BRUNEL UNIVERSITY

INFORMATION SECURITY GOVERNANCE

INFORMATION ASSET OWNERS HANDBOOK

Information Security

Information Asset Owners (IAO) Handbook

A university-wide information management and security policy

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	Michael Jenkins	Initial Draft	09/08/2018
V 0.2	Michael Jenkins	Amended text and copy-edit by ML	18/02/2019
V 1.0	Michael Jenkins	Approved Document	

Document Approval

The contents of this document are confidential to Brunel University London (BUL). Proprietary information presented in this document may not be used without written consent from BUL and remains the exclusive property of BUL unless otherwise agreed to in writing.

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

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

Document Distribution

Name	Title	Version	Date of Issue
	All IAO's and IAC's		
	DCO's / DRO		
	COO		
	CIO / SIRO		
	CFO		
	DPO		

Handbook Contents

PART 1 – BACKGROUND AND GOVERNANCE

1. Introduction

The *Information Asset Owner* (IAO) is a university mandated role, aligned to the Information Security Management System. Individuals are appointed as IAO and are responsible for ensuring that information assets are handled and managed appropriately. This means making sure that information assets are properly protected and that their value to the organisation is fully exploited.

An Information Asset Owner reports to the Senior Information Risk Owner (SIRO)[1], who in turn reports to the Executive Board.

The role is a standard requirement of an ISO 27001 *Information Security Management System* (ISMS) and supports the provision of a common, consistent and unambiguous understanding of what information is held, how important it is, how sensitive it is, the risk to it, and who is responsible for it.

2. Purpose of the Handbook

This handbook sets out the university’s approach to managing and securing its information and data assets. It explains the concept of an ‘*Information Asset’* and defines the role of the ‘*Information Asset Owner*’ who is responsible for each Information Asset. This handbook also acts as a specific guide for the IAO and sets out the primary responsibilities of an IAO for the risk and operational management of information assets including personal data and business critical information held within a college or directorate.

The handbook also explains how IAOs will report on metrics to the SIRO throughout the reporting cycle.

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*.”

[1] Chief Information Officer

A guiding principle of our Strategy document is that '*All information and systems will have identified owners*.' This document formally establishes the roles and responsibilities for IAOs within the University Information Security Management System framework.

3. 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.6.1.2 Information Security Roles and Responsibilities

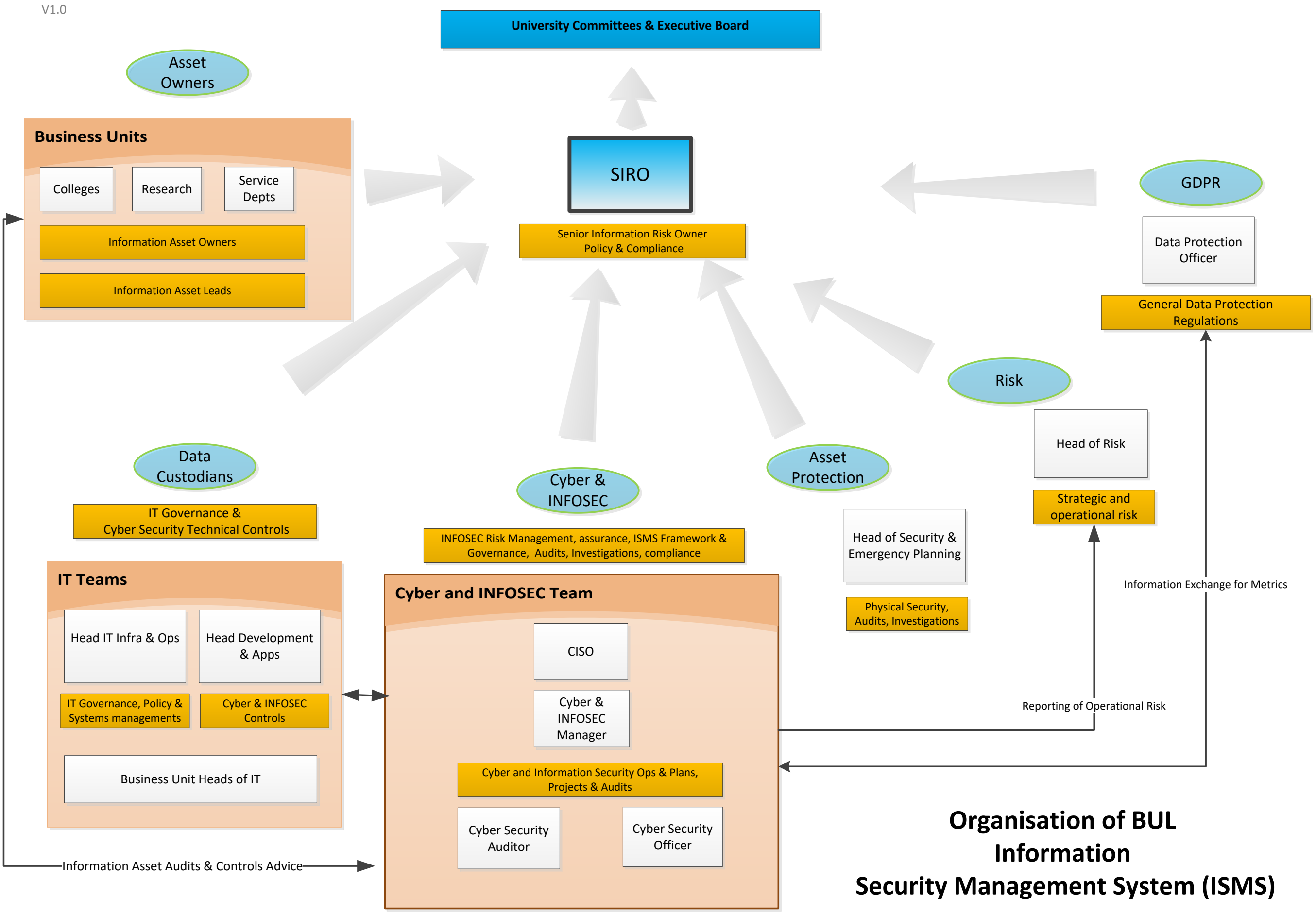
4. Background

The university holds a wealth of information. This information can be in different formats and held in a variety of locations and systems. It is essential that the university understands the information it holds so that we can adequately manage and protect it.

To manage this information, the university needs to have Information Asset Registers (IAR) which are managed by Information Asset Owners. Information Asset Owners are senior members of staff who have been appointed to be responsible for one or more identified information asset(s). This person will be responsible for ensuring that the Information Asset is accurately stored and maintained on the Information Asset Register. The full university Information Asset Register will be owned by the office of the Chief Information Officer (CIO).

Performing the role well brings significant benefits. It provides a common, consistent and unambiguous understanding of what information the university holds, how important it is, how sensitive it is, how accurate it is, how reliant the university is on it, and who is responsible for it.

The organisation of BUL Information Assurance is shown below:


V1.0
University Committees & Executive Board
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
Information Exchange for Metrics
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
Reporting of Operational Risk
Information Asset Audits & Controls Advice

Organisation of BUL Information Security Management System (ISMS)

5. Principles

The IAO role is about managing information not systems.

The driver for establishing the role of the IAO within the ISMS is to ensure that information assets, whether personal data or business data, are identified and securely handled. This also involves making sure that they are used in the way that is required, for as long as required.

The IAO is responsible for ensuring that information is protected appropriately, and where the information is shared, that proper *confidentiality, integrity and availability* safeguards apply and are in place.

The IAO role is about providing information assurance and making sure that action is taken to secure information assets, their movement and sharing is appropriately managed, and that contracts are in place where they are shared with 3rd parties.

An IAO can delegate responsibility to particular areas that can support the role but the IAO and SIRO retain the accountability for proper information management and handling.

6. Asset Management

An *information asset* is a body of information, defined and managed as a single unit, so that it can be understood, shared, protected and exploited effectively. Information assets have recognisable and manageable value, risk, content and lifecycles. They include physical and digital assets and are recorded in an information asset register – held centrally within the ISMS and locally within colleges and directorates.

The university SIRO will decide what information assets IAO's are responsible for. This could cover both sensitive personal data and non-personal information that is critical to business. It could be held in paper as well as electronic formats.

When an IAO is appointed, performance metrics will be discussed and agreed. Some of these will be directly related to the need to demonstrate compliance with mandatory requirements, but others may be specific to colleges or directorates.

7. Information Asset Register

An Information Asset Register (IAR) is a mechanism for understanding and managing the university's assets and the risks to them. The IAR should include links between the information assets, their business requirements or processes and any technical dependencies that there may be. An IAR is dynamic and should be consistently updated and improved to ensure each business unit develops a 'mature' understanding of the information that it holds.

The Cyber & INFOSEC teams have developed a standardised asset register but general information on the types of assets and how to develop the registers can be seen at Annex A.

–End Part 1-

PART 2 – IAO HANDBOOK AND ROLES

8. Roles and Responsibilities

Senior Information Risk Owner (SIRO)

The Senior Information Risk Owner is a Chief Officer with allocated lead responsibility for the organisation's information risks and provides the focus for management of information. The SIRO provides the Executive Board with assurance that information risk is being managed appropriately and effectively across the organisation and for any services contracted by the organisation.

Information Asset Owners (IAO)

The SIRO is supported by the BUL IAOs. The role of IAO is to understand what information is held, what is added and what is removed, who has access and why in their own area. As a result they are able to identify and address risks to the information assets they 'own' and to provide assurance to the SIRO on the security and use of the assets. The organisation has allocated this role to Directors and Senior Departmental Heads and/or Managers for each college, institute or directorate.

The CIO undertakes the role of Senior Information Risk Owner (SIRO) for BUL. 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 and 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 responsible for the protection of particular Information Assets[2]. IAOs may delegate information security tasks to managers or other individuals but remain accountable for the proper implementation of the tasks.

[2] The named asset owners are aligned to the ISMS information asset registers that have been completed within BUL.

The IAO is expected to understand the overall business goals of the university and how the information assets they own contribute to and affect these goals. The IAO should nominate at least one Information Lead to support the IAO on a day-to-date basis.

IAOs are responsible for:

- Leading and fostering a culture that values, protects and uses information for the good of the university.
- Knowing what information the asset holds, and what information is transferred in or out of it and what systems it links to.
- Knowing who has access and why, and ensuring that their use is monitored.
- Understanding and addressing risks to the asset, providing assurance to the SIRO and ensuring that any data loss incidents are reported and managed following BUL guidelines.
- 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 managing, securing and accessing the assets.
- Determining appropriate criteria for obtaining access to information assets[3].
- 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.
- Ensuring that contractual agreements exist for the transfer to, or processing by, any third party.

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.

An IAO will be required to consider the following questions:

- Do I understand what information assets I am responsible for (including personal and non-personal data) and has that understanding been properly documented within the Information Asset Register (IAR) and shared with the SIRO and others who need that information?
- Have I assessed and logged information risks to those assets?
- Do I have a plan for managing risks, and validating that security controls are in place?

[3] An IAO is accountable for who has access to information assets both internally and externally.

- Do my team(s) and third parties understand their roles and responsibilities in managing those risks and controls?

The SIRO, CISO, Cyber & INFOSEC team and Data Protection Officer are all organisational leads able to provide guidance support and advice in the management of information assets.

9. Risks to be Managed

An Information Asset Owner shall need to assure against:

- Inappropriate access to, or disclosure of, protectively marked or sensitive personal data by staff, contractors and outsiders, whether accidental or deliberate

- Inappropriate data sharing where too much or irrelevant data is shared internally, i.e. a full list with all personal data is provided where only numbers of a specific category have been requested.

- Information loss, particularly during transfer or movement of information, or as a result of business or regulatory change

- Loss of ready access to information

- Records management – that information assets are not retained for longer than required (either by law or for business need) as outlined in the corporate retention and disposal schedule.

- Business continuity/disaster recovery – that the relevant personnel are aware of the agreed continuity and recovery for their services.

- Loss of digital continuity – i.e. losing the ability to use information in the way required when required. By use we mean being able to find, open, work with, understand and trust your information. The lifecycle of a piece of information – and how long you need to use and keep it – is often different to the lifecycle of the IT system that we have to access and use it

10. Information Asset Administrators (IAA)

An Information asset administrator (IAA) should understand the overall business goals of the organisation and the importance of the information assets in supporting these goals. Information asset administrators should understand the IAOs responsibilities and lead in ensuring the methods outlined in Annex A are fully exploited to support delivery.

IAA’s will be expected to:

- Review the IAR on a six-monthly basis and ensure that the IAR is maintained and updated when new assets are created.
- Ensure that retention periods for information are documented in the retention schedule. Arrange for documented audits to ensure that information is deleted in accordance with retention periods.
- Ensure that decisions are clearly recorded against any information that is retained longer than its agreed retention period.
- Ensure that managers understand the importance of maintaining correct access controls of drives and systems.
- Carry out regular audits of systems and drives to ensure correct access controls are maintained.
- Ensure that local information handling guidelines are in place where required and that these refer to corporate guidance where appropriate.
- Provide assurance to the IAO on a regular basis.
- Attend training as required.

-End Part 2-

PART 3 – REPORTING TO SIRO

11. Annual Reporting

IAOs will be required to provide bi-annual assurance on the following areas to the SIRO. **This report will be presented to Executive Board and can be seen at Annex B.** It will include reporting that:

- Local procedures governing the use of data are in place and updated when required.
- Access control measures are in place for systems, which includes how access is granted and removed for users.
- Updates on data flows (links to other systems) and reasons are provided.
- Action following security incidents are monitored and updated.
- Any records management responsibilities are captured (for example, the retention schedule is reviewed annually and that any system(s) used to store information have been reviewed to ensure retention is reflected.)
- Contracts with data processers have the agreed information security and GDPR clauses and compliance with these are monitored. [4]
- Appropriate Information Sharing Agreements are in place and reviewed where required.
- Actions identified during audits are captured in the IAR where required.

12. Guidance and Training

All IAOs and Information Asset Administrators will receive the relevant baseline and on the job training to be able to undertake the roles and responsibilities. A specific IAO guidance shall be available to support the day-to-day management and security of the information assets under ownership.

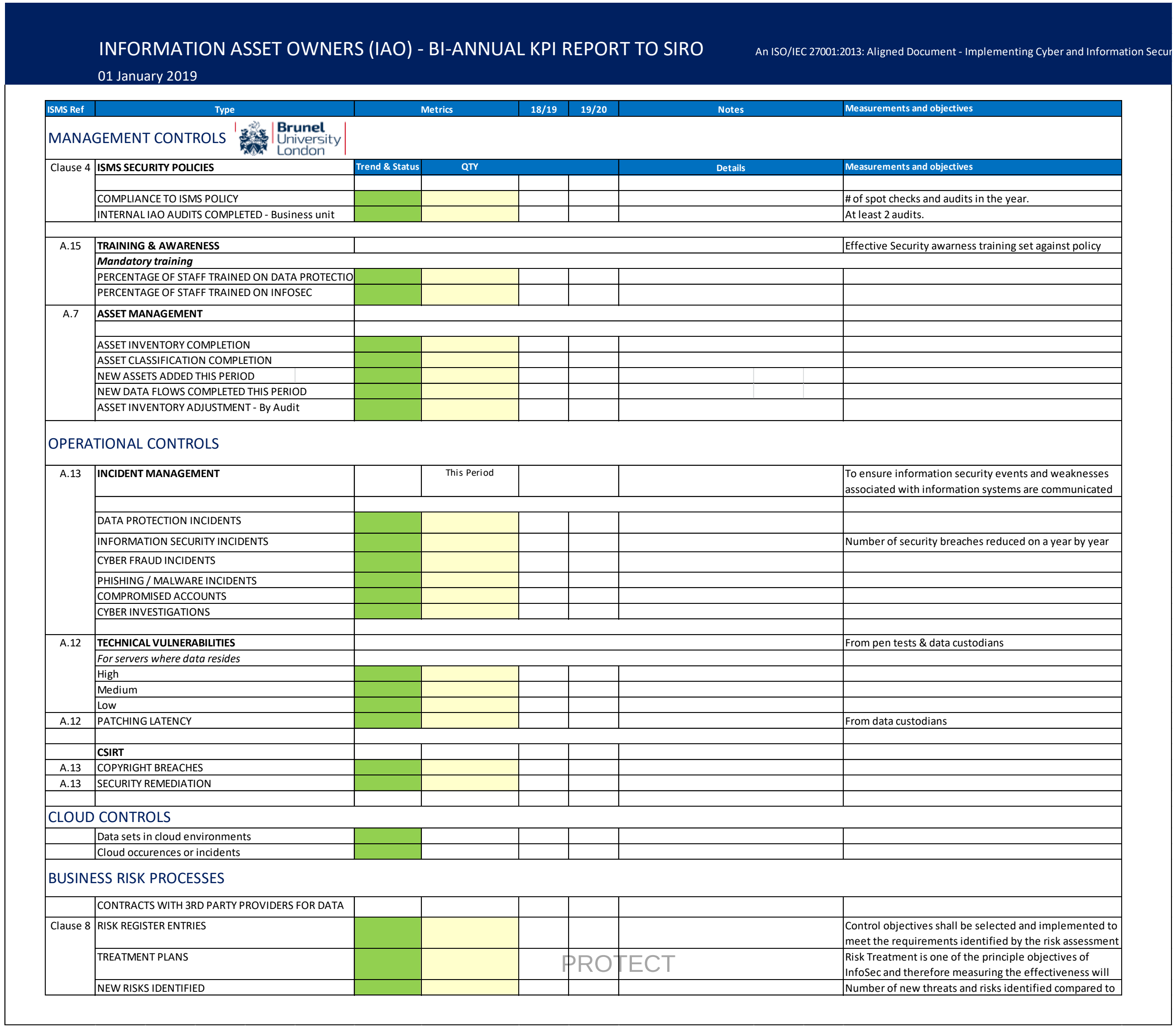
13. Governance, Approval and Review

This policy and the university's commitment to a robust information assurance framework are subject to continuous, systematic review and improvement. This university-wide policy operates as part of the ISMS and shall be governed by the Information subcommittee.

-End

[4] Clauses will be developed and agreed by the DPO. Additionally the DPO is the person who will draft and review any data-sharing agreements.

Appendix 1 Bi-Annual Reporting Template



INFORMATION ASSET OWNERS (IAO) - BI-ANNUAL KPI REPORT TO SIRO

An ISO/IEC 27001:2013: Aligned Document - Implementing Cyber and Information Secur

01 January 2019

ISMS Ref	Type	Metrics		18/19	19/20	Notes	Measurements and objectives
MANAGEMENT CONTROLS							
Clause 4	**ISMS SECURITY POLICIES**	Trend & Status	QTY			Details	Measurements and objectives
	COMPLIANCE TO ISMS POLICY						# of spot checks and audits in the year.
	INTERNAL IAO AUDITS COMPLETED - Business unit						At least 2 audits.
A.15	**TRAINING & AWARENESS**						Effective Security awarness training set against policy
	Mandatory training						
	PERCENTAGE OF STAFF TRAINED ON DATA PROTECTIO						
	PERCENTAGE OF STAFF TRAINED ON INFOSEC						
A.7	**ASSET MANAGEMENT**						
	ASSET INVENTORY COMPLETION						
	ASSET CLASSIFICATION COMPLETION						
	NEW ASSETS ADDED THIS PERIOD						
	NEW DATA FLOWS COMPLETED THIS PERIOD						
	ASSET INVENTORY ADJUSTMENT - By Audit						
OPERATIONAL CONTROLS							
A.13	**INCIDENT MANAGEMENT**		This Period				To ensure information security events and weaknesses associated with information systems are communicated
	DATA PROTECTION INCIDENTS						
	INFORMATION SECURITY INCIDENTS						Number of security breaches reduced on a year by year
	CYBER FRAUD INCIDENTS						
	PHISHING / MALWARE INCIDENTS						
	COMPROMISED ACCOUNTS						
	CYBER INVESTIGATIONS						
A.12	**TECHNICAL VULNERABILITIES**						From pen tests & data custodians
	For servers where data resides						
	High						
	Medium						
	Low						
A.12	PATCHING LATENCY						From data custodians
	CSIRT						
A.13	COPYRIGHT BREACHES						
A.13	SECURITY REMEDIATION						
CLOUD CONTROLS							
	Data sets in cloud environments						
	Cloud occurences or incidents						
BUSINESS RISK PROCESSES							
	CONTRACTS WITH 3RD PARTY PROVIDERS FOR DATA						
Clause 8	RISK REGISTER ENTRIES						Control objectives shall be selected and implemented to meet the requirements identified by the risk assessment
	TREATMENT PLANS						Risk Treatment is one of the principle objectives of InfoSec and therefore measuring the effectiveness will
	NEW RISKS IDENTIFIED						Number of new threats and risks identified compared to

Appendix 2

List of IAOs and IAC's

Directorate, College, Dept	Information Asset Owner	IS Information Asset Custodian Customer Relationship Managers
PILOT BUSINESS UNITS (2019)		
GLASS – Business Support and SITS	JILLY COURT	SENANI THOTABADUGE
CHLS – CLINICAL SCIENCES	MIKE KEIGHLEY	ALAN CHARIE
COMMERCIAL SERVICES	PETER BENT	ALAN CHARIE
HUMAN RESOURCES	GEMMA BAILEY	ALAN CHARIE
FINANCE	JAMES HOBSON	ALAN CHARIE
NEW 2020 BUSINESS UNITS		
STRATEGIC PLANNING	ROSA SCOBLE	SENANI THOTABADUGE OR ALAN CHARIE (As appropriate)
INFORMATION SERVICES	IAIN LIDDELL	SENANI THOTABADUGE OR ALAN CHARIE (As appropriate)
ESTATES	AKINTOYE OLUWATUDIMU	SENANI THOTABADUGE OR ALAN CHARIE (As appropriate)
CEDPS	PAUL WORTHINGTON	SENANI THOTABADUGE OR ALAN CHARIE (As appropriate)
STUDENT SERVICES	JILLY COURT	SENANI THOTABADUGE OR ALAN CHARIE (As appropriate)
RSDO	THERESA WALLER	SENANI THOTABADUGE OR ALAN CHARIE (As appropriate)
REGISTRY & LEGAL	JILLY COURT	SENANI THOTABADUGE OR ALAN CHARIE (As appropriate)
PROCUREMENT	IAIN WILCOCKS	SENANI THOTABADUGE OR ALAN CHARIE (As appropriate)

Appendix 3

IAO Works Programmes

Annual Tasks

Task	Start Date	Finish Date	Action
2018/19			
Information Asset Register Record of Processing Activity (ROPA)			To be submitted as part of the Information assurance evidence.
Data Flow Mapping Exercise			To be submitted as part of the Information assurance evidence.
Annual INFOSEC & Data Protection training			All staff to complete mandatory training
Confidentiality and Safe Haven Audit			To be submitted as part of the Information assurance evidence. Practice should be on-going
INFOSEC Spot Check and Record Keeping Audit			To be submitted as part of the Information assurance evidence. Practice should be on-going
Implement Local Induction for New Staff	On-going as and when new starters arrive.		
Reporting Incidents and Breaches.	On-going as required. Report to INFOSEC & DP team as and when events occur.		
Responding to Subject Access Requests.	On-going as required to support the data protection officer.		
Information Sharing Protocols & contracts	On-going. Ensure IAOs & Project Leads are aware of the Information Sharing requirements & contracts clauses required to protect data and consult with the DPO		
Privacy Impact Assessments	On-going. Ensure IAOs & Project Leads are aware of the DPIA template and consult with the data protection officer in relation to new or existing projects.		

FAQs

Information Assets and Information Asset Register (IAR)

Subject Heading	Definition and Actions needed to complete the audit process
What is an Information Asset Register (IAR) and why is it completed??	Keeping an information asset register will enable you to understand what information assets are held and how they support operations within your team.
	It will help you undertake the 'data mapping' task, as well as, prevent loss of information and data breaches. It will also help colleagues locate information for Freedom of Information requests in a timely manner. All information assets will be 'owned' by your team's IAO.
Why is an audit of the assets undertaken?	IAOs are required to identify and record information assets within the information asset register template provided. This practice is used to: • ensure that the information assets within BUL are managed effectively • Identify potential issues • protect and keep the asset secure.

Data Flow Mapping Exercise (DFM)

Subject Heading	Definition and Actions needed to complete the audit process
Why do we complete the Data Flow mapping process?	It is a legal requirement under the Data Protection Act 2018, that organisations must ensure that measures are embedded to avoid unauthorised and unlawful or accidental: • access • transfer • processing of • loss and destruction of • damage to personal data, including special category personal data
How does the DFM exercise produce the outcomes to inform the risks?	All questions on the template will need to be answered for each data flow process
	Once completed any information flows rated as 'red' or 'amber' risk will be reviewed by the IAO with support from the DP & INFOSEC Team or followed up via the BUL INFOSEC risk management process.

What information is included in this process?	• Identifies all transfers of information and also enables the DPO to identify potential issues which may require further assessment. • Will determine where, why, how and with whom the organisation exchanges information. • Record inbound and outbound information flows within the data flow mapping register:

Reporting Incidents & Breaches

Subject Heading	Definition and Actions needed to complete the process
Who should be notified of any data incidents or breaches?	The DPO and INFOSEC team should be notified, as they will then inform the SIRO
What type of incident should be reported?	Incidents that relate to loss or compromise of data, Cyber and Data Protection Act breaches.
How do I get further information?	For further guidance on reporting INFOSEC and DP incidents please refer to the cyber 365 intranet and data protection pages.
How do I encourage colleagues to report incidents?	Provide them with sufficient information to understand how reporting incidents will improve working practices, protect BUL IP and special category data, and reduce complaints.

Information Sharing Protocols/Agreements

Subject Heading	Definition and Actions needed to complete the process
What are information sharing protocols/agreements?	It is important to ensure that there is a balance between sharing information with other organisations for the purposes of operational and strategic business and keeping information secure and confidential. The organisation needs to ensure that mechanisms are in place to enable reliable and secure exchange of data within the constraints of the law, relevant guidance and service specific requirements.

Why does the organisation need to use them?	BUL uses information sharing protocols to put in place an agreement between parties to document: • The purpose for sharing the information • Who the information will be shared with • Structures for sharing information • Legislation and regulations which must be adhered to • Conditions of processing our data and INFOSEC standards required
How will this area of work help me with my IAO role?	From the work undertaken for the Information Asset register and the Data Flow Mapping exercise, IAOs should ensure that information sharing protocols are in place for outbound information flows. IAO's are also required to carry out assessments on the information flows between the organisation and its partners, and as a result complete and embed a local Information Sharing Service Agreement. The DPO & INFOSEC teams will support and advise on these processes.
Where can I obtain the protocol/agreement templates?	Information Sharing protocols and data processing templates and guidance are available from the DPO and CISO teams. The information sharing agreements once completed will need to be signed off by the DPO, SIRO and Legal teams

Data Protection Impact Assessments (DPIA's)

Subject Heading	Definition and Actions needed to complete the process
What is a Data Protection Impact Assessment (DPIA)?	A DPIA is a document that identifies the risk elements of a project and/or process. Guidance for the Introduction of New Processes for DPIAs can be found on the DPO intranet page. It is used for all new projects and changes to existing ones to assess the risk to personal data.

Why is a DPIA required?	IAOs are pivotal to the roll out of the BUL Information Assurance agenda and ensuring partner organisations handle information in a secure and appropriate manner. As part of this framework, we ask to support and encourage colleagues to consider risk implications to personal data when starting new projects and programmes, and effecting changes to existing systems and processes. This is now a legal requirement under DP Act 2018 and the GDPR. Ensure that you involve the DPO team during the project/programme initiation stage.
What are the benefits of identifying and introducing a DPIA	Identifying risk to personal data at an early stage will ensure; • compliant operations • necessary information sharing protocols in place • the organisation is aware of and can effectively monitor data and its processing • they are added to the Information Asset register • that System Level Security Polices are initiated where appropriate
	It will also ensure BUL is compliant with the Data Protection Act 2018 and mitigate subsequent fines from the Information Commissioner's Office.
What is the process for DPIA approval?	Once the DPIA has been completed, the document is forwarded to the DPO for approval and recommendations.
Where can I obtain the DPIA template?	The DPIA screening questionnaire can be obtained from the CISO and DPO.

Key Definitions

Subject	**Supporting information**
Controller	the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data
Processor	a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller
Data Subject	the identified or identifiable living individual to whom personal data relates
Personal data	any information relating to an identified or identifiable living individual

Special Category personal data (For this type of information even more stringent measures should be employed to ensure the data remains secure)	Personal data that contains details of the person's: • racial or ethnic origin • political opinions • religious or philosophical beliefs • trade union membership • genetic data • biometric data • health data • sex life or sexual orientation • Criminal convictions.
Processing (in relation to personal data)	Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as: • collection • recording • organization • structuring • storage • adaptation or alteration • retrieval • consultation • use • disclosure by transmission ,dissemination or otherwise making available • alignment or combination • restriction • erasure • destruction

Appendix 4

Identifying an IAO

An IAO must have the power to make decisions about how Information Assets are managed. Therefore, this role must be held by a senior member of staff.   These posts will typically be assigned to Directors or Heads of Department.

The post holder must have the skills, resources and authority to discharge the responsibilities and take action on any deficiencies in the relevant processes.

All IAOs must attend IAO training provided by the university which will include onsite sessions in the initial creation phase, followed by specific cyber security and data protection training sessions. IAOs must attend subsequent training where it is identified.

Identifying Information Assets

Assessing every individual file, database entry or piece of information isn't realistic - therefore the university and its departments needs to group information into manageable portions, and classify the data according to its value and sensitivity.

To assess whether something is an information asset, ask the following questions:

Value: Does the information have a value to the organisation? How useful is it? Will it cost money to reacquire? Would there be legal, reputational or financial repercussions if you couldn't produce it on request? Would it adversely impact operational efficiency if you could not access it easily? Would there be consequences of not having it?

Risk: Is there a risk associated with the information? Is there a risk of losing it? A risk that it is not accurate? A risk that someone may try to tamper with it? A risk arising from inappropriate disclosure?

Retention: Does the group of information have a manageable lifecycle? Were all the components created for a common purpose? Will they be disposed of in the same way and according to the same rules?