Ohio Administrative Code

Rule 3337-91-04 University credentials.

Effective: June 24, 2016

The version of this rule that includes live links to associated resources is online at

https://www.ohio.edu/policy/91-004.html

(A) Overview

Credentials issued at Ohio university are for the sole purpose of accessing university resources. They are often the first line of attack, and the last line of defense, in the protection of these resources. Because of this, they must be used with care, and adequately protected. This policy outlines those protections that must be observed by individuals, technical staff, and systems using credentials at the university and recommendations for their protection.

(B) Individuals

An individual to whom credentials have been issued has certain responsibilities in the care of those credentials. The following behaviors should be observed to reduce the risk of compromise to your credentials.

(1) Keep your credentials, secret questions, and their answers private and known only to you.

(2) Use unique credentials (username and password combination) for Ohio university that are different from any other service or website.

(3) Your credentials are for your personal authentication to university resources, and should not be used as a means to provision services to other users.

(4) If you suspect that your credentials have been compromised, change your credentials and questions immediately and inform the information security office by e-mail to security@ohio.edu.

(C) Credentials

Credentials exist to ensure that the individual gaining access to university resources through an account is the same individual to whom the access was given. The university acknowledges that not all accounts carry the same level of risk. Therefore the level of rigor and complexity requirements that are applied to ensuring the security of the credentials will be in line with the risk which a compromise of that account would present to the university or its community.

The university data stewards (see part (D) of policy 93.001) will review these complexity requirements on an annual basis. Any changes that need to take place between reviews will be identified by the university information security officer, and presented to the university data stewards for approval. Actual authentication complexity requirements will be captured in the "Authentication Credentials Complexity Standard," which strives to relate the strength of the credential with the risk that a compromise of that account would present to the university.

(D) Information system owners

It is the owner or manager of information services' responsibility to ensure that they comply with this policy and its associated complexity requirements. The recommended method is integrating with OIT authentication services and appropriately mapping individuals' accounts to the correct risk levels. Prior to integrating with OIT authentication services, permission must be obtained from the university information security officer and the chief information officer or their delegates. If a separate user credential is issued, the service owner must instruct their users to use different credentials than are used with their OhioID.

(E) Authentication servers

University authentication services are limited to those run and maintained by the office of information technology. It is the responsibility of the chief information officer or appointed delegate to ensure that the following are adhered to by all systems that perform authentication functions.

(1) Only those systems that are required and approved by the chief information officer or appointed

delegate may store passwords in any form. Those that store these passwords must store them in a cryptographically secure format.

(2) Authentication systems must encrypt password at all times during transmission.

(3) Authentication systems must be housed in the university datacenter or another approved location. Authentication systems must be administered by OIT.

(4) Authentication systems must be hardened in accordance with NIST 800-123.

(5) Administrators accessing authentication systems must use an approved multi-factor authentication to access.

The version of this rule that includes live links to associated resources is online at

https://www.ohio.edu/policy/91-004.html