IS Joiners and Leavers 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	Andrew Clarke	First Draft	06/08/2018
V 0.2	Andrew Clarke	CISO - define roles requiring further background checks to include DBS standard and Enhanced. Termination to remove access to be completed within 5 working days.	07/08/2018
V 1.0	Andrew Clarke	Approval HR	09/11/2018
V 1.1	Andrew Clarke	Annual Review – replace COO with CGO	15/06/2020

Document Approval

The contents of this document are classified as Protect to Brunel University London (BUL) information classification. 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.

Owner: Michael Jenkins	Chief Information Security Officer
Signature: MGJ	Date: 09 Nov 2018
Approver: Pekka Kahkipuro	Chief Information Officer
Signature: PK	Date: 09 Nov 2018
Distribution:	

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

Contents

1. About this document 4
1.1 Purpose 4
1.2 Responsibilities 4
1.3 ISO27001 Conformance 4
1.4 Scope 4
1.4 References 4
2.0 IS Joiners and Leavers Policy 5
3.0 Prior to Employment 6
4.0 During Employment 8
5.0 Termination of Employment 10
6.0 Change of Employment (Movers) 11
APPENDIX A - Background checks 12

1. About this document

1.1 Purpose of Document

This Policy establishes the area within Brunel University London covering employee joiners and leavers IS and Cyber requirements.

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

1.2 Responsibilities

Table 1 – responsibilities

Title / Role	Description
Cyber and Information Security Manager	• To ensure this policy is maintained and kept up to date; • To implement and ensure that all staff receive the necessary Security Awareness training.
Training and Recruitment Manager	• Responsible for providing the information required under this procedure; • To implement and ensure University Human Resources adhere to this policy.

1.3 ISO 27001 - Conformance

This section indicates the University Conformance to ISO27001:2013.

University ISMS Control Number	SOA – Number A.7 – Human Resources Security
ISO 27001:2013 Conformance Control	Information backup A.7.1 Prior to Employment A.7.2 During Employment A.7.3 Termination and change of Employment

1.4 Scope

This policy applies to the employment of all University employees, including temporary staff and contractors with access to University information and information systems.

The HR department is responsible for ensuring that this policy is implemented.

1.5 References

HR For Managers Policies

2.0 IS Joiners and Leavers Policy

2.1 Policy Summary

All University Staff, including temporary staff and contractors, will have appropriate verification checks conducted prior to the commencement of employment with the University. In addition, staff will be made aware of their security roles and responsibilities and ISMS information asset role and responsibilities through appropriate security awareness training and the publication of job descriptions and terms and conditions of employment.

Upon termination of employment with the University, all property and access rights to information and information systems will be promptly revoked.

2.2 Review & Evaluation

The owner of this policy is responsible for the implementation, maintenance and review of the policy, with the support of Human Resources Managers, in line with the following guidelines:

- Significant changes to University.
- Security incidents or regulatory changes.
- A yearly review should be undertaken to:
  - Assess the effectiveness of the policy;
  - Effects of changes to technology.
- Changes to this policy shall be approved by the ISC Meeting and communicated to all HR staff.

3 Prior to Employment

In order to prevent the misuse of University information and information systems, the University ensures that appropriate controls are in place to prevent potential misuse and to ensure personnel are suitable for the roles they are being considered for.

3.1 Roles and Responsibilities

All University personnel, including temporary and contract staff, will have documented information security roles and responsibilities defined.

3.2 Screening

Prior to employment within University, all potential employees will have background verification checks conducted (BPSS or DBS Basic minimum) . The results of these checks must be received prior to the candidate gaining access to University information and information systems.

In addition to normal background checks, the following roles require greater checks (see Appendix A):

- CGO (DBS Enhanced)
- CFO (DBS Enhanced)
- CIO (DBS Standard)
- CISO (DBS Enhanced)
- Head of Security (DBS Enhanced)
- Security ops manager (DBS Standard)
- Cyber & INFOSEC manager (DBS Standard)
- Cyber officer (DBS Standard)
- DPO (DBS Standard)
- Deputy DPO (DBS Standard)
- Senior HR posts (DBS Enhanced)
- IS Staff (Systems, networks, Development) (DBS Standard)
- Student Services (Counsellors) (DBS Enhanced)

3.3 Contract Staff

Confirmation of identity and qualifications of temporary / contract staff is the responsibility of the supplying agency, in addition the supplying agency is responsible for ensuring that all temporary / contract staff sign a confidentiality agreement that protects the confidentially of University information.

The University reserves the right to request that agencies provide the appropriate evidence to show that the activities have been undertaken and also occasionally audit agencies to verify that adequate checks are taking place.

3.4 3rd Party Contract Staff

Confirmation of identity and qualifications of any permanent, temporary or contract staff, when requiring access to University buildings, systems and information, is the responsibility of all third parties organisations.

University reserves the right to requests that 3rd parties provide the appropriate evidence to show that the activities have been undertaken and also occasionally audit 3rd parties to verify that adequate checks are taking place.

3.5 Terms & Conditions of Employment

All new employees are required to agree and sign the terms and conditions of their employment with the University.

4 During Employment

All staff employed within the University are expected to ensure that information security is applied throughout the organisation in accordance with published policies and procedures.

4.1 Induction

All staff employed by University are expected to complete the University induction process and the mandatory Data Protection and Cyber Awareness Security training modules.

All new staff are expected to attend at the first opportunity, the New Starters Security Awareness Presentation Seminar as soon as possible after commencing work at the University.

4.1.1 Checklist

Prior to an employee gaining access to the University network and data, it is necessary for the employee Line Manager to have completed and returned to HR the contract and employment fitness questionnaire and the New Staff Starter Form to detail what IT equipment and access is required to fulfill the role. This must then be distributed to the appropriate departments to action the requests and sign.

4.2 Management Responsibilities

Management are responsible for ensuring staff are made aware of and are adopting and implementing published policies and procedures and for ensuring a level of cyber and Information Security awareness throughout University.

4.3 Security Education, Awareness and Training

All University employees, including contactors and temporary staff, must complete the mandatory information security training on the Staff Development portal commensurate with the role being performed.

A formal information security induction programme sets out the University expectations prior to gaining access to University information and information systems.

Records are maintained by the Cyber & Information Security Manager of all staff having completed the induction training and the online Cyber Awareness training.

The University also considers on-going training to staff within the University and for ad-hoc training on a request basis.

4.4 Disciplinary Process

A formal disciplinary process has been established for misconduct by employees who are in breach of the information security policies and/or procedures. This process ensures correct and fair treatment for employees suspected of committing any breaches of security.

5 Termination and Change of Employment

The HR department is responsible for ensuring that a documented, coordinated termination process exists and incorporates the following:

5.1 Termination Responsibilities

HR is responsible for the implementation of the termination process within the University within 5 working days. In addition, HR will manage changes of employment.

Prior to an employee leaving, HR ensures that employees are notified in writing that they are still bound by the duty of confidentially and the preservation of intellectual property rights to University.

In the case of contract staff, termination responsibility may be undertaken by the appropriate agency.

5.2 Return of Assets

HR in conjunction with the employee line manager must ensure that all University property is returned prior to the termination of employment.
The EmployeeJoinerLeaver registry should be signed by the appropriate departments to corroborate the IT equipment returned and that access has been terminated.

5.3 Removal of Access

On resignation of employment HR will, in conjunction with the employee line managers undertake a risk assessment and determine whether existing access rights of an individual should be reviewed and reduced whilst working out their notice.

Upon date of termination, HR will advise IS and Operations within 5 working days for the removal of access.

6 Change of Employment (Movers)

The HR department is responsible for ensuring that a documented, coordinated moving/role-change process exists and incorporates the following:

5.1 Change Responsibilities

HR is responsible for the implementation of the changes of employment (move role) process within the University within 5 working days.

In the case of contract staff, responsibility may be undertaken by the appropriate agency.

5.2 Change of IS access permissions

HR will ensure that IS are advised of the change of employment and the requisite changes (both additional and removal) to access that is required within 5 days.

APPENDIX A: Background checks

i) DBS Check/Employment Background Check

A Disclosure and Barring Service check (or DBS check for short) is the term used for the analysis and record of a person's past, looking specifically at any convictions, cautions, reprimands and warnings they may have received.

DBS checks, also known as disclosures, may also include soft intelligence held by the police. This information is not always contained within the Police National Computer (PNC). For example, a person may not have been convicted of a particular offence, but a local police force may have intelligence which should be disclosed as it may affect the suitability of a person for a particular job.

There is no difference between a CRB and DBS check.

There are three levels of disclosure DBS check. The level required will depend on the job and the duties in question. These levels of disclosure are:

1. Basic level disclosure – this is a non-specific check that is available to anyone who requires certification, and is available to anyone, for any purpose. It is commonly used for personal licence holders, couriers or similar. A basic disclosure details only unspent criminal convictions; cautions, warnings, reprimands and convictions held on the Police National Computer.

2. Standard level disclosure (subject to eligibility in accordance with legislative criteria with the exception of the DBS filtering rule[1])– this more in-depth check is often required for careers such as accountants. A Standard disclosure details all spent and unspent criminal convictions; cautions, warnings, reprimands and convictions held on the Police National Computer.

3. Enhanced level disclosure (subject to eligibility in accordance with legislative criteria with the exception of the DBS filtering rule)) - Individuals who wish to work with vulnerable people will require this disclosure. An Enhanced Disclosure (like the Standard Disclosure) details all criminal history; cautions, warnings, reprimands and convictions held on the Police National Computer. Additionally, checks against the DBS Children and Adult barred list (where appropriate) and information provided by local police forces. This type of disclosure can only be

[1] On the 29th May 2013 legislation came into force that removed certain old and minor conviction information, from the Exceptions Order of the Rehabilitation of Offenders Act. In practical terms this means that not all conviction information will be displayed on a Standard or Enhanced DBS Disclosure. These rules are described as the DBS Filtering Rules.
Those 18 years old or over at the time of offence - **Convictions** will be removed if:

- 11 years have passed since the date of the conviction; AND
- it is the individual's only offence, AND
- it did not result in a custodial sentence
- **Cautions** will be removed after 6 years

Those under the age of 18 at the time of offence - **Convictions** will be removed if:

- Same rules apply as above however the elapsed time is reduced to 5.5 years
- **Cautions** will be removed
- Same rules apply as above however the elapsed time is reduced to 2 years.

Information never Filtered from a Certificate - The DBS Filtering Rules stipulated that the following information MUST be included on the following, and so will never by Filtered from a Certificate:

- Cautions relating to an offence from a list agreed by Parliament
- Convictions relating to an offence from a prescribed list (see DBS website for list)
- Where the individual has more than one conviction, all convictions will be included.
- Convictions that resulted in a custodial sentence

applied for by an organisation against the adult and children's barred list too, depending on the role of an individual or the job for which they are applying.

ii) Baseline Personnel Security Standard (BPSS) – is not a security clearance but the minimum background screening check used for positions that would be working with or for Government Departments.
A BPSS check consists of verification made up of the following four parts (known as RICE):

• Right to work — Nationality and Immigration Status (including an entitlement to undertake the work in question)

• Identity — ID data check (electronic identity authentication – name, address, aliases, links, accounts etc.)

• Criminal records — Search for unspent convictions only (Basic Disclosure) , though is slightly more expansive.

• Employment history check — Confirmation of past three years employment (minimum) history/activity