netwrix

Password Policy Best Practices

Avoid common password weaknesses

- Easy-to-guess passwords, especially “password”.
- Your name, the name of your spouse or partner name, or other names.
- A string of numbers or letters like “1234” or “abcd”, or simple patterns of letters on the keyboard, like “asdfg”.
- Your phone number or your license plate number, anybody’s birth date, or other information easily obtained about you (e.g., your address, town or alma mater).
- Passwords of all the same letter.
- Words that can be found in the dictionary.
- Default passwords, even if they seem strong.
- Any of the above followed or preceded by a single digit.

Protect your password

- It is vital to remember your password without writing it down somewhere, so choose a strong password or passphrase that you will easily remember. If you have a lot of passwords, you can use password management tools, but you must choose a strong master key and remember it.
- Be aware of how passwords are sent securely across the Internet. URLs (web addresses) that begin with “https://” rather than “http://” are more likely to be secure for use of your password.
- If you suspect that someone else may know your current password, change it immediately.
- Change your password periodically (every 90 days for a strong password, every 180 days for a passphrase), even if it hasn’t been compromised.
- Don’t type your password while anyone is watching.
- Avoid using the same password for multiple websites containing sensitive information.

Keep your passwords strong

- Use a minimum of 10 symbols, including numbers, both uppercase and lowercase letters, and special symbols.
- Even better, use passphrases consisting of a minimum of 15 symbols using letters and numbers.

Follow password policy best practices for system administrators

- Configure a minimum password length of at least 10 characters for passwords or 15 for passphrases.
- Enforce password history, with at least 10 previous passwords remembered.
- Set a minimum password age of 3 days.
- Set a maximum password age of 90 days for passwords and 180 days for passphrases.
- Enable the setting that requires passwords to meet complexity requirements. This setting can be disabled for passphrases but it is not recommended.
- Reset local admin passwords every 180 days. This can be done with the free Netwrix Bulk Password Reset tool.
- Reset service accounts passwords once a year during maintenance.
- For domain admin accounts, use strong passphrases with a minimum of 15 characters.
- Track all password changes by enabling password audit policies. This can be done with Netwrix Auditor for Active Directory.
- Create email notifications for password expiration. This can be done with the free Netwrix Password Expiration Notifier tool.

Control password policy and monitor password use with Netwrix Auditor

- ✓ Easily review your password policy settings
- ✓ Be notified about changes to your password policy
- ✓ Keep tabs on user password changes and password resets
- ✓ Quickly find accounts with passwords that never expire or are not required
- ✓ Automatically remind users to change their passwords before they expire

Download Free 20-Day Trial

CORPORATE HEADQUARTER:	**PHONES:**
300 Spectrum Center Drive Suite 200 Irvine, CA 92618	1-949-407-5125 Toll-free (USA): 888-638-9749
565 Metro Place S, Suite 400 Dublin, OH 43017	1-201-490-8840
5 New Street Square London EC4A 3TW	+44 (0) 203 588 3023

OTHER LOCATIONS:

Spain:	+34 911 982608
Netherlands:	+31 858 887 804
Sweden:	+46 8 525 03487
Switzerland:	+41 43 508 3472
France:	+33 9 75 18 11 19
Germany:	+49 711 899 89 187
Hong Kong:	+852 5808 1306
Italy:	+39 02 947 53539

SOCIAL:

netwrix.com/social