CORNELL UNIVERSITY
Cornell Institute for Social and Economic Research Policy

POLICY
Volume: RD

Chapter: AC-1

Responsible Executive: CRADC Secure Data Services Manager

# CRADC Access Control Policy

Responsible Office: Cornell Institute for Social and Economic Research

Originally Issued: 12/1/2015

Revised: 9/30/16

## POLICY STATEMENT

In order to comply with the terms set forth in the Data Use Agreement, Cornell Restricted Access Data Center (CRADC) must limit system and network access only to authorized users.

This policy covers all stages in the life-cycle of user access, including authorizing access, granting initial access, updating access as user roles change, and removing users who no longer require access.

## REASON FOR POLICY

CRADC recognizes that protecting information technology and data requires authorized users to act responsibly when using these resources. CRADC researchers, system administrators, and data custodians must strictly control access to information resources under their direction or ownership.

## POLICY GUIDELINES

These guidelines address the establishment of procedures prior to account provisioning and the effective implementation of authorization of access, account provisioning, change in status,

unsuccessful logon attempts, session lockout, account expiration, account re-enabling, record keeping, and account de-provisioning.

**Prior to Account Provisioning:**

**Institutional Review Board (IRB) Authorization:** Unless determined otherwise by Cornell Institutional Review Board for Human Participants (IRB), all researchers allowed on the CRADC servers are required to complete the CITI training course on Social & Behavioral Research Basic, Stage 1 satisfactorily. CRADC relies on the confirmation from the Office of Sponsored Programs (OSP) that approved researchers have satisfactorily passed the CITI training course on Social & Behavioral Research Basic, Stage 1, in addition to their Conflict of Interest (COI) statement.

In instances where Cornell's IRB states that an IRB review is not necessary for a project, such as business data which contain no human identifying characteristics, researchers will not be expected to complete the CITI training course on Social & Behavioral Research Basic, Stage 1. CRADC relies on confirmation from the Office of Sponsored Programs that these data do not require IRB review for Cornell's processing approval.

**Office of Sponsored Programs (OSP) Data Use Agreement (DUA):** CRADC accepts projects and provisions unique user accounts for faculty/staff/students once the Data Use Agreement between Cornell University's Office of Sponsored Programs and the Data Provider has been executed. Any project with an internal agreement from Cornell University for Cornell data is exempt from approval by OSP, but must retain approval of IRB and the CRADC User Agreement.

**CRADC User Agreement:** In addition to the final approval from OSP, which includes the IRB review as necessary, each researcher is required to complete a user agreement with CRADC covering the usage of the CRADC servers. CRADC User Agreements are only sent to a researcher for signature once CRADC has final approval from OSP, or internal agreement from Cornell University for Cornell data.

**Authorization of Access:**

Access to CRADC infrastructure systems may only be granted by the Office of Sponsored Programs after all appropriate processes and paperwork have been filed. In all cases, access must comply with applicable legal requirements.

No independent authorization is required for information technology personnel to conduct routine system protection, maintenance, or management purposes in accord with internal protocols and processes. Likewise, requests for access in connection with litigation, legal processes, or law enforcement investigations, or to preserve user electronic information for possible subsequent access in accordance with this policy, need no independent authorization if made by Cornell University's Office of the General Counsel.

**Account Provisioning:**
Upon receiving a signed CRADC User Agreement, the Secure Data Specialist proceeds with account creation. Once the account has been created, the researcher is notified via an email of their unique account user name and provided a secure link to their temporary password. All temporary passwords, by Active Directory Group Policy, must be changed upon initial login to any CRADC server.

**Change in Researcher Status:**
It is the responsibility of the Principal Investigator to inform the CRADC staff within ten business days of any changes in project staffing such that a researcher is no longer permitted to access the restricted data. CRADC staff will disable the researcher's access to the project files within two business days and notify the Office of Sponsored Programs. The Office of Sponsored Programs will then notify the Data Provider of said project staff changes. CRADC will re-enable or de-provision the user account based on the final decision as communicated by OSP on behalf of Cornell University and the Data Provider.

**Unsuccessful Logon Attempts:**
A policy is defined on the Domain Controller that locks all accounts after three unsuccessful logon attempts. A lockout period is enforced before the researcher can attempt to logon again.

**Session Lockout:**
Dependent upon the Data Provider's Data Use Agreement, a screensaver session lockout will occur after 15 minutes of non-activity. If the Data Provider agreement establishes criteria requiring idle sessions be suspended after less than 15-minutes of non-activity, special requests can be accommodated.

**Account Expiration:**
User account access remains dependent on the existing project requirements, as stipulated within the Data Provider's Data Use Agreement and approved by OSP, IRB, and the CRADC User Agreement. Any project with an internal agreement from Cornell University for Cornell data is exempt from approval by OSP, but must retain approval of IRB and the CRADC User Agreement. At the expiration of any existing project requirement, the user account will be disabled. When the requirement has been approved and all existing project requirements are complete, the user account will be re-enabled.

**Record Keeping:**
The CRADC Data Support Specialist oversees the management of CRADC projects and user accounts through a management system, and implements the unique project and user accounts within Active Directory Users and Computers on the CRADC domain controller. User accounts are created by the CRADC Data Support Specialist upon notification of completion of all required University and Data Provider signatures (i.e. Data Use Agreement, internal Cornell data, and/or Institutional Review Board). During any status update, the CRADC Data Support

Specialist ensures that both the management system and the CRADC domain controller are synchronized on researcher status and forthcoming expiration dates.

**Account De-provisioning:**
Account de-provisioning is based upon notification via an OSP communication. De-provisioning occurs within three business days.

**CISER Secure Data Services Staff De-provisioning:** Any change in the CISER Secure Data Services staff will be communicated via email to the Data Provider through OSP. The staff account will be disabled on the last day of employment within CISER Secure Data Services and the account terminated shortly thereafter.

## Entities Affected by this Policy

CRADC Secure Data Services Manager, CRADC Secure Data Specialist, CISER Information Technology staff, CRADC account holders and affiliated CRADC staff.

## 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

NIST Special Publication (SP) 800-53

FIPS Publication 200

CRADC Policies

CRADC Procedures

## Contacts

If you have questions about specific issues regarding this Sharing, Transmission and Distribution of Restricted Data Policy, call the following offices:

| | | | |
|---|---|---|---|
| William Block | block@cornell.edu | CISER Director | 607-255-4081 |
| Stephanie Jacobs | cradc@cornell.edu | CRADC Secure Data Services Manager | 607-255-4081 |
| Michelle Edwards | cradc@cornell.edu | CRADC Secure Data Specialist | 607-255-4081 |
| Janet Heslop | jheslop@cornell.edu | CISER Director of Information Technology and Security Liaison | 607-255-4081 |
| Kim Burlingame | Kb269@cornell.edu | CISER Sr. System Administrator | 607-255-4081 |

| | | | |
|---|---|---|---|
| Cornell University Security Office | security-services@cornell.edu | | 607-255-6664 |

## RESPONSIBILITIES

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

| | |
|---|---|
| CRADC Secure Data Services Manager | Interpret this policy, provide clarification and education, and oversee implementation of operational and business processes to facilitate compliance. |
| CISER Director of Information Technology and Security Liaison | Implement operational, physical, and technical equipment and tools to facilitate compliance. |
| CISER Sr. System Administrator | Responsible for performing tasks in accordance with established policy guidelines. |
| CRADC Affiliated Staff | Responsible for knowing and assisting with tasks as related to this policy. |
| CRADC Researcher | Responsible for knowing and abiding by the Data Provider Agreement and this policy. |

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.