Policy Statement
This policy establishes measures that must be taken to report and respond to a possible breach or compromise of restricted data, including the determination of the systems affected, whether any restricted data have in fact been compromised, what specific data were compromised and what actions are required for forensic investigation and legal compliance.

Policy Guidelines
Cornell Restricted Access Data Center (CRADC) is committed to compliance of restricted data. For the purpose of this document, restricted data relates to any nonpublic data that is protected by regulation, law or policy and/or is subject to contractual access restrictions as defined by a Data Use Agreement (DUA). CRADC, as the Data Custodian of these data, along with the authorized research team (Researcher), are obligated to adhere to the conditions set forth by the Data Provider in a signed DUA and this policy.

Reporting:
It is the responsibility of the Researcher to contact CRADC’s Security Liaison in a timely manner, in accordance with Cornell University Policy 5.4.2, Reporting Electronic Security Incident, if the Researcher suspects or is aware of a compromise creating risk of unauthorized access to restricted data.
Response:
Upon receipt of such report, the CRADC Security Liaison, the CRADC Secure Data Services Manager, and the Sr. Systems Administrator will convene to review the report. Upon initial review, the Cornell University Security Office will be notified to assist, according to Cornell University Policy 5.4.2, Reporting Electronic Security Incident.

Process Steps:
1. Identify:
   a. Nature of incident to best of knowledge
   b. Identify data involved
   c. Establish Data Provider contact information
   d. Identify systems involved, remove from network if applicable
   e. Review applicable policies, regulations and/or laws involved
2. Recovery and Response:
   a. Contact Cornell University IT Security Office for assistance in forensics
   b. Secure the system and preserve it without change
   c. If deemed necessary, the Security Office will alert Cornell University Data-Loss Incident Response Team
   d. Resolve situation
3. Communicate:
   a. Contact Office of Sponsored Programs (OSP)
   b. OSP will contact Data Provider to inform of current situation
   c. If required, notify individuals of data theft
4. Document:
   a. Create an incident report
   b. Document lessons learned
   c. Update necessary documentation

Entities Affected by this Policy
CRADC Secure Data Services Manager, CRADC Secure Data Specialist, CISER Information Technology staff, and CRADC account holders.

Who Should Read this Policy
CRADC Secure Data Services Manager, CRADC Secure Data Specialist, CISER Information Technology staff, CRADC account holders and affiliated CRADC staff.
RELATED DOCUMENTS

Cornell University Policy 5.1, Responsible Use of Information Technology Resources

Cornell University Policy 5.4.1, Security of Information Technology Resources

Cornell University Policy 5.4.2, Reporting Electronic Security Incidents

Cornell University Policy 5.8, Authentication to Information Technology Resources

Cornell University Policy 5.9, Access to Information Technology Data and Monitoring Network Transmissions

Cornell University Policy 5.10, Information Security

CONTACTS

If you have questions about specific issues regarding the CRADC Restricted Data Security Breach Reporting and Response Policy, call the following offices:

<table>
<thead>
<tr>
<th>Name</th>
<th>Email</th>
<th>Role</th>
<th>Telephone</th>
</tr>
</thead>
<tbody>
<tr>
<td>William Block</td>
<td><a href="mailto:block@cornell.edu">block@cornell.edu</a></td>
<td>CISER Director</td>
<td>607-255-4081</td>
</tr>
<tr>
<td>Stephanie Jacobs</td>
<td><a href="mailto:cradc@cornell.edu">cradc@cornell.edu</a></td>
<td>CRADC Secure Data Services Manager</td>
<td>607-255-4081</td>
</tr>
<tr>
<td>Michelle Edwards</td>
<td><a href="mailto:cradc@cornell.edu">cradc@cornell.edu</a></td>
<td>CRADC Secure Data Specialist</td>
<td>607-255-4081</td>
</tr>
<tr>
<td>Janet Heslop</td>
<td><a href="mailto:jheslop@cornell.edu">jheslop@cornell.edu</a></td>
<td>CISER Director of Information Technology and Security Liaison</td>
<td>607-255-4081</td>
</tr>
<tr>
<td>Kim Burlingame</td>
<td><a href="mailto:Kb269@cornell.edu">Kb269@cornell.edu</a></td>
<td>CISER Sr. System Administrator</td>
<td>607-255-4081</td>
</tr>
<tr>
<td>Cornell University Security Office</td>
<td><a href="mailto:security-services@cornell.edu">security-services@cornell.edu</a></td>
<td>University Security Office</td>
<td>607-255-6664</td>
</tr>
</tbody>
</table>

RESPONSIBILITIES

The following are major responsibilities each party has in connection with this policy.

<table>
<thead>
<tr>
<th>Role</th>
<th>Responsibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRADC Secure Data Services Manager</td>
<td>Interpret this policy, provide clarification and education, and implement operational and business processes to facilitate compliance.</td>
</tr>
<tr>
<td>CISER Director of Information Technology and Security Liaison</td>
<td>Implement operational, physical, and technical equipment and tools to facilitate compliance.</td>
</tr>
<tr>
<td>Role</td>
<td>Responsibility</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>CISER Sr. System Administrator</td>
<td>Responsible for performing tasks in accordance with established policy guidelines.</td>
</tr>
<tr>
<td>CRADC Affiliated Staff</td>
<td>Responsible for knowing and assisting with tasks as related to this policy.</td>
</tr>
<tr>
<td>CRADC Researcher</td>
<td>Responsible for knowing and abiding by the Data Provider Agreement and this policy.</td>
</tr>
</tbody>
</table>