Department	Information Technology
	12
Author	Andrea Di Felice
Revision Number	2
Classification	Internal

Essex Europe - Password Guidelines and Policy

Passwords are a critical component of information security. Passwords serve to protect user accounts; however, a poorly constructed password may result in the compromise of individual systems, data, or network. This guideline provides best practices for creating secure passwords and provides details on the policies currently implemented on the two major platforms of the Company (Windows Active Directory and QAD).

1. Construction Guidelines

Strong passwords are long, the more characters you have the stronger the password. We recommend a minimum of 14 characters in your password. In addition, we highly encourage the use of passphrases, passwords made up of multiple words. Examples include “It’s time for vacation” or “finally_somebody_to_love”. Passphrases are both easy to remember and type, yet meet the strength requirements. Poor, or weak, passwords have the following characteristics:

- Contain less than eight characters.
- Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.
- Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.
- Are some version of “Welcome123” “Password123” “Changeme123”

2. Correct behaviors

- Users must use a separate, unique password for each of their work related accounts.
- Users may not use any work related passwords for their own, personal accounts.
- Passwords must not be shared with anyone, including supervisors and coworkers. All passwords are to be treated as sensitive and confidential.
- Password must not be printed on computer screens or keyboards or left in plain sight.
- Users must lock their PC when they leave it unattended.
- Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.

3. Active Directory Policy

The current Active Directory policy is enforced through the Global Policy Object tool and the “Default Domain Policy”.

The main settings currently in place are the following:

- Enforce Password History: 12 passwords remembered. This means that the system keeps track of the last 12 entered passwords (the goal is to prevent password re-usage).
- Maximum Password Age:90 days. This means that users are required to change their password every 90 days.
- Minimum Password Age: 7 day. This means that users cannot change their password more than once every 7 days.
- Minimum Password Length:8 chararcters. This means that passwords shorter than 8 characters are rejected by the system.
- Password Must Meet Complexity Requirements:enabled. This means that the system checks that passwords are sufficiently complex: passwords must contain at least 1 character belonging to 3 out of 5 characters categories (uppercase characters of European languages, lowercase characters of European languages, base 10 digits, non alphanumeric characters, any Unicode character that is categorized as analphabetic character but is not uppercase or lowercase).
- Account Lockout Duration: 15 minutes. This means that once the user is locked out(due to wrong password insertion), a time range of 15 minutes is necessary before theaccount can be accessible again.
- Account Lockout Threshold: 5 invalid logon attempts. This means that users have 5 possibilities of typing the right password. If they fail the account is locked out.
- Reset account lockout counter after: 15 minutes. This means that after 15 minutes the counter keeping track of invalid logon attempts is automatically reset.The current QAD password policy can be viewed from menu 36.3.24 (Security Control) and it is shown below.

4. QAD Password Policy

The following policies are currently in place on the ERP system.

- Minimum Length: 8 characters. Self-explanatory.
- Minimum numeric characters: 1. Self-explanatory.
- Minimum non numeric characters: 1 . Self-explanatory.
- Minimum Re-use days: 360 . The same password cannot be re-used before 1 year.
- Minimum Re-use changes: 12. The same password cannot be re-used before having changed it 12 times.
- Password Expiration days: 90 . Password must be changed every 3 months.

- Warning days: 10. Ten days before expiration, warnings start to be shown to end users.

5. Revision History

Revision Number	Date of Change	Responsible	Summary of Change
1	16/11/2021	Andrea Di Felice	New format,revision history and new header
2	24/11/2022	Andrea Di Felice	Revision