Ibn Sina University
Password Policy

Purpose

This Policy has been compiled to define the base level Password requirements for use within Ibn Sina University (ISU). The policy demonstrates ISU's commitment to information security and its proactive approach for addressing risks within the campus.
One of the vital components for an organisation to operate a secure and controlled information systems environment is the deployment of approved security mechanisms that support its security services (identification and authentication, access control, data integrity and confidentiality). One of the key mechanisms is the definition and implementation of a uniform Password Policy throughout the organisation. Any deviation from the Password Policy defined herein, will require prior written approval of the Director of Information Systems Services (ISS).

Scope

The Password Policy applies to all accounts used to access ISU ICT resources. The Password Requirements defined in this document apply to all systems that have the facilities to cater for them. Where systems do not have the facilities to cater for the Password Requirements then alternative requirements, on a case by case basis, can be implemented with the prior approval of the Director of Information Systems Services.

Ownership & Implementation

Whereas this Password Policy document is owned by the University, it will be maintained by the Director of Information Systems Services in consultation with the IS Governance Committee and other relevant areas within ISU.
The custodians of individual systems, servers, workstations, desktops and other devices are responsible for the enforcement of the Password Policy.

Password Requirements

Minimum Password Length

Passwords should be easy to remember but hard to guess, so passphrases should be used instead of traditional passwords. The length of passwords must always be checked automatically at the time that users construct or select them. All passwords must have at least fourteen (14) characters.

Passwords Must Not Be Reused

Users must not construct passwords, which are identical or substantially similar to passwords that they had previously employed. On all multi-user machines, system software or locally developed software must be used to maintain an encrypted history of previous fixed passwords. This history file must be employed to prevent users from reusing fixed passwords. The history file must minimally contain the last four (4) passwords for each user-ID.

Password Expiration

Password expiration should be enforced on all accounts. The expiration period for user passwords should be set to 12 months after which the user should be forced to change the password before any other work can be performed.

Consecutive Unsuccessful Login Attempts

To prevent password guessing attacks, the number of consecutive attempts to enter an incorrect password must be strictly limited. After five (5) unsuccessful login attempts, the account must be locked for at least one hour or until it is reset by a system administrator.

Difficult-To-Guess Passwords

All user-chosen passwords for computers and networks must be difficult to guess. Derivatives of user-IDs, and common character sequences such as "123456" must not be employed. Likewise, personal details such as spouse's name, vehicle license plate, PPS or social security number and birthday must not be used unless accompanied by additional unrelated characters.

Cyclical Passwords

Users are prohibited from constructing fixed passwords by combining a set of characters that do not change, with a set of characters that predictably change. In these prohibited passwords, characters that change are typically based on the month, a department, a project, or some other easily-guessed factor. For example, users must not employ passwords like "X34JAN" in January, "X34FEB" in February, etc.

System-Generated Passwords

If system-generated passwords are used, they must be generated using the low order bits of system clock time or some other frequently changing unpredictable source.

Storage of System-Generated Passwords

If passwords or Personal Identification Numbers (PINs) are generated by a computer system, they must always be issued immediately after they are generated. Regardless of the form they take, un-issued passwords and PINs must never be stored on the involved computer systems.

Assignment of Expired Passwords

The initial passwords issued by a security administrator must be valid only for the involved user's first on-line session. At that time, the user must be forced to choose another password before any other work can be performed.

Password-Based Boot Protection

All workstations, no matter where they are located, must use an access control system approved by the ISS. In most cases, this will involve screen-savers with fixed-password-based boot protection along with a time-out-after-no-activity feature.

Display and Printing of Passwords

The display and printing of passwords should be masked, suppressed, or otherwise obscured so that unauthorized parties will not be able to observe or subsequently recover them. This includes, and is not limited to, passwords written on a piece of paper, where the paper might or might not be stored in a secure (under the keyboard, inside a drawer, in purse or wallet, etc.) location.

Protection of Passwords Sent Through the Mail

If sent by regular mail, e-mail or similar physical distribution systems, passwords must be sent separately from user-IDs. These mailings must have no markings indicating the nature of the enclosure. Passwords must also be concealed inside an opaque envelope that will readily reveal tampering.

Encryption of Passwords

Passwords must always be encrypted (non-clear text) when held in storage for any period of time (backup media, batch files, automatic log-in scripts, software macros, etc.) or when transmitted over networks. This will prevent them from being disclosed to wire-tapers, technical staff who are reading systems logs, and other unauthorised parties. Passwords assigned by an administrator for a particular account (initial account creation, or password resets for existing accounts) and systems used for account management are excluded from this specific requirement.

Prevention of Password Retrieval

Computer and communication systems must be designed, tested, and controlled so as to prevent both the retrieval of, and unauthorised use of stored passwords, whether the passwords appear in encrypted or unencrypted form.

Incorporation of Passwords into Software

To allow passwords to be changed when needed, passwords should not be hard-coded (incorporated) into software developed or modified by ISU employees or third parties.

System Access Control with Individualized Passwords

Computer and communication system access control must be achieved via passwords, which are unique to each individual user. Access control to files, databases, computers, and other system resources via shared passwords (also called lockwords) is prohibited, unless permission is obtained from the Director of Information Systems Services who will consult with relevant members of staff.

Passwords for each internal/external Network Device

All ISU network devices (routers, firewalls, access control servers, etc.) should have passwords or other access control mechanisms. A compromise in the security of one device, will therefore not automatically lead to a compromise in other devices.

Changing Vendor Default Passwords

All vendor-supplied default passwords must be changed before any computer or communications system is used for ISU business operations.

Suspected Disclosure Forces Password Changes

All passwords must be promptly changed if they are suspected of being disclosed, or known to have been disclosed to unauthorised parties.

Password Sharing Prohibition

Regardless of the circumstances, passwords must never be shared or revealed to anyone else besides the authorised user. To do so exposes the authorised user to responsibility for the actions that the other party takes with the password.

Password for personal use only

Users are responsible for all activity performed with their personal user-IDs. User-IDs may not be utilised by anyone but the individuals to whom they have been issued.
Users must not allow others to perform any activity with their user-IDs. Similarly, users are forbidden from performing any activity with IDs belonging to other users (excepting anonymous user-IDs like "guest").

Disclosure of incorrect log-in information

When logging into a ISU computer or data communications system, if any part of the log-in sequence is incorrect, the user must not be given specific feedback indicating the source of the problem. Instead, the user must simply be informed that the entire login process was incorrect.

Related Documentation

Users should be familiar and comply with the following related documents;
a. Remote Access Policy
b. Network Connectivity Policy
c. *Mobile Computing Policy*
d. *ICT Security Policy*

For further details on any aspect of this policy, please contact: Director, ICT Tel: 0912202278