Unique Identifiers

Date: 08/22/19 rev.	**Policy ID:** UVAW - 7	**Status:** Approved

Contact Office: Office of Information Technology

Oversight Executive: Director of Information Technology

Applies to: Every person with computing access on the UVa-Wise network(s)

Reason for Policy: To ensure authentication and provide a secure computing environment to insure the confidentiality, integrity and availability of College resources.

Definitions:

Policy Statement: Best practices dictate the use of individual identifiers to gain access to College resources i.e. computers, servers, databases, e-mail, etc. Following these best practice procedures enables users to better utilize the resources available while minimizing the risks inherent in digital technologies. The protection of College resources is not a responsibility to be taken lightly and while it is necessary to allow access to sometimes sensitive information needed to perform job functions etc. It is imperative that controls over that access be maintained.

Procedures:

1.0 Every person with computing access will have a unique ID
- 1.1 All potential employees/contractors who will access sensitive/critical data must pass a background check.
- 1.2 Limit/control access and contractually require all third parties with access to sensitive/critical data to adhere to applicable industry security requirements and standards.
- 1.3 All potential employees/contractors who will access sensitive/critical data must pass a background check.
- 1.4 Limit/control access and contractually require all third parties with access to sensitive/critical data to adhere to applicable industry security requirements and standards.
- 1.5 All users will be identified with a unique username before allowing them access to computer resources.
  - 1.5.1 The College is working toward methods and equipment that will require this identifier even on public access machines.

1.5.2 All systems storing and/or handling sensitive data must require unique usernames and sharing of usernames and/or passwords is absolutely prohibited.

1.5.3 A warning screen must be displayed that requires user acknowledgement and identifies the computer system as a UVa-Wise and/or VA system protected by law, notification of monitoring, no expectation of privacy, and unauthorized access is subject to disciplinary action and legal prosecution.

1.6 In addition to the unique username, a password, token device, or biometric is required.

1.7 During transmission and storage on all communication systems and system components passwords must be encrypted.

1.8 Administrators of systems storing sensitive data must use some method of user identification verification before resetting passwords.

1.9 First-time passwords and password resets will be set to a unique value and will be required to change at first logon.

1.10 Users who no longer need access to data will have access revoked immediately.

1.11 E-mail and web share account users who are no longer associated with the College shall be removed at the start of the next fall or spring semester.

1.12 Group and shared passwords are not permitted on any College system.

1.13 Systems should require user passwords be changed at least every 90 days. Sensitive User ID's, such as system administrators, and information security professionals shall change their passwords every 60 days.

1.14 Passwords shall no less than eight (8) characters and will conform to complexity rules. (Passwords should contain upper- and lower-case letters, at least one number and at least one special character.)

1.15 Password history will be enforced for previous twenty (20) passwords.

1.16 Passwords attempts are limited to ten (10) attempts and then locked out for twenty (20) minutes or until an administrator enables the user ID.

1.17 If a session has been idle for more than 15 minutes, the user must be required to re-enter the password to re-activate (access) the workstation, server or other device.

1.18 Access to any database containing sensitive data must be authenticated.

Related Information: See also Authentication of Users Policy PCI – 8 and Choosing Good Password guidelines at http://www.uvawise.edu/oit/security/good_passwords.html

Background: Approved by Brian Ward, CIO – UVa-Wise, June 12, 2006
Revised to bring policy in line with current standards – 08/22/19
