A.7.0 Human Resource Security
Document Information

<table>
<thead>
<tr>
<th>Reference</th>
<th>ISMS 27001</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category</td>
<td>Information Security Management System (ISMS)</td>
</tr>
<tr>
<td>Title</td>
<td>A.7.0 Human Resource Security</td>
</tr>
<tr>
<td>Purpose</td>
<td>Staff and researcher HR processes</td>
</tr>
<tr>
<td>Owner</td>
<td>Information Governance Management Group (IGMG)</td>
</tr>
<tr>
<td>Author</td>
<td>Charles Hindmarsh</td>
</tr>
<tr>
<td>Compliance</td>
<td>ISO 27001</td>
</tr>
<tr>
<td>Review plan</td>
<td>Annually</td>
</tr>
</tbody>
</table>

Related Documents

- University of Leeds Information Protection Policy
- ISMS Mandatory Clauses
- A.5.0 Information security policies
- A.6.0 Organisation of information security
- A.8.0 Asset management
- A.9.0 Access control
- A.10.0 Cryptography Controls
- A.11.0 Physical and environmental security
- A.12.0 Operations security
- A.13.0 Communications security
- A.14.0 Systems acquisition, development and maintenance
- A.15.0 Supplier Relationships
- A.16.0 Information security incident management
- A.17.0 Information security aspects of business continuity management
- A.18.0 Compliance

Version History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Update by</th>
<th>Change description</th>
<th>Approved By</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>27/06/2016</td>
<td>Samantha Crossfield/</td>
<td>Initial version</td>
<td>Barry Haynes (Chair of IGMG)</td>
<td>20/10/2016</td>
</tr>
<tr>
<td></td>
<td></td>
<td>David Batty</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.0</td>
<td>12/10/2018</td>
<td>Charles Hindmarsh</td>
<td>New format of ISMS</td>
<td>Andy Pellow (Chair of IGMG)</td>
<td>22/03/2019</td>
</tr>
<tr>
<td>2.1</td>
<td>20/09/2019</td>
<td>Charles Hindmarsh</td>
<td>Update to A.7.2.1</td>
<td>Andy Pellow (Chair of IGMG)</td>
<td>25/09/2019</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Contents
Introduction .................................................................................................................................. 3
Purpose ......................................................................................................................................... 3
Applicability .................................................................................................................................. 3
A.7.1 Prior to Employment ........................................................................................................ 3
  A.7.1.1 Screening ....................................................................................................................... 3
  A.7.1.2 Terms & Conditions ....................................................................................................... 3
    A.7.1.2.1 IRC Terms and Conditions ....................................................................................... 3
A.7.2 During Employment/Engagement ..................................................................................... 3
  A.7.2.1 Management Responsibilities ....................................................................................... 3
  A.7.2.2 Information Security Awareness, Education and Training ........................................... 3
    A.7.2.2.1 Standard Training ....................................................................................................... 4
    A.7.2.2.2 Further Training ......................................................................................................... 4
    A.7.2.2.3 Training Review ......................................................................................................... 4
    A.7.2.2.4 IRC Staff .................................................................................................................... 5
  A.7.2.3 Disciplinary Process ...................................................................................................... 5
A.7.3 Termination & Change of Employment ............................................................................. 5
  A.7.3.1 Termination or Change of Employment Responsibilities ............................................... 5
Introduction
The Integrated Research Campus (IRC) is a University of Leeds (UoL) IT service. It provides secure technical infrastructure and services for research data handling, analytics, application processing and development.

Purpose
This document provides an overview of the Human Resources policies that are in place. It also provide the policy for the tasks DST will perform and maintain.

Applicability
This policy applies to everyone who requires access to use IRC services.

A.7.1 Prior to Employment

A.7.1.1 Screening
Staff screening processes are outside of the scope of the ISMS and are managed by HR. These can be found at http://hr.leeds.ac.uk/policies.

Registration of Post Graduate Researchers are outside of the scope of the ISMS and managed by the Student Education Service. Their policies are found at: https://ses.leeds.ac.uk/info/22108/registration_enrolment_and_attendance/787/registration

A.7.1.2 Terms & Conditions
Employment Terms and conditions are set and managed by Human Resources including policies on fraud, bribery and whistle-blowing.

A.7.1.2.1 IRC Terms and Conditions
In signing the IRC User Agreement, users agree to the terms of use for using the IRC services set out in the agreement and within the ISMS. The signed agreements will be kept by DST.

A.7.2 During Employment/Engagement

A.7.2.1 Management Responsibilities
Managers with responsibility for staff will have their responsibilities defined as part of their job description. They must ensure that their staff complete the UoL Human Resources induction process, ensure their information security training is current and monitor and review other tasks necessary for the role.

A.7.2.2 Information Security Awareness, Education and Training
The Information Security Awareness, Education and Training policy sets the procedure for training all IRC users and staff. This includes recording and monitoring
participation and competence in training, and communicating the implications of non-conformance.

The purpose of the information security training is to develop a culture of best practice in information governance that contributes to the successful delivery of the ISMS. Training has been designed to ensure that training addresses the ISMS objectives with consistency.

The training procedure applies to all IRC users. Everyone has a responsibility for being appropriately competent in IG.

The Data Services Team (DST) ensures there is access to ISMS policies and procedures via the intranet, to supplement training and ongoing understanding.

Managers or Principal Researchers with responsibility for team members must ensure that all necessary training is completed and maintained.

A.7.2.2.1 Standard Training
As IRC systems hold data that has been classified as ‘IRC-Confidential’ or ‘IRC-Secure’ (see A.8.2 Information Classification), all IRC users must undertake University of Leeds Information Security Essentials Training annually and Information Security Advanced Training every three years to ensure they have understanding of data protection, data management, information security, confidentiality and Freedom of Information Act. Evidence of taking training must be provided to and recorded by DST before an IRC user account is created. As per University Information Protection Policy, an IRC account will be disabled if training is not maintained.

A.7.2.2.2 Further Training
Additional researcher training may be required by some dataset providers to uphold IG good practices or because of ethical-legal or contractual reasons. Where this is required, the Principal Investigator must ensure DST are aware of the requirement as the project is developed. Evidence of completing the course must be provided to and recorded by DST.

A.7.2.2.3 Training Review
The Information Governance Management Group (IGMG) maintain and oversee the IRC Information security awareness, education and training policy.

The DST will maintain IRC user training records on SharePoint and will inform users if their training records are no longer compliant with the ISMS requirements. Failure to present evidence of training to a manager, auditor or the DST will result in loss of access.
A.7.2.2.4 IRC Staff
Staff are also responsible for updating their training record as per HR policy.

A.7.2.3 Disciplinary Process
Disciplinary processes are managed by HR. Their policies are located here:

- [http://hr.leeds.ac.uk/info/26/conduct_capability_and_grievance/236/support_staff_procedure_agreement](http://hr.leeds.ac.uk/info/26/conduct_capability_and_grievance/236/support_staff_procedure_agreement)
- [http://hr.leeds.ac.uk/info/26/conduct_capability_and_grievance/237/statutes](http://hr.leeds.ac.uk/info/26/conduct_capability_and_grievance/237/statutes)

Users who do not comply with IRC policies will have their user account disabled.

A.7.3 Termination & Change of Employment

A.7.3.1 Termination or Change of Employment Responsibilities
Responsibilities for information security remain valid following change of employment which is set out in the [University's policies, procedures and codes of practice](http://hr.leeds.ac.uk/info/26/conduct_capability_and_grievance/236/support_staff_procedure_agreement) and communicated through a University contract.

Update to an employee status will be made on the central HR system and will trigger a notification to IT to remove network access to IT University Systems.