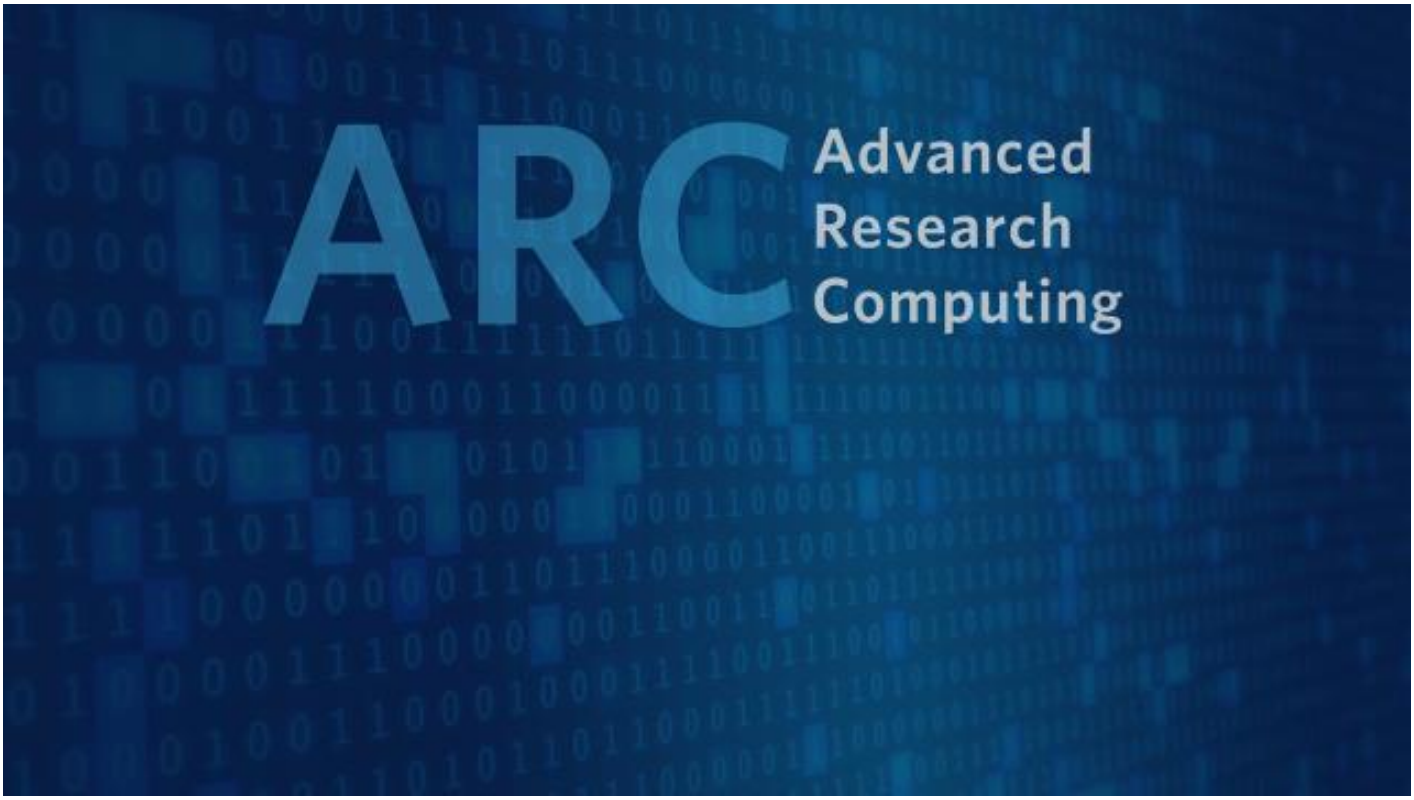
ARCS-14: REDCap Reporting, Logging and Monitoring

Version 2.0.0



THE UNIVERSITY OF BRITISH COLUMBIA

REDCap Reporting, Logging and Monitoring

1. Introduction

1.1 Purpose
This standard defines the reporting, monitoring and logging requirements for REDCap, including both system and security logs as a well as audit logs.

1.2 Scope
This Standard applies to all servers that collectively house the REDCap platform managed by UBC Advanced Research Computing (ARC). This includes the associated **REDCap Flex** production, pre-production, and development; application and database instances.

2. Standard

Effective logging and monitoring procedures (i.e. continual monitoring and/or periodic reviews) provide ongoing assurance that the UBC ARC REDCap platform, and the information it holds, is secure and that confidentiality and integrity are ensured. In the event of a security breach, **Audit Logs** are relied upon to determine whether or not information has been accessed or modified without authority.

Logs are generally intended to be used for maintenance and troubleshooting, as well as detecting and investigating information security events. Access for other purposes must be approved using one of the following methods:

- Internally, within UBC, in accordance with *UBC Information Security Standard M8 - Logging and Monitoring of UBC Systems*,
- Externally to law enforcement via Campus Security; or
- Externally to other entities via authorization from the Office of the University Counsel.

All transactions must be logged at the server layer, application layer, and database layer. Regular log review is required, and where appropriate, alerts of **Privileged Account** significant activities must be automatically transmitted to the **ARC Sensitive Research Team**.

All logs will be retained in Splunk and queried through SQL scripts at intervals described in the following sections.

2.1 Security Logging
Logs must record system faults to facilitate attack and unauthorized activity detection. Logs must be monitored to determine the use of system resources and to detect information security events (e.g. failed logons, simultaneous logins from different geographic locations, escalation of privilege, attacks against the system, etc). Monitoring software must be configured to send an alert to the **ARC Sensitive Research Team** when appropriate.

2.2 Audit Logs
REDCap has a built in audit trail which records all activities and data viewed or modified by a given user. REDCap **Audit Logs** will be scraped and retained in Splunk for review by the **ARC Sensitive Research Team**.

2.3 Server logs
The platform server logs have been integrated into a central logging and monitoring server that consolidates logs and allows system administrators to better monitor the health and stability of the system.

2.4 Database logs

REDCap logs both system level and project level events such as logins, data exports and record updates. REDCap provides project level logging information. In addition to viewing update history for individual records, authorized users can query the project logs for the following logged events:

- Data exports
- Project design and management
- User management
- Record creation, update, deletion
- Record locking
- Electronic signatures
- Record (page) views

2.5 Change Logs

REDCap is actively maintained by the development team at Vanderbilt University, and regularly releases updates containing security bug fixes and other changes. The **ARC Systems Administrators** will make the new release available once vetted in the pre-production environment and applied to the production system.

2.6 REDCap Version Monitoring

REDCap version release notes will be received by the **ARC Research Platforms Team**, triaged and assessed for significance and impact. The **ARC Sensitive Research Team** may be consulted to determine which the appropriate upgrade version and schedule.

Security patches and upgrades will follow the regular schedule as outlined in the *ARCS-21 System Maintenance* standard unless it is deemed that a REDCap upgrade is necessary for the security and stability of the application.

2.7 Project Monitoring

2.7.1 Stale Projects

Projects that have been inactive for six (6) months will be flagged by setting the project to offline and the **Project Owner** contacted by **ARC REDCap Support** to ascertain the status of the project. Projects will be marked as complete if no response is received within 30 days**.** Stale online projects will be monitored for on a monthly basis.

2.7.2 Development Status Use

Projects will be monitored to ensure no actual study data is entered while the project is still in Development status. Development status must only be used for designing and testing data forms. Projects must be moved into Production status before real data can be entered into forms.

ARC REDCap Support will contact the **Project Owner** if a project is:

- In Development status with more than 50 records, or
- In Development status for six (6) months or longer.

Projects that meets the criteria above and that have not been moved to Production status after 30 days are subject to be moved offline.

2.7.3 Practice/Just for fun Use

Projects must not be designated as Practice/Just for fun for more than six (6) months. **ARC REDCap Support** will move any project identified as Practice/Just for fun to Offline and contact the **Project Owner** to ascertain the status of the project.

2.7.4 Maximum Project Size

Projects are limited to 2GB (two gigabytes) in total size. The **Project Owner** will be notified if their project has exceeded the 2GB limit, and will be given 30 days to reduce their project size below this limit. Projects that exceed 2GB beyond the 30 day window will be inactivated.

2.8 User Monitoring

The following **User** activities must be logged and monitored:

- Login, logout, access to resource(s),
- Actions performed by **User** and the time they were performed,
- Any access to or modification of records.
- Simultaneous login.

2.8.1 Active Users with suspended Primary User

All **Primary User** and **Sponsored User** accounts will be monitored to ensure compliance with *ARCS-22 System Access Control*. **Sponsored Users** must have an active sponsor to maintain access to REDCap. **Users** activity will be monitored on a regular basis to ensure compliance.

2.9 Securing logs

All logs must be protected from unauthorized access and modification, by storing them on the database server outside the **Demilitarized Zone (DMZ)**. No one should be able to modify or delete log information.

2.10 Log retention

All logs must be retained for a minimum of 90 days, and be retrievable in a timely manner.

3. Procedures

Log review must be completed according to the ARC log review procedures.

4. Responsibility

4.1 ARC Sensitive Research Team

Is responsible for investigating suspected or confirmed security or privacy incidents in REDCap.

4.2 ARC Platforms Team

Is responsible for monitoring **User** activity logs and project logs, taking appropriate corrective actions, including notifying Users.

5. References

ARCG-01 Glossary of Terms
ARCG-02 Glossary of Standards
UBC Information Security Standard M8 Logging and Monitoring of UBC Systems

Effective Date:	28-AUG-2019		
First Released:	28-AUG-2019		
Last Revised:	17-MAR-2023		
Last Reviewed:	22-MAR-2023		
Approved By:	ARC Management Team		
	22-MAR-2023		