Password Policy

Divya T. Aradhya

Create a document to be used as a written password policy. The policy will be given to database users in an organization.

An organizational written password policy is to serve one main purpose: Data Security. It needs to protect the company's digital information from illegal access, malicious additions and edits, from deletion, from being locked out, from being tampered and exploited, and from being distributed. The threats could be intention or unintentional, internal or external.

Password Creation-

1. The use of long-tailed pass*phrases* is encouraged than a pass*word*. (This increase the length and safeguards against brute attacks, and also makes remembering passwords intuitive for the dataset users.)

   Note: For the purpose of convenience the word "pass*phrase"* will be referred to as a "pass*word"* in this document.
2. Password created for one system may not be used for others. (To limit repercussions of a possible breach)
3. Passwords shall have a minimum of eight characters with a mix of alphanumeric, upper and lower cases, and special characters. [1] (This safeguards against dictionary and brute-force attacks)

Password Change-

1. All default passwords and vendor-supplied passwords of all software and hardware will be changed immediately on installation. (To prevent illegal access and hacks)
2. Users need to change their passwords at least once in three months and may not reuse the last three passwords while doing so. (To prevent against a possible brute force attack

which takes more than three months to crack, and to safeguard against breached passwords)

Password Storage-

1. Passwords shall be memorized and never written down or recorded along with corresponding account information or usernames. [2] (To prevent password theft)
2. Passwords must not be remembered by unencrypted computer applications such as email. Use of an encrypted password storage application is acceptable, although extreme care must be taken to protect access to said application. [2] (To prevent password theft and misuse)

Password Sharing-

1. Passwords shall not be transferred or shared with others unless the user obtains appropriate authorization to do so. [2] (To prevent password misuse)

   All passwords are to be treated as sensitive, confidential Company information. [1]
2. Passwords may not be part of any communication media like letters, emails, message boards, online forms, phone calls, phone texts, and videos, amongst others. (To prevent password theft)
3. When communicating a password to an authorized individual orally, the user must take measures to ensure that the password is not overheard by unauthorized individuals. [2] (To prevent password breach)
4. Password creating patterns, rules, that you follow to make it easy to remember, will not be disclosed or discussed. (To prevent malicious users from guessing passwords).

5. If for any reason a user has the knowledge of another's password, the user is expected to raise an alert on the disclosure and this password will be immediately reset. (To close disclosure gaps and mitigate risks)

Password Protection-

1. The "Remember Password" feature of applications and web-browsers should NOT be used. [1] (To prevent password breach)
2. If there is a situation of a possible breach, or theft, or compromise, or disclosure, due to carelessness or a malicious attack, or any other reason, the password will be reset immediately. (To mitigate risks and prevent escalation of possible breaches)
3. No password hints will be created, and the user must rely on his memory for recalling the password. (To prevent password guessing)

Incorrect Password Monitoring-

1. Logs of incorrect password attempts will be maintained. (To study possible malicious attacks)
2. After five incorrect attempts the user id will be locked and the user needs to contact the Admin for a password reset. (To prevent access using password-guessing)

Policy Compliance-

1. The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner. [2]
2. Exceptions may be granted in cases where security risks are mitigated by alternative methods, or in cases where security risks are at a low, acceptable level and compliance with minimum security requirements would interfere with legitimate academic or

business needs. To request a security exception, the user must contact the Office of Information Security. [1]

References

[1] Enterprise Information Technology Services: Home. (n.d.). Retrieved from https://eits.uga.edu/access_and_security/infosec/pols_regs/policies/passwords/password_standard/

[2] Password Protection Policy. (n.d.). Retrieved from https://www.sans.org/security-resources/policies/general/pdf/password-protection-policy