Supply Management

PURPOSE

HIC Services requires the security of its information to be maintained in order to ensure that it is able to rely on its information for its business needs and meets its statutory, regulatory and contractual obligations. Such security is critical to achieve and maintain ISO/IEC 27001:2013 based security controls.

SCOPE

This will cover all suppliers to HIC which have an effect on the security of its information

RESPONSIBILITIES

<table>
<thead>
<tr>
<th>ROLE</th>
<th>RESPONSIBILITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Development Team</td>
<td>Responsible for implementing monitoring within applications and for actively monitoring the Service Catalogue for service status.</td>
</tr>
</tbody>
</table>

PROCEDURE

Steps

1. Where possible, service monitoring is performed throughout the entire life of a service / project within HIC. In the occurrence of an important event, relevant members of staff are notified. Levels of expected service will be agreed with the Client during the requirements stage.
2. Any organisation accessing, processing, communicating, or managing HIC's information must do so such that HIC's legal, regulatory and contractual obligations are met.
3. Any handling of personal data beyond the HIC environment must obtain the necessary approvals from the data controller prior to processing.
4. Access to information assets and systems will be the minimum necessary to achieve business purposes.
5. Supplier personnel may only enter HIC's premises with appropriate identification and may only enter areas of HIC's premises commensurate with their function and, where appropriate (for example, in security areas), escorted by HIC staff.
6. Where a supplier is contracted to manage a service utilising or connected to HIC information, information assets or information systems, the supplier must ensure that an information security management system employed to secure HIC data, information assets or information systems is in place and where appropriate complies with ISO/IEC 27001. Evidence must be provided to HIC of compliance with the standard, either through formal certification or otherwise to HIC's satisfaction before any HIC information, information assets or information systems are accessed by the supplier.
7. Suppliers must have a security incident reporting process in place to a standard and design acceptable to HIC to ensure that any incidents involving HIC information are immediately reported to HIC. Suppliers must agree to undertake any remedial action required by
HIC and ensure that this is implemented in an auditable manner.

APPLICABLE REFERENCES
- Registered company office address and registration number in the UK
- For Definitions see ISMS Glossary

QUALITY RECORDS
- Supplier Assessment
- Catalogue of suppliers

DOCUMENT CONTROLS

<table>
<thead>
<tr>
<th>Process Manager</th>
<th>Point of Contact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Keith Milburn</td>
<td><a href="mailto:hicbusiness-support@dundee.ac.uk">hicbusiness-support@dundee.ac.uk</a></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Version Number</th>
<th>Effective Date</th>
<th>Edited By</th>
<th>Edition Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>08/01/16</td>
<td>Graham MacKay</td>
<td>New Procedure</td>
</tr>
<tr>
<td>25/02/20</td>
<td>Tracey Stewart (Data Entry Team Leader)</td>
<td>Updated cover sheet with new approved process information</td>
<td></td>
</tr>
<tr>
<td>30/06/20</td>
<td>Duncan Heather (Governance Manager)</td>
<td>Reviewed, no changes made</td>
<td></td>
</tr>
<tr>
<td>1.1</td>
<td>Symone Sheane (Project Coordinator)</td>
<td>Updated to a Standard Operating Procedure template.</td>
<td></td>
</tr>
</tbody>
</table>
| 1.2            | 08/02/24       | HIC Operational Group      | Changed title of SOP. Removed "any processing of personal data outside the HIC environment may only take place with the express
Last Review Date | Triggers
--- | ---
26/02/24 | • Annual Review  
| | • Internal Audit (conducted by TASC annually) has identified opportunities for improvement (OFI) or nonconformities (NC)  
| | • External Audit has identified OFI or NC  
| | • Significant Event has highlighted OFI  
| | • Client Complaint has highlighted OFI  
| | • HIC All Staff (individuals of) have identified OFI

Approved by the HIC Ops Group Date | Approved by the HIC Exec Date
--- | ---
05/02/24 | N/A

| 1.3 | 26/02/24 | Symone Sheane | Moved SOP to Confluence from SharePoint |  
| | | | |  

Copyright Health Informatics Centre. All rights reserved. May not be reproduced without permission. All hard copies should be checked against the current electronic version within current versioning system prior to use and destroyed promptly thereafter. All hard copies are considered Uncontrolled documents.