Keeping data safe: how to implement a secure repository

Jenny Evans - University of Westminster
Tom Reany - Lead Repository Developer, Haplo
Dr Peter Trible - System Administrator, Haplo

Traditionally Repository Managers and Repositories have focused on supporting open access and making all data and outputs available without restriction. But there are increasing requirements to restrict access, especially when extending repositories to handle research data, and the GDPR adds significant financial penalties, in addition to reputational damage, if you get it wrong. The University of Westminster and Haplo worked together to ensure the security of their repository.

<table>
<thead>
<tr>
<th>Risk</th>
<th>Threat</th>
<th>Probability</th>
<th>Impact</th>
<th>Risk level</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accidental access by an unauthorized user (who’s record)</td>
<td>Access to sensitive image</td>
<td>1</td>
<td>2</td>
<td>Moderate</td>
<td>Use appropriate access controls and ensure all users are trained.</td>
</tr>
<tr>
<td>Removal of service to a user</td>
<td>Inactive or non-responding server</td>
<td>1</td>
<td>3</td>
<td>High</td>
<td>Ensure the system is monitored and issues are resolved promptly.</td>
</tr>
<tr>
<td>Data corruption</td>
<td>Intrusive code that corrupts data</td>
<td>2</td>
<td>3</td>
<td>High</td>
<td>Regularly back up data and ensure systems are monitored.</td>
</tr>
<tr>
<td>Accidental access to an unapproved file</td>
<td>Malicious code that uploads data</td>
<td>2</td>
<td>3</td>
<td>High</td>
<td>Use appropriate access controls and ensure all users are trained.</td>
</tr>
<tr>
<td>Unauthorized access to confidential files</td>
<td>Malicious code that uploads data</td>
<td>2</td>
<td>3</td>
<td>High</td>
<td>Regularly back up data and ensure systems are monitored.</td>
</tr>
</tbody>
</table>

A threat model helps clarify priorities and the actions you need to take to reduce risk.

Risks are a threat to:
- Confidentiality: Can the data be accessed without knowledge of the person’s identity?
- Integrity: Can the data be altered or deleted?
- Availability: Can the research data be accessed when required?

Evaluating systems for security assurance

Repository software

Is the particular system appropriate? Is the FBS (Federated Research System) or the Haplo system appropriate for the data you are managing?

Repository software

Is the particular system appropriate? Is the FBS (Federated Research System) or the Haplo system appropriate for the data you are managing?

Repository software

Is the particular system appropriate? Is the FBS (Federated Research System) or the Haplo system appropriate for the data you are managing?

Repository software

Is the particular system appropriate? Is the FBS (Federated Research System) or the Haplo system appropriate for the data you are managing?

Evaluating systems for security assurance

Repository software

Is the particular system appropriate? Is the FBS (Federated Research System) or the Haplo system appropriate for the data you are managing?

Evaluating systems for security assurance

Repository software

Is the particular system appropriate? Is the FBS (Federated Research System) or the Haplo system appropriate for the data you are managing?

Evaluating systems for security assurance

Repository software

Is the particular system appropriate? Is the FBS (Federated Research System) or the Haplo system appropriate for the data you are managing?

Evaluating systems for security assurance

Repository software

Is the particular system appropriate? Is the FBS (Federated Research System) or the Haplo system appropriate for the data you are managing?