Brunel University London

BRUNEL UNIVERSITY

INFORMATION ASSURANCE GOVERNANCE

INFORMATION ASSET OWNERS TASK LIST

Information Assurance

Information Asset Owners (IAO)

Task List – FOR PILOT

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

1. Introduction

This document sets out the TASK LIST for *Information Asset Owners* (IAO's). This is a suggested list of formal actions that should be completed by you and your staff as part of assessing the 'assurance' levels of your data.

The list is set out in chronological order with the annual list shown as an appendix. For any questions related to this list and the way to complete them, contact the CISO.

2. Task List

Task list for the BUL IAO Framework in 2020:

Task	Finish Date	Action
Update and complete your business unit **Information Asset Register**	End of May	To be submitted as part of the Information assurance submission to SIRO[1] and CISO in September.
Identify and document in the asset register where the data is held – which system or which server	End of July	Liaise with Heads of IT dept to identify data locations. Which system or server.
Provide a list of staff members who have completed the mandatory INFOSEC and Data Protection Training Encourage staff to complete it by early Sept	End of Aug	Liaise with professional development for lists of completion. Report as percentages of staff who have completed the training.
Provide a formal RFI[2] to the Head of IT dept on **security patching records** for the servers where your data is stored.	End of July	See separate RFI form to issue to the IT dept.
Provide a formal RFI to the Head of IT dept on **technical vulnerabilities** for the servers your data is held on.	End of July	See separate RFI form to issue to the IT dept.
Provide a formal RFI to the Data Protection Officer for known and reported data breaches for your business unit.	End of June	See separate RFI form to issue to the DPO.
Issue awareness training posters and aide memoires to all your staff. (provided)	End of Aug	Suggest posters are issued as a rolling plan and aide memoires issued once to all staff. Signpost staff to the cyber 365 intranet page.
Identify on the asset register where your data is shared with external 3rd parties. Confirm if a contract is in place with the 3rd party	End of Aug	CISO will check contracts for data protection & INFOSEC clauses.

[1] Senior Information Risk Owner
[2] Request for Information

Complete spot checks on staff to ensure: • all information is marked with a classification • Clear desk policy is adopted. • Data assets are adequately stored and secured	End of Aug	Spot checks via dept heads or team leaders.
For highly sensitive and university confidential data, conduct a detailed check of staff who have access to that data.	By end June	Check with IT who have the access rights and amend accordingly to who should have access to that data. Report any changes made in the report below.
Submit the Information Assurance report and KPI form to CISO & SIRO by end of Oct 2020.	End Oct	CISO will provide the report and KPI form – submission is to include all the evidence above incl asset registers etc.
Establish a formal process within the Directorate/College for reporting INFOSEC & DP incidents to the IAO.	End of Aug	Incidents to be reported include: Data Protection incidents (also reported directly to DPO) Information Security incidents (loss of non-personal data etc) Staff members who have become a victim of phishing, cyber-fraud, or cyber-crime. (all work related)

The IAO Ethos and Aims

- To promote a culture within your business unit that values, protects and manages information responsibly for the good & benefit of the university.
- Encourage and promote good practice for data protection & INFOSEC amongst your staff and departments.
- Ensure that lessons are learnt should things go wrong.
- Establish ways for individuals to feel confident in reporting information risks to senior management and then demonstrate that action is taken in response.
- The effective handling of data to guard against data loss.

-end-

Appendix 1

IAO Annual Works Programmes

Annual Tasks

Task	Start Date	Finish Date	Action
2020/21			
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		
Data Protection 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.		