

Appendix F, Section 2

Web-Enabled Data Repository: Test Phase

Agency:

Department of Children, Families and Learning (DCFL)

TIS Evaluation Meeting Date:

2 June 1999

State Archives Staff:

Mary Klauda, Shawn Rounds

DCFL staff:

Mark Manning, Theresa Mish, Mary Lillesve, Michael Riecken (Signature Software contractor)

Agency Function:

To help communities measurably improve the well-being of children through programs that focus on education, community services, prevention, and the preparation of young people for the work environment. Department efforts emphasize achieving positive results for children and their families. Its programs address family breakdown, violence, and poverty. The department strives to make accessible its educational and community resource services and encourages collaboration between state education professionals and social services advocates in order to meet the needs of Minnesota's children and families.

System Name:

Minnesota Electronic Curriculum Repository (MECR)

System Function:

The MECR is a quality-controlled database of curriculum materials that supports the implementation of the Minnesota Graduation Standards. The repository contains information on content standards, scoring criteria, large processes and concepts, state model performance packages, assessment tasks, learning activities, and other learning resources. The primary users of the MECR are teachers and other educational professionals (e.g., administrators, curriculum developers, technology specialists, counselors) seeking high-quality curriculum materials to design and deliver instruction for the standards. Other users might include parents, students, policy makers, legislators, and in-service teacher training program staff. Access primarily is web-based and available at: <http://mecn.state.mn.us/home> [NOTE: As of 2003, MECR and this URL are no longer active].

System Development Phase:

Operational as of 1 June 1999

Background:

DCFL is responsible for development of the MECR. The system was planned and developed as a way to better implement and disseminate information about the Minnesota Graduation Standards. The MECR also will allow for efficient and timely updates of curriculum guidelines as graduation standards are updated by the Legislature.

The MECR is available to school districts via the Internet and CD-ROM. The CD-ROM version includes Java Runtime, a mini web server, an Internet browser, the entire contents of the database, source code, documentation, and executables. There currently are no version-tracking procedures. Software will be updated as the system warrants.

Users can create assessment tasks, learning activities, and learning resources based on the MECR once user accounts are established. School districts can change the curriculum to suit individual district goals, but after having done so, districts are responsible for curriculum content and implementation. The system does not support random changes. However, new curriculum information can be submitted for approval and inclusion to the MECR.

Prior to the MECR, the official version of state curriculum guidelines existed in paper formats. Most of the data in the MECR is new content. Once the system is operational, the electronic version will be considered the official record. State models and rules that serve as background for the MECR will remain in paper formats; policy documents for the MECR are in both paper and digital formats.

The MECR is subject to Minnesota Statutes, Chapter 3501, which established the Graduation Standards. The Data Practices Act (Minnesota Statutes, Chapter 13) does not apply to the system since none of the system data is about individuals. However, since individuals set up user accounts to log on to the system, data practices issues may pertain to the log-on information. This may require further investigation.

Records retention requirements for MECR data have not been fully identified. Permanent retention of any graduation standards information has yet to be addressed. Retention may be based on graduation years and/or updates of graduation standards. Plans are in place to have snapshots of the system data for graduation standard years.

MECR staff thought it would be a good idea to retain snapshots of the web presentation of the MECR for historical purposes. The system has some capture mechanism, and CD-ROMs may be a viable means for retaining snapshots.

During the initial stages of system development, the MECR web pages were hosted by Signature Software. The site will move to DCFL soon after the system is operational.

System Documentation:

DCFL does not have an agency-wide methodology for all aspects of system documentation. For the MECR, system operating procedures currently are in development. New entries are tracked in a log that records creators, dates of creation, and whether or not the new entries are approved. Design reviews and system tests were performed and documented before the MECR went into

production. Maintaining audit trails of hardware and software changes may be considered in the future. There is an archive of all software. No one is able to make changes to the system without going through a change-request procedure followed by a review process.

DCFL has documentation on the procurement and installation of MECR's hardware. Hardware is self-installed by staff and installation procedures are outlined. There have been no hardware modifications on the MECR to date, although the physical location of the system will be changing and that move will be documented. Future issues of hardware maintenance need to be addressed, specifically issues of cost and staff responsibilities. Documentation exists, or will exist, on the procurement, installation, modification, and maintenance of the system software. DCFL, as an agency, is finalizing a policy about use of agency-authorized hardware and software, and the MECR will be subject to the terms of that policy.

The MECR is connected to the communication network infrastructure at DCFL. DCFL documents all network procurement, installation, modifications, and maintenance. The Internet is the only means of external system access to the MECR, and it is the system's main connection with school districts. School districts can choose to install MECR onto their own network systems off CD-ROM through a documented installation procedure.

System Documentation—Policy and Procedures:

System documentation includes conventions and procedures for developing, programming, and testing. Periodic functional tests are performed that are basically self-testing routines for objects before they are plugged into the system; the tests are not documented thoroughly. There is user documentation on applications and associated procedures for entering and accessing data in the MECR. There is database documentation only for the initial raw data entry. There are applications and procedures for internal indexing of the database, but no indexing for external systems data. System output, namely the web user interface, is documented.

System documentation includes record formats and codes for the database and procedures for identifying when system records become official. Additions to the MECR must be approved by a review authority and new entries are considered works-in-progress while they are under review. Records become official after review, approval, and publication. This is the only quality-assurance and control-check on system data. There is a mechanism for routine performance of system backups, but documentation on this is not complete. Backups are stored in secure, off-line, off-site storage; there are no integrity tests performed on backups. Storage mediums do not regularly undergo statistical sampling in order to identify data loss and corresponding causes, however MECR staff felt that this was an important consideration for the future. System documentation does not include plans for migration of records to new systems and media. There is an installation guide designed primarily to assist school district systems administrator in installing the MECR on different systems. User documentation and training on the MECR for mid-level administrators is available.

System Security—User Authorization:

Information in the MECR is public, and DCFL wants the public to be able to easily access system data. To promote access, there is a generic user account for people who wish to access the MECR, but who do not want to identify themselves. These users have limited read-only access and can print any public data.

Some users must be authenticated prior to being given access to certain areas of the system, and identification and access procedures for these people have been established and documented. Although each user has a unique identifier and password, there is no way for DCFL to monitor sharing of identifiers and passwords. User names and user identifiers are unique; passwords are not guaranteed to be unique. There is no means to control the use of access scripts and embedded passwords on the client-side of the system. The system terminates individual user sessions after a certain time period of inactivity. Password rules include a minimum password length, but do not establish expiration dates or a maximum number of log-on attempts.

A help desk responds to any security incidents. System security administrators approve access for users. There are no formal procedures in place to ensure that user access corresponds to the level of access necessary to perform job functions. Staff positions have not been reviewed to ensure that they have been assigned appropriate security levels. MECR staff thought that there should be such procedures in the future. Permissions to create, modify, and delete records are granted only to authorized users with proper clearance. Modification of record identifiers is prohibited. Permissions are assigned to user groups rather than individual users. DCFL maintains lists of all current and past authorized users, but lists do not include corresponding privileges and responsibilities. These lists are not reviewed regularly to make adjustments for removal of former employees or clearances for workers with new job duties, but MECR staff felt that some method of review should be implemented.

System Security—Internal:

MECR staff felt that issues of access to all systems documentation need to be addressed by DCFL as an agency. For the MECR, system output and storage devices are in a locked, controlled-access facility. There are controls to ensure security while data is being archived or moved, and procedures have been established for moving system backups to off-site storage. The DCFL information systems office has procedures for, and documentation on, the sanitization and disposal of all agency software and storage media when no longer needed. There are no procedures for sanitization and disposal of obsolete hardware, nor any policies addressing re-use of software, hardware, or storage media. There currently is no online insecurity-detection mechanism, but this issue will be addressed in the future. MECR staff felt that there should be a better process to minimize failure of primary security measures and more timely review of security procedures and rules. Various safeguards maintain the MECR's physical security. Plans are underway to train security administration personnel, ensuring their complete knowledge of MECR's security system.

System Security—External:

There are security measures relating to remote access to the MECR via the Internet; there are no direct telephone connections to the MECR. Non-system records and data are not imported directly into the MECR. Verification of the sender/source, origin, and integrity of non-system

records takes place through the approval process. After approval, records/data are entered into the system. There currently is no means to detect viruses on non-system records. MECR staff felt that there should be an automatic mechanism to scan the system on a routine basis.

Audit Trails:

The MECR does not have traditional audit trails. Two forms of access logs are maintained instead: access logs as a function of the web server and internal access logs in the database that includes incoming URL information. Status logs for records in the database are maintained, but they are overwritten so that only the most current status is available. Anyone with access to directories on the server can access the audit data. Ideally, this information should be available only to the database or system administrator. Access logs are backed up on the same schedule as the rest of the system. A system logs and tracks users, noting user identifiers, record identifiers, dates, times, and types of usage.

Disaster Recovery:

There is no disaster recovery plan, but there is recognition by DCFL information systems staff of the need.

Record Data:

Data in the MECR is considered an official record only after it has gone through the approval process. Components of a complete or final record depend on the record type. Generally, record components include type and identifier, creator, current status, status date, and record information. MECR data is not considered transactional. Upon approval, the original content, format, and structure are preserved, and each record can be printed or represented as it originally appeared at time of official acceptance. Record data, documents, and metadata are not accessed, displayed, and managed as a unit. MECR staff will need to define a records disposition plan for the MECR, as well as determine who is responsible for authorizing and altering that policy.

Record metadata includes unique identifiers, dates of creation, creator and documentation of creator's authorization, date and time of modification (i.e., server date and time), modifier (individual or organization) and documentation of modifier's authorization, and indication of authoritative version. The media type is always the network, the format is always keyed-in internally, and the location of record is always within the database.