFOSEC
INFOSEC Risk Management, assurance, ISMS Framework & Governance, Audits, Investigations, compliance
Asset Protection
Head of Security & Emergency Planning
Physical Security, Audits, Investigations
IT Teams
Head IT Infra & Ops
Head Development & Apps
IT Governance, Policy & Systems managements
Cyber & INFOSEC Controls
Business Unit Heads of IT
Cyber and INFOSEC Team
CISO
Cyber & INFOSEC Manager
Cyber and Information Security Ops & Plans, Projects & Audits
Cyber Security Auditor
Cyber Security Officer
Information Exchange for Metrics
Reporting of Operational Risk
Information Asset Audits & Controls Advice
Organisation of BUL Information Security Management System (ISMS)

Annex B

Data Owner and Custodian Roles

A Data Owner has administrative control and has been officially designated as accountable for a specific information asset dataset. This is usually the most senior officer in a Directorate or College division. Some examples of Data Owners include the Registrar and student data; The CFO for financial data; & the HR Director for employee data. Within colleges this role will fall to the Director of College Operations or the Institute Director of Operations for research. In most cases, the Data Custodian is not the Data Owner.

Data Custodians are IT services and / or locally appointed persons responsible for the technical environments. A system administrator or Data Custodian is a person who has technical control over an information asset dataset. Usually, this person has the administrator or root account or equivalent level of access. This is a critical role and it must be executed in accordance with the access guidelines developed by the Data Owner.

Data Users also have a critical role to protect and maintain BUL information systems and data. For the purpose of information security, a Data User is any employee, contractor or third-party provider who is authorised by the Data Owner to access information assets.

General Responsibilities of the Data Owner

1. Ensure compliance with BUL policies and all regulatory requirements as they relate to the information asset.

2. Assign an appropriate classification to information assets. BUL has three classifications of information assets:

- University Confidential
- Protect
- Unclassified

3. Determine appropriate criteria for obtaining access to information assets. A Data Owner is accountable for who has access to information assets within their functional areas. A Data Owner may decide to review and authorised each access request individually or may define a set of rules that determine who is eligible for access based on business function, support role, etc. Access must be granted based on the principles of least privilege as well as separation of duties.

4. Bi-annually, the Data Owner is also responsible for reviewing who has been given access to ensure accuracy. University audits of information assets will take place annually as part of the ISMS.

5. Ensuring that Data Custodians implement reasonable and appropriate security controls to protect the confidentiality, integrity and availability of University Data.

BUL has published guidance on implementing reasonable and appropriate security controls based on three classifications of data: Unclassified, Protect and University Confidential. See the BUL-POL-8.2 Information Classification for more information. Data owners will often have their own security requirements specified in contractual language and/or based on various industry standards. Data owners should be familiar with their own unique requirements and ensure Data Custodians are also aware of and can demonstrate compliance with these requirements. The Cyber and Information Security Manager can assist with mapping controls identified in the BUL-PROC-8.02 Information Classification to controls mandated by contract(s) or industry standards.

General Responsibilities of the Data Custodian

1. Assign and remove access to others based upon the direction of the Data Owner.
Assigning access to the information asset dataset so others can perform their respective job functions is an important and necessary part of the Data Custodian's job.

2. Produce reports or derivative information for others. In many cases the Data Custodian is also responsible for producing, interpreting, and distributing information based on the datasets to which he or she has access.

3. Log all information provided and access granted to others. A log of all information that is disseminated must be kept including the dataset used, the receiving party, and the date. Likewise, access granted to others must be logged including the access level granted and the dataset in question.

4. Implement appropriate physical and technical safeguards to protect the confidentiality, integrity, and availability of the information asset dataset. Data Custodians are expected to work with Data Owners to gain a better understanding of these requirements. Security controls must be documented and shared with the Data Owner.