Secure Research in Citadel

Presented by: Ryan Fedon and Irene Kopaliani
What is Citadel?

- Streamlined, secure deployment
- Supports collaboration both within and outside of Princeton
- Separation duties
- Data export control
- Available on-demand, with minimal maintenance
- Post-quantum cryptography ready
Why to use Citadel?

CUI (NIST SP 800-171)

FISMA (NIST SP 800-53)

HIPAA

Always restricted data

- Social Security numbers
- Bank account numbers
- Driver’s license numbers
- State identity card numbers
- Credit card numbers
- Data subject to HIPAA
- Data subject to GDPR

Protect Our Info (princeton.edu)
Research Data Security | Research Integrity and Assurance (princeton.edu)
Demo

Citadel
Secure Research Infrastructure
Requesting Project Tenancy

1. IRB, ISO, or ORPA recommends Citadel tenancy.

2. PI completes tenancy application in ServiceNow.

3. The Citadel Steering Committee reviews the application and votes within five days.

4. For approved applications, the environment is provisioned and configured.
Requesting Access to the Project

Citadel

About

Secure Research Infrastructure (Citadel) supports collaboration both within and outside of the University through secure, multi-user virtual machines with encrypted data. It prevents unauthorized access, change, and distribution of sensitive data such as Controlled Unclassified Information (CUI), Intellectual Property (IP), and Export-Controlled Data (ITAR/EAR). Sensitive data is fully encrypted with user-owned public/private keys and is not accessible by system administrators. Only those with explicit access have the keys to decrypt the data. Citadel users are required to complete the initial training and ongoing annual refresher.

Important Notes

1. Complete required training before onboarding.
3. Complete the Request form.

To get started, visit: KB0013057 Article
<table>
<thead>
<tr>
<th></th>
<th>Additional Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Each project needs to have 2-3 sub-admins to administer data and user controls.</td>
</tr>
<tr>
<td>2</td>
<td>Sub-admins are members of the research group.</td>
</tr>
<tr>
<td>3</td>
<td>All users must complete onboarding training and sign the Rules of Behavior.</td>
</tr>
<tr>
<td>4</td>
<td>Sub-admins must complete additional training during the onboarding process.</td>
</tr>
<tr>
<td>5</td>
<td>Mandatory annual security training is less than two hours.</td>
</tr>
<tr>
<td>6</td>
<td>The Primary Investigator is responsible for approving access to their data for each researcher.</td>
</tr>
</tbody>
</table>
Questions?

Contacts:

| Ryan Fedon       | Dr. Irene Kopaliani, C|CISO CISA, CISM, CDPSE, CISSP, CCSP |
|------------------|-----------------------|
| rfedon@princeton.edu | ik8@princeton.edu     |