

LexEVS 6.1 Information Systems Security Plan

Contents of this Page
- Information Systems Security Plan - A list of the industry standard security controls expected in this product - The components of the CBIIT technologies used for security controls - Any expected deviation from the standards

Document Information
Author: Craig Stancl Email: Stancl.craig@mayo.edu Team: LexEVS Contract: ST12-1106 Client: NCI CBIIT National Institutes of Health US Department of Health and Human Services

Sign off	Date	Role	CBIIT or Stakeholder Organization	Reviewer's Comments (If disapproved indicate specific areas for improvement.)
---	---	---	---	---
---	---	---	---	---
---	---	---	---	---

The **purpose of this document** is to document the security plan for the National Cancer Institute Center for Biomedical Informatics and Information Technology (NCI CBIIT) caCORE **LexEVS Release 6.1**.

Information Systems Security Plan

A list of the industry standard security controls expected in this product

- [HTTPS](#)  REST security (if needed)
 - Possible uses:
 - URI Resolver administration
 - CTS2 Development Framework administration
 - LexEVS REST secure ontology access/token transfer
- [RFC 2196](#) 
 - Specifically, section [3.1.2 Separation of Services](#) 
 - This architecture will allow services to be separated to those needing to be exposed externally and those that do not.
 - Services NOT to expose externally:
 - URI Resolver administration
 - CTS2 Development Framework administration

The components of the CBIIT technologies used for security controls

None

Any expected deviation from the standards

None