University at Buffalo Password Policy

Summary

University at Buffalo (UB) relies upon the use of university-provided digital credentials – for example, your UBITName and password – to provide authentication for access to UB online IT resources and information. Passwords constitute a first line of defense to protecting access to university information and information systems. Any compromise of authentication credentials used by the university community impacts the confidentiality and integrity of university IT systems and information. Users are required to create strong passwords and secure and to protect their university passwords.

Policy

POLICY STATEMENT

Individual Accountability: All users of university systems are individually assigned a user-id (e.g., UBITName) and password for the purpose of accessing UB online systems. In accordance with UB “acceptable use policies,” users are individually accountable for activities performed with their user-ids and passwords. Passwords may not be shared with anyone, including with administrative assistants or secretaries. UB passwords are considered to be regulated, private data.

• Do not reveal a password over the phone to anyone
• Do not reveal/include a password in an email message
• Do not reveal a password to your supervisor, manager, or co-workers
• Do not talk about a password in front of others
• Do not fall for phishing scams that attempt to get you to reveal your password or other personal information
t  • The University of Buffalo and legitimate businesses will never ask you to reveal your password in unsolicited email messages or telephone calls to you
• Do not use the “Remember Password” feature of applications

Password Security: Passwords for UB systems should not be identical to those used for personal/non-UB online accounts.

Password Strength Requirements: User and system passwords shall be constructed with strength and complexity that minimize the likelihood of successful password guessing or brute force attacks. Passwords with strength and complexity must have the following characteristics:

• Between 8 and 32 characters in length
• Must contain at least
  • One lowercase character (a-z)
  • One uppercase character (A-Z)
  • One numeric character (0-9)
  • One non-alphanumeric character from this set: !#$%&'()*+,-./:;@

Category: Information Technology
Responsible Office: Enterprise Infrastructure Services
Responsible Executive: Vice President and Chief Information Officer
Date Established: 4/29/2008
Date Last Revised: 11/01/2013
Date Posted to Library:
• Have no more than two pairs of repeating characters, such as “aa”
• Cannot be an old password used within the past 365 days

Good passwords must be easy for you to remember. To create passwords that can be easily remembered, use the basis of something you know well, such as a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

**Password Refresh** (Aging): Passwords shall be refreshed periodically to reduce the impact of disclosure due to undetected theft of passwords. Passwords must be changed on a more frequent basis that depends on the risk to the information being managed, processed, or stored. If the account credentials of a user or system are suspected to have been disclosed or otherwise compromised, the user shall take immediate steps to change and protect the password.

• All passwords should be changed at least once every semester
• Passwords for users with access to non-public University data/information must be changed every 180 days.
• Passwords for users with access to regulated private data (including credit/debit card data, social security numbers, state-issued drivers’ license and non-drivers’ identification data, and protected health information) must change their passwords every 90 days.

**System Requirements**

• **Transmission of User-ids and Passwords:** ISO 27001/17799 security standards, Payment Card Industry (PCI) standards, and NIST and other security organization standards prohibit clear text transmission of user-ids (e.g., UBITNames) and passwords. UB adheres to these standards and prohibits transmission of user-ids and passwords in clear text.

• **System-based Password Files:** UBITName: The use of system-based password files raises the risk that a compromised system will expose the password file to dictionary/rainbow table attacks. UBITName passwords should not be distributed to system-based password files. In cases where this is not possible, additional security protections and periodic audits must be implemented to reduce the risk of unauthorized access to the password file. Password processing should always use an off-system password verification process based on Kerberos. (Windows AD and LDAP use Kerberos.)

• **Auditing and Testing:** UB passwords should periodically be run through standard password tools to ensure that the password strength-checking done in the password reset facility is still effective and meets the standard for length specified in this policy.

• **Access Control:** Access to systems which do not use the UBITName for access control should be reviewed regularly, and access for individuals should be removed when they no longer meet the criteria for which they were granted access. Termination of employment, retirement, and job duty changes are just some of the reasons that access may no longer be appropriate. Access can be removed by the system/application administrator changing the account password or removing the userid.

Systems that do not use UBITNames for authentication/authorization and which do not have a tie to an automated process for userid disabling after separation from the
University should be reviewed for possible inclusion in the UBITName system or have some automatic account disablement implemented.

At a minimum, monthly reviews of access should be performed for all systems handling sensitive data, regardless of their authentication method.

- **Third Party Use**: The use of UB authentication directly or indirectly by an off-campus entity or other third party is explicitly prohibited without the approval of the UB Information Security Officer.

**BACKGROUND/REASON FOR POLICY**

The purpose of this policy is to establish minimum standards for the protection, complexity, and refresh interval for University passwords. The application of individual accountability and the principle of least privilege are applied in this policy.

**APPLICABILITY**

This policy applies to all users who have user and/or system accounts in any IT systems that interface with UB authentication systems.

---

**Contact Information**

**Responsible Office:**
Office of the CIO
517 Capen
University at Buffalo
716-645-7979

**Procedures:**
Information Security Officer
Office of the CIO
517 Capen
University at Buffalo
716-645-7979
sec-office@buffalo.edu

**Related Information**

**University Documents:**
[UB Computer and Network Use Policy]