LexEVS 6.3 Information Systems Security Plan

Document Information

Author: Craig Stancl, Scott Bauer, Cory Endle
Email: Stancl.craig@mayo.edu, bauer.scott@mayo.edu, endle.cory@mayo.edu
Team: LexEVS
Contract: S13-500 MOD4
Client: NCI CBIIT
National Institutes of Heath
US Department of Health and Human Services

Contents of this Page

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) **LexEVS Release 6.3**.

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
  - Specifiically, 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