Identity Access Management (IAM) for MNLARS

Data Practices Commission meeting
Tuesday, November 25, 2014

MNIT SERVICES
Information Technology For Minnesota Government

Identity Access Management is a top priority for the MNLARS project. Users gaining access to MNLARS will be limited to certain data elements needed to perform their job functions. During all business requirements sessions, access to data is specifically planned and documented.

New roles have been created to manage oversight and access to MNLARS. These roles are:

Data Practices Representative (DPR): the DPR is a role within DVS that:

1. Reviews and approves users agreements
2. Determines access levels based on roles
3. Conducts audits for purposes of access (all queries are electronic and captured for audit purposes)
4. Controls hours of access
5. Approves access, if a DUR is not available
6. Suspends, terminates, and/or changes access, as needed.

Access unit – business partner to DVS such as a deputy register

Data Use Representative (DUR): the DUR is the contact at the access unit level. Their role is to:

1. Verify personal data of new users and approve access
2. Manage ongoing access for their specific users
3. Ensure annual DVS training is conducted
4. Assign access based on user roles
5. Conduct quarterly audits to verify their user list
6. Temporarily suspend for internal business practices such as leave of absences.

All approved MNLARS data users are required to create a user profile containing specific personal information. This information includes: full name, address, DL number, and phone number. All new access units are required to submit a User Agreement which is assigned an agreement number. Users are granted access based on the terms and permissible uses specified in the user agreement.