**Document Control**
Reference: BUL-POL-8.1
Issue No: 2
Issue Date: 26/04/18
Page: 1 of 12

# Information Security Asset Owners Policy

## 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 | 09/10/2017 |
| V 1.0 | Michael Jenkins | Approved Exec | 26/04/2018 |
| | | | |

## 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 | |
| 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. 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 Document

This document 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 document also sets out the primary responsibilities of an Information Asset Owner for managing the risks to personal data and business critical information held within a department.

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*."

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 IAO 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<br>SOA – Number A.8 – Asset Management |

[1] Chief Information Officer

| | |
|---|---|
| ISO 27001:2013<br>Conformance Control | Information Classification Objective<br>A.6.1.1 Information Security Roles and Responsibilities<br>A 8.1 Asset Management |

## 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 CIO office.

The IAO will provide assurance to the Senior Information Risk Owner (SIRO) on the security and use of their assets. They are responsible for ensuring that specific information assets are accessed, handled and managed appropriately. This means making sure that information assets are properly protected and that their value to the organisation is fully exploited.

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.

## 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 it is 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, its movement and sharing is appropriately managed, and that contracts are in place where it is 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.

## 8. Roles and Responsibilities

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 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.

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 university good.
- Knowing what information the asset holds, and what information is transferred in or out of it and what systems it links to.
- Know who has access and why, and ensure that their use is monitored.
- Understanding and addressing risks to the asset, provide assurance to the SIRO and ensure 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.

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

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

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?

- 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 – 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.

- Internal threat – staff acting in error or deliberately, or external parties getting your information illegally and exposing it/acting maliciously to defraud.

- 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

- Poor quality of information and poor quality assurance, for example, of datasets

- Poor change management – business needs change, systems change, your information risk appetite may change, so you need to keep your policies and processes in step accordingly

## 10. Information Leads

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

Information Leads 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 over 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 and that these refer to corporate guidance where appropriate.
- Provide assurance to the IAO on a regular basis.
- Attend training as required.

## 11. Annual Reporting

IAOs will be required to provide annual assurance on the following areas to the SIRO. This report will be presented to Executive Board.

- That local procedures governing the use of data are in place and updated when required.

- That access control measures are in place for systems, which includes how access is granted and removed for users.
- That updates on data flows (links to other systems) and reasons are provided.
- That action following security incidents are monitored and updated.
- That 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.
- That appropriate Information Sharing Agreements are in place and reviewed where required.
- That actions identified during audits are captured in the IAR where required.

## 12. Guidance and Training

All IAO's and Information leads 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-

## Annex A

## Identifying an IAO

An IAO must have the power to make decisions about how Information Assets are managed. Therefore this role must be 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 GDPR 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 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?