	DOC No: AEU01009	TITLE: IT Password Policy			**Advanex Europe Ltd** Head Office: Southwell Site Mill Park Way, Southwell Nottinghamshire, UK, NG25 0ET ☎: 00 44 (0) 1636 815555 📠: 00 44 (0) 1636 817725 Bilborough Site ☎: 00 44 (0) 115 9293931 📠: 00 44 (0) 115 9295773 Video Conference IP:80.176.189.113 www.advanexeurope.co.uk
	Revision.	Date	Supersedes	Page	
ADVANEX	01	27 March 2018	None	1 of 3	

DOCUMENT APPROVAL

Author's Signature:

Your signature indicates that this document has been prepared in accordance with company standards or guidelines and adequately reflects the tasks and deliverables necessary.

Signature .... **Date** 27-MAR-2018
Print Name Ashley Reast
Title IT Manager

Reviewer's Signature:

Your signature indicates that, you have reviewed this document and that it accurately and completely reflects the tasks and deliverables necessary.

Signature .... **Date** 27/3/18
Print Name Ian Beardsmore
Title Managing Director

Signature .... **Date** 27 MAR 2018
Print Name Marian Mullings
Title Finance Director

Quality Assurance/Compliance Approver's Signature:

Your signature indicates that this document complies with company standards or guidelines; and that the documentation and information contained herein complies with applicable regulatory, corporate, divisional/departmental requirements, and current Good Manufacturing Practices.

Signature .... **Date** 28Mar2018
Print Name Gary Crawley
Title QA & Systems Manger

1.0 PURPOSE

1.1. This policy is designed to protect the organisational resources on the network by requiring strong passwords along with protection of these passwords.

2.0 SCOPE

2.1. The policy covers all employees who are responsible for one of more account or have access to any resource that requires a password.

3.0 TERMS, DEFINITIONS & ABBREVIATIONS

3.1. N/A

4.0 HEALTH, SAFETY & ENVIRONMENTAL

4.1. N/A

5.0 ASSOCIATED DOCUMENTS

5.1. N/A

6.0 PROCEDURE

6.1. OVERVIEW

6.1.1. Employees at Advanex must access a variety of IT resources, including computers and other hardware devices, data storage systems and other accounts. Passwords are a key part of IT's strategy to make sure only authorised people can access those resources and data.

6.1.2. All employees who have access to any of those resources are responsible for choosing strong passwords and protecting their log-in information from unauthorised people.

6.2. PASSWORD CREATION

6.2.1. All passwords should be reasonably complex and difficult for unauthorised people to guess. Employees should choose passwords that are at least eight characters long and contain a combination of upper- and lower-case letters, numbers and other special characters. These requirements will be enforced with software when possible.

6.2.2. In addition to meeting those requirements employees should also use common sense when choosing passwords. They must avoid basic combinations that are easy to crack. For instance, choices like "password", "password1" and Pa$$w0rd", are equally bad from a security perspective.

6.2.3. A password should be unique, with meaning only to the employee who chooses it. That means dictionary words, common phrases and even names should be avoided. One recommended method for choosing a strong password that is still easy to remember: Pick a phrase, take its initials and replace some of those letters with numbers and other characters and mix up the capitalisation. For example, the phrase "This may be one way to remember" can become "TmB0WTr!".

6.2.4. Employees must choose unique passwords for all of their company accounts, and may not use a password that they are already using for a personal account.

6.2.5. All passwords must be changed regularly, with the frequency based on the sensitivity of the account in question. This requirement will be enforced using software when possible.

6.2.6. Default passwords – such as those created for new employees when they start or those that protect new systems when they are initially set up – must be changed as quickly as possible.

6.2.7. For more advice on creating/changing passwords please speak with IT.

6.3. PROTECTING PASSWORDS

6.3.1. Employees may never share their passwords with anyone else in the company, including co-workers, managers, administrative assistants, IT staff members, etc. Everyone who needs access to a system will be given their own unique password.

6.3.2. Employees may never share their passwords with any outside parties, including those claiming to be representatives of a business partner with legitimate need to access a system.

6.3.3. Employees should take steps to avoid phishing scams and other attempts by hackers to steal passwords and other sensitive information.

6.3.4. Employees must refrain from writing passwords down and keeping them at their workstations. See above for advice on creating memorable but secure passwords.

6.3.5. Employees may not use password managers or other tools to help store and remember passwords without IT's permission.

6.4. COMPROMISED PASSWORDS

6.4.1. If the security of a password is in doubt – for example, if it appears that an unauthorised person has logged into the account you must:

6.4.2. Immediately report the compromise to IT in writing and verbally

6.4.3. Change to a new secure password immediately across all systems