Password Policy for Illinois Institute of Technology

Ashutosh Joshi

Cyber Security Management in Information Technology

Illinois Institute of Technology

Date: 04/30/2020

1. **Overview:**

Password plays an important role in securing account for the ever university. The passwords should meet some criteria so that it can be more secured and can not be compromised and what should a user, student or staff keep in mind while creating, working, saving and implementing these passwords.

1. **Purpose:**

**The** purpose is to create the password policy to all users and staff who’s are related or working with Illinois Institute of Technology.

1. **Scope:**

**This policy applies** to the Illinois Institute of Technology that uses passwords for authenticate its users and staff. All passwords used by Illinois Institute of Technology must adhere these standard unless technically infeasible.

1. **Poilcy:**
2. **Password Guidelines.**

Password Guidelines helps us to create a secure password that will be more secure from our random generated or personal generated password. There are some guidelines which we can follow.

1. When creating a password maintain that the password should be 8-characters minimum length requirement and maximum 40 characters.
2. Password must contain at least on character listed below
3. Uppercase Alphabets (A-Z)
4. Numbers (0-9)
5. Lower case Alphabet (a-z)
6. Password must contain some special characters like ! @ # $ % ^ & \* {| \} - \_: “ and it can contain spacebar also.
7. Password should not contain any used or previous passwords for any other accounts. It should be very unique from the previously used passwords.
8. Password must not contain
9. Any repeated numbers or any personal phone numbers.
10. Any name (First, middle, last name or initials), place, things or pet names that are easy to guess.
11. Any group of three or more character or non-English words.
12. It should not contain any word that can spelled completely.
13. **Working with Passwords.**
14. Password Storing. Storing a password is always been problem for mostly users. The password should store in the clear text.
15. Password Sharing. Password sharing should be done by the user.
16. Multifactor Authentication Factor. Multifactor authentication should be used while logging into every password protect sites. This will increase the security for the user.
17. Security Questions. Security questions will increase the security for the user and security questions can be used for password resetting also when user try to change its password anytime.

1. **Password Protection.**
2. Password Sharing. Password sharing should not be done. While sharing the password it ends up in the wrong hands due to little mistake.
3. Storing password. Password storing should not be done. If any user wants to store the password either it should be encrypted or contain another authentication for getting that password. Which will prevent that password getting into the wrong hands. Password should be stored in the non-reversible format.
4. Embedding and hard-coding. Saving password in any browser is common thing for all of us but saving this password compromises our password security. Saving password feature from browser should be turn off by the user.
5. Always enable two-way authentication. Two-way authentication plays an important role in password protection. Every user should use this to improve their security. It also removes those user whos’ somehow gain access to their password but won’t be able to go further due to two-way authentication.
6. Resetting password. Password resetting should be mandatory after 180 days for every user. New semester new password should create this we increase the security for the user. The new password should be different from the recent used on and should follow the above password guidelines.
7. Password encryption. Password must be encrypted during storage and transmission over the college networks.
8. Pre-assign passwords. Pre-assign password should be change by the user if he’s using the account more than one time.
9. Computer lab passwords. Computer labs should provide each individually user a new password for accountability purpose. If this is not feasible than appropriate mitigation controls must be in place to minimize the risks.
10. Shared account passwords. Sharing devices or resources is a common thing for university but the password should be changed if any user leaves the group or new person added to that particular group. This will help to gain access to those authorized users

Only which are registered.

1. **Account lockout policy for wrong passwords**

The steps should be taken when user forget its password or password or if he thinks the password is compromised.

1. Too many attempts. The attempts for the wrong password should be 5, after 5 wrong passwords the account will be locked for 12 hours.
2. Unsuccessful login. While logging in we forget username or password, most sites tell what we forgetting like username or password. The system should not tell us about what is wrong with like password or username.
3. Login suspension. If any user gets an email or encounter any password or username changed than without its permission than the account should be suspended till the result obtained or minimum for 24 hours.
4. Resetting password. Contact help desk at respective numbers after detailed information provided by the student, then new link for a new password will be provided to the student for access any accounts.
5. Changing rested password. If a student or user has rested their password than it should be changed with 3 days, otherwise the user has to get another new rested password for the account.
6. **Special policy for staff and administrative.**

**T**he password for some high access user like staff and administration should require more attention for our policies

1. Password changing. Password changing for the user with the high privileged should be changed within every 90 days to make account more secure.
2. Two passwords for one account. The two passwords help user with most privileged feature to secure their account. The first password should be created by the administration or by the password handling team. Second, password should be made by the user himself so the account is more secure than ever.
3. Security questions. This should be applied as the essential features for password protection and resetting the if anyone wants to change their passwords.
4. **Enforcement**

**Th**e chief information officer or administrator is responsible for implementing, reviewing and monitoring policies. Illinois Institute of Technology should protect its password resources and if anyone to do inappropriate things to passwords or it’s resources than its access to the password should be revoked.