REDCap
Security Statement

Version 1.0.0

THE UNIVERSITY OF BRITISH COLUMBIA

REDCap Security Statement

1. Introduction

This document summarizes the security architecture and controls of the REDCap instances managed by UBC Advanced Research Computing (ARC). For additional detail, please refer to the associated standards that govern the REDCap platform. For more information please contact redcap.support@ubc.ca

2. REDCap Software

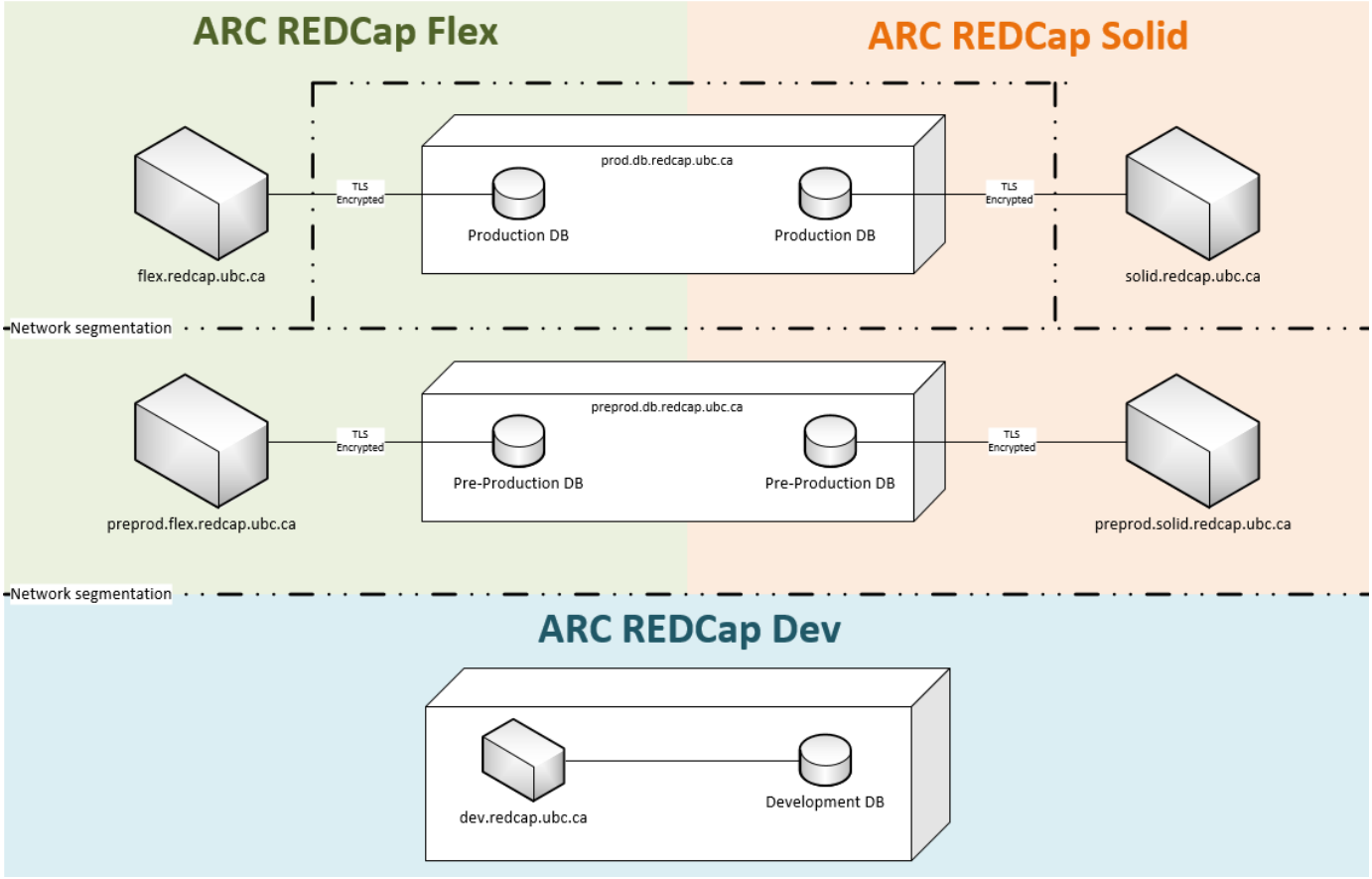
The REDCap software provided by the projectredcap.org developers is installed “AS-IS”. UBC ARC does not conduct any additional review of the software code provided. Release notes and change logs posted as part of the regular releases at projectredcap.org are monitored and urgent fixes and/or security patches identified will be prioritized to apply to the version available at the UBC ARC instances. For additional detail concerning the REDCap application in general please refer to: https://projectredcap.org/wp-content/resources/REDCapTechnicalOverview.pdf

3. Platform Architecture

All servers for the REDCap platform are located in British Columbia, Canada within the UBC University Data Centre: A modern secure data center with pass-card restricted and logged entry, generator-backed UPS protected power, and video surveillance.

The platform is deployed across multiple virtual machines to separate production, pre-production, and development; web application and database servers:

- Production web servers reside on a DMZ network protected by a next generation firewall. External access is only available over TLS (version 1.2 minimum) encrypted connections with Forward Security enabling cypher suites and HSTS enabled.
- Production database servers reside on a separate network segment and are not accessible to the external network. Connections between the web application server and database server are TLS encrypted.
- Pre-Production web and database servers are not externally accessible and are only accessible from the internal administrative network for testing purposes. Their configuration is otherwise identical to the production systems.



4. Access Control

For end users, the REDCap platform is integrated with UBC's Campus Wide Login (CWL) system as described in the *ARCS-12 REDCap Access Control* standard. Privileged accounts used to administrate the platform are limited to the UBC ARC team, must use encrypted SSH connections from the internal network to access platform servers and require multi factor authentication.

Users accessing the **REDCap Flex** instance have the option to use multi-factor authentication. The **REDCap Solid** instance requires multi-factor authentication for all **Users**.

5. Maintenance and Patching

To facilitate required upgrades and patches the REDCap platform has a pre-set maintenance window the third (3rd) Tuesday of every month between 1300h and 1400h Pacific Time. Users will be notified in advance when the window will be required in a given month. Upgrades and Patches will be performed in accordance with the *ARCS-13: REDCap Maintenance* standard.

6. Vulnerability Scanning

The REDCap Platform is periodically scanned using a variety of automated vulnerability scanning tools. Scans are conducted, at a minimum, in conjunction with annual maintenance cycles for each instance. Reports are reviewed and inform the maintenance and patching priorities for the platform in accordance with the *ARCS-13: REDCap Maintenance* standard.

7. Backup

Both instances of the REDCap platform follow the same general procedure for backups. A complete database extract is performed nightly; this extract is encrypted and maintained per the database retention schedule. In addition to this extract, the entire REDCap application server is also captured via a system snapshot, which is retained following the VM retention schedule. For further detail refer to the *ARCS-15: REDCap Backup* standard.

8. Data Retention and Destruction

8.1 Active Storage

Data stored on the platform will be managed in accordance with the *ARCS-05: Data Retention and Destruction* standard. Projects that have been archived will be subject to deletion after one (1) year. The **Project Owner** may request data destruction of a project for which they are responsible.

8.2 Backup Storage

No facility exists to request the deletion of data stored in backups of the REDCap platform. Data stored on backup systems will be deleted automatically based on the retention schedule defined in section 5.2 and as mandated by the *ARCS-15: REDCap Backup* standard.

Effective Date:	28-AUG-2019		
First Released:	28-AUG-2019		
Last Revised:	27-AUG-2019		
Last Reviewed:	28-AUG-2019		
Approved By:	ARC Management Team		
	28-AUG-2019		