Responsible Use of University Directory Service (UDS) Data Policy
The University of Wisconsin-Madison

Background

The UDS provides applications and services at the University of Wisconsin-Madison with demographic, role and contact data to support identity management, authentication and authorization.\(^{(i)}\) The following policy is designed to ensure judicious and compliant use of that information, protecting the security and privacy of that data where necessary.

Policy

1. UDS data use must be authorized by the appropriate data custodians for student, employee or other data using the UDS authorization request form. This form specifies what data elements are needed for what purpose. UDS consumers\(^{(ii)}\) will be notified annually to reapply for authorization. The data obtained must be used only for the specific purpose identified on the request form and not for any other purpose, and must not be supplied to other applications.

2. UDS data use must comply with the applicable State of Wisconsin and Federal laws and regulations concerning privacy and security as well as complying with University policy. UDS data use is specifically bound by the University FERPA Policy (https://registrar.wisc.edu/ferpa_overview_fac.htm) and University Responsible Use Policy (https://kb.wisc.edu/itpolicy/cio-responsible-use).

3. UDS data may be used for purposes of providing identity management, which includes, for example, directory authentication and authorization services, and contact information.

4. UDS consumers must provide details on what UDS data they store locally.

5. UDS consumers must take all necessary precautions to secure UDS data in transmission and in storage. This includes utilizing security best practices as posted at https://it.wisc.edu/about/office-of-the-cio/cybersecurity/.

6. Consumers of UDS data will be held responsible for any security breach traceable to their use or specific authorization and will be held liable for any willful misuse or deliberate system damage traceable to their use and specific authorization.

7. Periodic and random audits will be performed on use of UDS data by the Office of Cybersecurity.

8. Consumers of UDS data must provide access logs and access to systems containing UDS data upon request to the Office of Cybersecurity.

\(^{(i)}\) Identity management refers to the policies, processes and technologies by which the identities of persons are proofed, registered and maintained. Authentication is the process of validating that identity. Authorization is providing access rights and privileges based on that identity.

\(^{(ii)}\) UDS consumers refers to applications or services that use data from the UDS.
Authority
Issued by the UW-Madison Vice Provost for Information Technology.

Enforcement
See provisions 6, 7 and 8 of the policy.

Contact
Please address questions or comments to policy@cio.wisc.edu.

References
IT Policy Glossary: https://kb.wisc.edu/itpolicy/glossary