A.14.0 System Acquisition, Development & Maintenance
### 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) Documents</td>
</tr>
<tr>
<td>Title</td>
<td>System Acquisition, Development &amp; Maintenance</td>
</tr>
<tr>
<td>Purpose</td>
<td>Defining who is responsible for system acquisition &amp; maintenance</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>
<tr>
<td>Related Documents</td>
<td><strong>University of Leeds Information Protection Policy</strong></td>
</tr>
<tr>
<td></td>
<td>ISMS Mandatory Clauses</td>
</tr>
<tr>
<td></td>
<td>A.5.0 Information security policies</td>
</tr>
<tr>
<td></td>
<td>A.6.0 Organisation of information security</td>
</tr>
<tr>
<td></td>
<td>A.7.0 Human resources security</td>
</tr>
<tr>
<td></td>
<td>A.8.0 Asset management</td>
</tr>
<tr>
<td></td>
<td>A.9.0 Access control</td>
</tr>
<tr>
<td></td>
<td>A.10.0 Cryptography Controls</td>
</tr>
<tr>
<td></td>
<td>A.11.0 Physical and environmental security</td>
</tr>
<tr>
<td></td>
<td>A.12.0 Operations security</td>
</tr>
<tr>
<td></td>
<td>A.13.0 Communications security</td>
</tr>
<tr>
<td></td>
<td>A.15.0 Supplier Relationships</td>
</tr>
<tr>
<td></td>
<td>A.16.0 Information security incident management</td>
</tr>
<tr>
<td></td>
<td>A.17.0 Information security aspects of business continuity management</td>
</tr>
<tr>
<td></td>
<td>A.18.0 Compliance</td>
</tr>
</tbody>
</table>

### 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>David Batty</td>
<td>Initial version</td>
<td>Barry Haynes (Chair of IGMG)</td>
<td>20/10/2016</td>
</tr>
<tr>
<td>2.0</td>
<td>01/03/2019</td>
<td>Charles Hindmarsh</td>
<td>New ISMS format</td>
<td>Andy Pellow (Chair of IGMG )</td>
<td>22/03/2019</td>
</tr>
<tr>
<td>2.1</td>
<td>18/09/2019</td>
<td>Charles Hindmarsh</td>
<td>Modified intro and A.14.2.1, A.14.2.1.2, A.14.2.5.1 &amp; A.14.2.6 as this is now out of scope</td>
<td>Andy Pellow (Chair of IGMG )</td>
<td>25/09/2019</td>
</tr>
</tbody>
</table>
Contents

Purpose ................................................................................................................. 4
Applicability ........................................................................................................... 4
A.14.0 System Acquisition, Development & Maintenance ......................... 4
A.14.1 Security Requirements of Information Systems ......................... 4
  A.14.1.1 Information Security Requirements Analysis and Specification ........ 4
  A.14.1.2 Securing Application Services on Public Networks ...................... 4
  A.14.1.3 Protecting Application Services Transactions ............................ 5
  A.14.2.1 Secure Development Policy ......................................................... 5
    A.14.2.1.1 Security Principles ................................................................. 6
    A.14.2.1.2 Apply Defence in Depth ....................................................... 6
    A.14.2.1.3 Use a Positive Security Model .......................................... 6
    A.14.2.1.4 Fail Securely ........................................................... 6
    A.14.2.1.5 Run with Least Privileges .................................................... 6
    A.14.2.1.6 Avoid Security by Obscurity ................................................ 7
    A.14.2.1.7 Keep Security Simple ......................................................... 7
    A.14.2.1.8 Detect Intrusions ............................................................... 7
    A.14.2.1.9 Don't Trust Services ......................................................... 7
  A.14.2.2 System Change Control Procedures ........................................ 7
  A.14.2.3 Technical Review of Applications after Operating Platform Changes ...... 7
  A.14.2.4 Restrictions on Changes to Software Packages ......................... 7
  A.14.2.5 Secure System Engineering Principles ................................... 8
  A.14.2.6 Secure Development Environment .......................................... 8
  A.14.2.7 Outsourced Development ......................................................... 8
  A.14.2.8 System Security Testing .......................................................... 8
  A.14.2.9 System Acceptance Testing ..................................................... 8
A.14.3 Test Data ............................................................................................... 9
  A.14.3.1 The Protection of Test Data ....................................................... 9
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 sets the acquisition, maintenance and application development policies within the IRC Information Security Management System (ISMS).

Applicability
System acquisition and maintenance applies to UoL IT. The development of applications applies only to IT and/or 3rd parties who develop applications with interfaces for collecting storing and processing information. IRC projects can develop their own small applications, but they are restricted to operating in their isolated environment. There is no requirement for researchers to follow secure application development principles. However should an application hosted outside of a VRE be required to interact with the internet, the following policies should be followed.

A.14.0 System Acquisition, Development & Maintenance
A system acquisition policy is managed by UoL IT and is out of scope for this ISMS.

A.14.1 Security Requirements of Information Systems

A.14.1.1 Information Security Requirements Analysis and Specification
A risk assessment is conducted for every project as per the Information Security in Project Management policy (A.6.1.5). The output defines the service specification needed to fulfil the requirements of a project.

A.14.1.2 Securing Application Services on Public Networks
Information security is designed into all architecture layers (business, data, applications and technology) balancing the need for information security with the need for accessibility. All IRC-Confidential or IRC-Secure information is protected by risk mitigating controls, such as encryption (A.10.1.0) during transmission outside the trusted research environment.
A.14.1.3 Protecting Application Services Transactions

The following security controls or features set out in Table A.14.1.3.1 are considered for code that will collect and process information, particularly when the data is classified as IRC-Confidential or IRC-Secure.

Table A.14.1.3.1 Security Controls

<table>
<thead>
<tr>
<th>Test</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Authentication:</td>
<td>The ability to uniquely identify users and processes that are attempting to access the program or its data (such as with IDs and passwords, biometrics etc.).</td>
</tr>
<tr>
<td>2. Access control:</td>
<td>The ability to allow only appropriate access to data (such as with file rights, encryption, etc.) based on its sensitivity and who should have access to it.</td>
</tr>
<tr>
<td>3. Auditing &amp; logging:</td>
<td>The ability to log access attempts (both successful and unsuccessful) at least to privileged areas, or sensitive information.</td>
</tr>
<tr>
<td>4. Input/output &amp; data validation:</td>
<td>The ability for the application to determine that data entered and received by the user is in an acceptable format and will not compromise the security of the application, or cause it to crash.</td>
</tr>
<tr>
<td>5. Encryption:</td>
<td>All information must be encrypted in transmission across public networks.</td>
</tr>
<tr>
<td>6. Physical:</td>
<td>Physical issues including environmental threats such as power failure, physical access to offices, infrastructure and data should all be considered and appropriate features and measures implemented.</td>
</tr>
</tbody>
</table>

A.14.2 Security in Development and Support Processes

A.14.2.1 Secure Development Policy

This policy applies to anyone who is commissioned to create an application to be used by multiple users for the collection and processing of information. This includes:
1. Installable software packages programmed for use within the IRC, virtual or desktop computers.
2. Web applications deployed on the IRC infrastructure.

The IRC Information Governance Management Group (IGMG) are responsible for maintaining this document.

A.14.2.1.1 Security Principles
The principles in the following sub-sections must be applied throughout the process of software development. A summary for each principle is cited or adapted from the Open Web Application Security Project (OWASP) website, which also signposts to further information.

A.14.2.1.2 Apply Defence in Depth
Layered security mechanisms must be in place to increase security as a whole. A VRE will not interface directly with the internet or campus network. Any public facing web applications must be located in a DMZ. The design and development of a public facing application, must be approved by the IT Assurance Team.

A.14.2.1.3 Use a Positive Security Model
A ‘positive’ security model defines what is allowed and rejects everything else. For example, web applications by default have web authentication turned on by the server - this automatically disallows all users until the web application file allows the specific users or groups. This same mechanism applied to IP addresses - default IP address request filtering means that IP address and IP address ranges must be defined in the web application file. This applies a ‘whitelist’ (positive), rather than ‘blacklist’ approach.

A.14.2.1.4 Fail Securely
Handling errors is a key aspect of secure coding. It is important that failures are handled so that exceptions do not enable behaviour that the countermeasure would not normally allow. For example, web page query strings are checked for valid key value pairs - if either is incorrect then a generic error is issued and if the query string sends parameters to the database this process will not be called and a database connection is not established.

A.14.2.1.5 Run with Least Privileges
The principle of least privilege is required to perform the business process. An example of this is database connection privileges from web applications. If there are multiple sets of user groups with varying data access privileges then separate account groups are set up to consistently constrain access. For example, set up a read only access group for read users and a read/write access group for editor users.
A.14.2.1.6 Avoid Security by Obscurity
Security by obscurity is alone a weak security mechanism, however when combined with all principles it can be used as an additional layer of security. For example, web applications use a custom error page which do not reveal unneeded server information such as server type, version details.

A.14.2.1.7 Keep Security Simple
Attack surface area and simplicity go hand in hand. It is important to keep security simple. For example, authentication should avoid double negation, e.g. ‘if (!user.isNotFound())’ should be replaced with ‘if (user.isFound())’.

A.14.2.1.8 Detect Intrusions
Collect and record any information regarding access and usage that can assist in detecting and monitoring unauthorised actions. Real time monitoring is not assumed to be sufficient. For example, web applications use database logging to track every query sent to the server.

A.14.2.1.9 Don’t Trust Services
Some applications may refer to external systems that are likely to have differing, less secure policies. This could include built software in the IRC gateway using user’s resources on a local system such as a date and time. Such variables, when critical, should validated against a reliable source such as a web server date and time values.

A.14.2.2 System Change Control Procedures
Applications that are developed and contained within a VRE, are not subject to formal change control.

Changes to internet facing applications will need approval through the University of Leeds change process as defined in Change Management Policy (A.12.1.2).

Refer to the Technical Vulnerability Management Policy (A12.6).

A.14.2.4 Restrictions on Changes to Software Packages
The following must be observed with regard to software:

1. All software acquired by the IRC must be installed by the DST.
2. Only software which has an agreed research use, is approved by DST and is properly licensed will be loaded onto a Virtual Research Environment.
3. Except for backup or archival purposes, copying of any software is expressly prohibited as such action may expose the University to an infringement of copyright laws.
4. The use of unlicensed software is not permitted under any circumstances as such action may expose the University to prosecution.
5. Personal, non-research software, programs or utilities may not be installed on any IRC system, unless it has been approved by DST. This includes public domain, shareware or bulletin board software.
6. Only IT can provide and modify infrastructure configuration.
7. Upon termination of a research project the DST will recover any IRC owned software for redeployment.

A.14.2.5 Secure System Engineering Principles
Where applications have been developed to collect information across public infrastructure:

1. Communications must be encrypted.
2. Applications must be user acceptance tested and security tested (as per A.14.2.8) by IT Assurance against the OWASP security principles.
3. High risks must be remediated.

A.14.2.6 Secure Development Environment
The VRE is a secure environment. It does not have the ability to interact with the internet or other VREs and is limited to authorised project members only.

A.14.2.7 Outsourced Development
Applications that are developed by a 3rd party are built to fulfil a research requirement are subject to University IT approval and procurement policies as well as testing by the IT Assurance Team.

A.14.2.8 System Security Testing
Application security testing must be completed before the application is exposed to the campus network or the internet. This is to ensure any compatibility issues arising from different environments do not affect the running of the application or introduce new security vulnerabilities.

1. All applications are tested and validated against the OWASP Secure Coding Practices.
2. Testers must differ from the person(s) who developed the application.
3. Automated systems can be used to test systems.

A.14.2.9 System Acceptance Testing
Applications are subject to user acceptance testing.
A.14.3 Test Data
Test data should be created for the purposes of developing the application. Testing must not be carried out on active research data.

A.14.3.1 The Protection of Test Data
It is the responsibility of the Principal Investigator to ensure there is sufficient test data available to prove the code works and that testing is not performed using live data.