University of California, Davis

Secure Research Computing Environment Policy

Revision History

<table>
<thead>
<tr>
<th>Date:</th>
<th>Version</th>
<th>Author:</th>
<th>Description:</th>
</tr>
</thead>
<tbody>
<tr>
<td>5/17/2018</td>
<td>1.0</td>
<td>Ira Tarshis</td>
<td>Developed initial draft</td>
</tr>
<tr>
<td>10/4/2018</td>
<td>1.1</td>
<td>Jackson Muhirwe</td>
<td>Edits</td>
</tr>
</tbody>
</table>
I. Purpose

The UC Davis Information and Educational Technology Department (IET), in its commitment to support research involving highly regulated data, has developed the Secure Research Computing Environment (SRCE). Researchers may find the SRCE particularly useful for complying with heightened security standards (such as NIST 800-171) imposed by granting agencies or outside data owners. The UC Davis SRCE is designed to meet or align with these heightened security standards; the exact security standards of the SRCE are documented in the SRCE Security Standards documents (Exhibits A-N).

In order for the SRCE to maintain heightened security standards, all users of the SRCE are required to participate and securely manage their portion of the environment and their responsibilities to the heightened security standards of the SRCE; no exceptions from these requirements or responsibilities will be granted. This policy defines the requirements for use of the SRCE.

II. Definitions

A. Research Unit—a unit led by a Research Unit Head who facilitates and manages research on behalf of UC Davis. A Research Unit may include any number of Principle Investigators.

B. Research Unit Head—an individual that carries overall responsibility for a Research Unit’s projects and supervision of Workforce Members. UHs may manage multiple research projects each headed by a PI. UHs may supervise any number of PIs. This role is equivalent to a Workforce Manager as defined in IS-3.A UH might be the same Workforce Member as a Principle Investigator (PI). In such cases, this Workforce Member is responsible for both roles.

C. Principal Investigator—an individual that manages research projects and Workforce Members on behalf of UC Davis and reports to a UH. A particular PI might also serve as UH for a particular research project. In such cases, this individual is inherently responsible for both roles. Also a Workforce Manager as defined in IS-3.

D. Sub-Environment—an environment within the SRCE that is provisioned for a particular data set or PI.

E. Unit IT—an individual or group of individuals responsible for user accounts, administration, and security of all Research Unit IT systems for Research Units with access to the system.

F. SRCE Security Standards—Exhibits A-N as referenced in this document. The SRCE Security Standards are not public and will be shared during the SRCE onboarding process (before any individuals are required to sign this document) to the Research Unit Head and any other individuals engaging with the SRCE.

G. Service Manager—the individual responsible for the day to day management tasks associated with the system as delegated by the Service Owner. The Service Manager may in turn delegate tasks to other Service Provider Workforce Members.

III. Policy

A. UC Davis SRCE Security Standards (Exhibit A-N) will be published and maintained by IET. These security standards will be reviewed every three years by UC Davis Information Security Office (ISO) and UC Davis Enterprise Infrastructure Services (EIS).
B. IET will have the SRCE Externally evaluated to the NIST 800-171 standards on a periodic basis, will maintain a third party attestation report for the SRCE.

C. IET will manage and maintain the SRCE shared infrastructure – this includes provisioning a Sub-Environment to the Research Unit Head or faculty responsible for that Sub-Environment’s research.

D. Research Unit Heads, Principal Investigators, faculty members, and all other users of the SRCE must comply with this policy and all SRCE Security Standards (Exhibit A-N). Compliance with the SRCE Security Standards (Exhibit A-N) includes, but is not limited to, the following:
   1. Research Unit Heads must manage and maintain responsibility for access control to their Sub-Environments.
   2. Research Unit Heads must work with their Unit IT to ensure the components within their IT environments that access the SRCE and their SRCE Sub-Environments are compliant with this policy and the SRCE Standards (Exhibits A-N).

E. Any research unit that utilizes the SRCE is subjected to an audit of their use of the SRCE. Audits will be conducted by the ISO or by a third party reviewer at the direction of the ISO.

F. In order for the SRCE itself to maintain heightened security standards, non-compliance with any part of this policy or any part of the SRCE Standards (Exhibits A-N) will result in the following actions:
   1. Upon a determination by IET that a Research Unit is not in compliance with the SRCE policy, the SRCE Standards, or the Service Level Agreement for the SRCE, IET will inform the Research Unit of this determination of non-compliance and the Research Unit will be placed on SRCE probation. The non-compliant Research Unit will then be required to submit to an extended review and monitoring period.
   2. If a Research Unit’s non-compliance is more than incidental, then the Research Unit will be required to contact and consult with the ISO and provide any requested information to the ISO. Upon successful consultation, the ISO will provide recommendations for achieving mitigation and/or remediation of non-compliance. Research Units must implement all ISO recommendations.
   3. If a Research Unit is unable to comply with any of the requirements of this policy, they should apply for an exception using the UC Davis Policy Exception Process. Details for the exception process can be found on this link http://kb.ucdavis.edu/?id=0700
   4. If IET finds on-going, pervasive, and/or systemic non-compliance with this policy or with the SRCE Security Standards (Exhibits A-N) or security deficiencies, or if the Research Unit fails to correct any non-compliance in a timely manner after notification by IET, then the Research Unit’s use of the SRCE will be terminated.

IV. Roles and Responsibilities

A. Research Unit Heads are responsible for
   1. Ensuring that their Research Units, Principal Investigator(s), and delegates are compliant with this policy and the SRCE Standards (Exhibits A-N).
   2. Properly delegating duties to their Unit IT as needed, as well as to their research support staff as needed.
3. Ensuring that all delegations of responsibility are clear and unambiguous.

4. Complying with any other Research Unit Head’s responsibilities defined in this policy or in the SRCE Standards (Exhibits A-N) that have not been expressly delegated to and accepted by another individual.

5. Informing the ISO of any confirmed or suspected security issues, security breaches, or non-compliance with this policy or the SRCE Standards within 2 days.

6. Signing this policy and the SRCE Service Level Agreement and reading, understanding, and agreeing to this policy and the SRCE Security Standards (Exhibit A-N) prior to any access or use of the SRCE by the Research Unit or Research Unit Head.

B. The SRCE Service Manager will inform the ISO and the users of the SRCE of any significant issues within the SRCE.

C. IET is responsible for
   1. Maintaining guidance documentation regarding the implementation and applicability of security standards as specified in the SRCE Security Standards (Exhibit A-N).
   2. Managing, maintaining, and supporting the SRCE’s shared infrastructure and developing a cost recovery model as specified in the SRCE SLA.

V. Further Information

A. [Link to more information on IT catalog]

B. [Link to Knowledge Base articles]

C. For more information or questions please contact the ISO at cybersecurity@ucdavis.edu or EIS at srce@ucdavis.edu.

VI. References


B. SRCE Security Standards (Exhibits A-N)


Appendix

Standards for implementing this policy include the following:

Exhibit A, 3.1 SRCE Access Control Policy
Exhibit B, 3.2 SRCE Awareness Training Policy
Exhibit C, 3.3 SRCE Audit and Accountability Policy
Exhibit D, 3.4 SRCE Configuration Management Policy
Exhibit E, 3.5 Identification and Authentication Policy
Exhibit F, 3.6 SRCE Incident Response Policy
Exhibit G, 3.7 SRCE Maintenance Policy
Exhibit H, 3.8 SRCE Media Protection Policy
Exhibit I, 3.9 SRCE Personnel Security Policy
Exhibit J, 3.10 SRCE Physical Protection Policy
Exhibit K, 3.11 SRCE Risk Assessment Policy
Exhibit L, 3.12 SRCE Security Awareness Policy
Exhibit M, 3.13 SRCE System and Comm Protection Policy
Exhibit N, 3.14 SRCE System and Information Integrity Policy