Password Policy

Policy

Devices and systems connected to the University of Wisconsin-Madison network must require passwords meeting the minimum standards set by the Office of the Chief Information Officer and, if possible, technically enforce them. Faculty, staff and students must adhere to the minimum passwords standards for all systems and applications that come into contact with University resources.

Systems That Cannot Comply with Minimum Standards

If the minimum standards cannot be met, the system must be protected by other means, such as, but not limited to, a dedicated firewall, limited network access or multi-factor authentication.

Background

The University of Wisconsin-Madison’s network and information systems provide the technical foundation for conduct of its academic, research and administrative missions. Providing this open access to information technology is imperative to ensuring academic freedom at the institution. An important part of providing this network access is ensuring that the network and associated information is secure.

The purpose of this policy is to provide guidance to faculty, staff, students and other authorized users regarding passwords in order to protect individual and University information and resources. Adherence to this policy will help ensure that the university network and information systems are secure and available to all.

Authority

Issued by the UW-Madison Vice Provost for Information Technology.

Enforcement

The University reserves the right to:

- suspend access to preserve the confidentiality, integrity and availability of the network, systems or information;
- periodically audit passwords for compliance; and
- pursue disciplinary action because of non-compliance.

Contact

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

References

IT Policy Glossary - https://kb.wisc.edu/itpolicy/glossary
Password Standard

Background

The following standards have been developed in concert with the university community and established by the Office of Cybersecurity.

Requirements

- Passwords chosen must:
  - be a minimum of eight (8) characters in length;
  - be memorized; if a password is written down it must be secure;
  - contain at least one (1) character from three (3) of the following categories:
    - Uppercase letter (A-Z)
    - Lowercase letter (a-z)
    - Digit (0-9)
    - Special character (~`!#$%^&*()+=_{}[]\'|;:"'?/>.,);
  - be private;

- Passwords chosen must not:
  - contain a common proper name, login ID, email address, initials, first, middle or last name.

Recommendations

- It is strongly recommended that:
  - passwords are changed twice per year (e.g., when clocks are adjusted in the spring and fall);
  - each password chosen is new and different.

Contact

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

References

Password Policy - http://kb.wisc.edu/itpolicy/cio-password-policy
IT Policy Glossary - https://kb.wisc.edu/itpolicy/glossary

Password Standard Reference at: https://kb.wisc.edu/itpolicy/cio-password-standard
Effective: Feb 17, 2006 Revised: Feb 17, 2006, RevB History at: https://kb.wisc.edu/itpolicy/cio-password-history
Reviewed: Mar, 2015 Review in: Two years Maintained by: Office of the CIO, IT Policy

Copyright © 2006 Board of Regents of the University of Wisconsin System