Security Fundamentals for Research

The following recommendations are actionable steps that members of research teams (including non-UMN affiliated) can take to protect the confidentiality and integrity of their data.

### Identify the data

<table>
<thead>
<tr>
<th>Principal Investigator</th>
<th>University Contacts and Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classify the data according to UMN policy and identify the data security level of the system(s) collecting and storing the data: cla.umn.edu/latis/protecting-your-data</td>
<td><a href="mailto:security@umn.edu">security@umn.edu</a></td>
</tr>
<tr>
<td>Consult if grant or contract requirements include specific information security frameworks, such as FISMA, ITAR, NIST 800, or others.</td>
<td>University Office of the General Counsel</td>
</tr>
<tr>
<td>Periodically review the data classification and security level of your data or projects.</td>
<td>University Export Control Officer: research.umn.edu/units/rco/export-controls/overview</td>
</tr>
</tbody>
</table>

### Evaluate the technology

<table>
<thead>
<tr>
<th>Principal Investigator</th>
<th>University Contacts and Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use existing UMN IT services: it.umn.edu</td>
<td><a href="mailto:security@umn.edu">security@umn.edu</a></td>
</tr>
<tr>
<td>Configure self-managed services to comply with UMN Information Security Standards: it.umn.edu/information-security-standards</td>
<td></td>
</tr>
<tr>
<td>Review vendor information security documentation periodically: it.umn.edu/information-security-standards/vendorsupplier-management</td>
<td></td>
</tr>
</tbody>
</table>
Take information security training

**Principal Investigator**

- Include relevant, current information security guidance, such as incident reporting, in lab manuals, standard operating procedures or orientation/onboarding trainings.
- Coordinate online information security training annually for your research teams: [it.umn.edu/good-practice/participate-in-information-security](it.umn.edu/good-practice/participate-in-information-security)

**Team Member**

- Complete the information security training online or during lab training.
- Review Secure U or other information security communications to keep informed, such as phishing, scams, vulnerabilities, and more: [it.umn.edu/safe-computing](it.umn.edu/safe-computing) [it.umn.edu/secure-u](it.umn.edu/secure-u)

**University Contacts and Resources**

- security@umn.edu

Keep access up-to-date

**Principal Investigator**

- Remove or suspend access promptly, such as for students over summer break. Include in off-boarding process.
- Review access to data and to physical spaces annually.

**Team Member**

- Notify PI promptly if access is no longer needed.
- Return ownership of folders, documents, or any stored data to the PI.

**University Contacts and Resources**

- security@umn.edu
- Department IT
- Building access coordinator(s)

Report security incidents or send any security questions to **security@umn.edu**