

SECURITY PLAN VERSION 1.0
NEBRASKA STATEWIDE COORDINATED DATABASE SYSTEM
November 25, 2003

This document pertains to security issues for the University of Nebraska Public Policy Center Nebraska Statewide Coordinated Database website. The University of Nebraska's Public Policy Center serves as the responsible owner of this database system and website.

Security of the statewide coordinated database information and hardware is important because the information must be credible and accurate.

Further definition of the security plan will be developed after the Project Manager begins work (December 1, 2003) at the Public Policy Center.

Architecture

The distributed database architecture, or batch system structure, will enable database owners to store data locally, and regularly connect through the Internet to a central server to send a copy of their database to a central data repository, where aggregate information will be stored.

A central server will be established for hosting services. The set-up of the server will accommodate future development and enhancements, including scalability (i.e., the robustness of the system) and flexibility (e.g., project-defined features and look) and supporting the ability to import and export data using the xml data translation standards. It is expected that a robust package (e.g., SQL, Oracle) will be implemented.

Centralized (permanent connectivity with full access rights to the Systems Administrator) or decentralized (which quickly grows unmanageable for more than just a few sites and may be organizationally cumbersome) architecture would not provide the economical, scalable solution to database owners' desire to manage their information locally. Internet connectivity will be used as it is less expensive and more reliable than creating an independent Wide Area Network (especially across the distances this project entails) and should minimize software requirements and avoid technical issues associated with installing software, fixing bugs, and providing other technical support.

Physical Security

The server will be housed in a limited access and climate-controlled facility. If the server is maintained by a vendor, one of the issues that we will require the vendor to specify is the physical security of the hardware. If approved by the Department of Commerce, and found in the best interests of the project, the Public Policy Center may decide to purchase and house the server and its component parts. The server will be logged as a part of the Public Policy Center's on-going inventory control system.

Data Security

The Public Policy Center will use a variety of safeguards to protect information from loss, misuse, alteration or destruction. Requisite passwording and security features will be implemented to ensure access to the coordinated database only by those with proper training and authority.

The distributed architecture will allow database owners the ability to share only designated database elements, and maintain other elements for their agency use only.

Data Accuracy

Processes will be developed for urgent updating (e.g., license revocation of a child care provider) and for removing resources (e.g., a provider chooses not to be included).

This document is supplemented by relevant policies and procedures established by the University of Nebraska:

- General Privacy Policy (As approved by the Faculty Senate – January 2003) at <http://www.unl.edu/is/about/UNLprivacy.pdf>
- Executive Memorandum No. 16, Policy for Responsible Use of University Computers and Information Systems at http://www.nebraska.edu/about/exec_memo16.pdf