



Request for Comments: Draft Password Policy

(Updated 4.29.2008)

1.0 Introduction

This policy establishes University password requirements for UB IT and departmental IT accounts. These requirements are necessary to help ensure personal security, to protect University business, research, and academic interactions, and to meet information security legal requirements and standards.

Passwords are often the weakest link in securing data due to the creation and use of weak passwords, the proliferation of automated password cracking programs, and the activities of malicious hackers and spammers. This policy provides guidance on creating and using passwords in ways that maximize password and information security.

2.0 Scope

This policy applies to anyone accessing systems that hold or transmit University at Buffalo data and includes departmental and central IT accounts and resources.

3.0 Policy

All University passwords must follow University at Buffalo password standards. In general a password's strength will increase with length, complexity, and frequency of changes. Stronger passwords are required for high-risk systems, such as those that provide access to critical or the most sensitive, private, regulated data.¹

4.0 Password Standards

4.1 Individual Responsibilities

Passwords for newly activated IT accounts must be changed at first use in order to ensure that only the person who has been assigned the account knows the password. IT Account owners are expected to comply with UB's [Computer and Network Use Policy](#).

In addition, IT Account owners are expected to do the following.

- Password Selection and Protection
 - Passwords should be strong and carefully protected as described in [CERT](#)

¹ Private, regulated data include the following: (1) Social Security Numbers, (2) bank credit/debit card or other financial account numbers, (3) state-issued driver's license and non-driver's identification numbers, and (4) protected health information. The [NY State Security Breach and Notification Act](#) requires that state entities notify residents and non-residents of any breach of their private, regulated data. NYS offices must be notified as well.

[recommendations](#). Passwords should be a minimum of 8 characters. The use of longer passwords or passphrases is recommended if the system you are using supports them. A passphrase is a longer version of a password and is typically composed of parts of multiple words. A good passphrase also contains a combination of upper- and lower-case letters, and numeric and punctuation characters

- Passwords should be protected and should not be written down and left in your desk or on your computer system. Protect them as you would protect other personal information such as your bank account PIN and other private information.
 - Do not share your passwords with anyone. Any attempt to encourage you to share your password should be reported to the UB Information Security Office. The only exception to this rule is for passwords for special operational accounts which represent functional campus services such as bursar, provost, registrar accounts. Do not use a UB password and username for any non-UB system or application.
- [Password Changing and Aging](#)
 - Periodically changing your password each semester is a recommended best practice, and is required whenever you have reason to believe that your password has been revealed. For example, if you have entered your password on a computer system you suspect has been compromised, it is required that you change your password.
 - The University will implement specific password aging and resetting, as well as system automatic lock-out requirements in alignment with the level of assurance standards that will allow UB to fully participate in federated authentication and authorization communities, such as InCommon and federal government groups. Password aging will be put in place on central UB IT systems by July 1, 2008.

4.2 System Requirements

- [Automatic Lock-out](#)

Automatic password lock-out, after a limited number of unsuccessful login attempts, is highly recommended, but not required at this time. Automatic password lock-out has a high return on investment according to Gartner and other security experts. The number of attempts should be set high enough to prevent easily triggering the lock-out, but low enough to minimize the chance that automated password cracking attempts will be successful. It is recommended that automatic lock-out removal after a reasonable period measured in minutes also be implemented to reduce the support cost and denial of service impact of automatic lock-outs. After January 31, 2009 automatic lockout will be required on central UB IT systems.

- [Transmission of UB User-IDs and Passwords](#)

Some applications currently in use at UB allow user-ids and passwords to be transmitted over the network as clear text. The ISO 27001/17799 security standards, Payment Card Industry standards, and NIST and other security organization standards prohibit clear text transmission of user-ids and passwords. After December 31, 2008, all transmission of UB IT Names and Passwords in clear text will be prohibited.

- [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.)
 - *Other*: For non-UBITName accounts, access to a system's password file should be prevented by all possible means since acquiring the password file on most systems permits harvesting of accounts and passwords regardless of the encryption technique used.
- [Auditing and Testing](#)

The Information Security Officer may periodically request that password files be processed using standard password cracking tools for servers supporting all enterprise-wide services. Weak passwords should be reported to the owner and the Information Security Officer.

UB passwords should periodically be run through new and existing 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 document.

- [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 by which they were granted access. Termination of employment, retirement, and job duty changes are just some of the reasons why 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 agreement of the UB Information Security Officer.

5.0 Contacts

Please contact the following office if you have questions or comments about this policy and procedures:

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