TechSture
Technologies

Password Policy

Document No – TT-ITP/01

Document Release Note

Document Version	1.0	**Release Date**	

Prepared By		**Approved By**
Pathik Patel		**Chetan Patel**

Document Revision History

Version	Date	Change Description	Modified By	Reviewed By	Approved By
1.0					

Purpose

The purpose of this policy is to define the standard for the creation of strong passwords, the protection of those passwords and the frequency of change.

Scope

This policy concerns all computer system and servers operated or maintained by Techsture Technologies, regardless of location, where responsibility for user management and control resides with the IT team of Techsture Technologies.

Policy

	DOs & DON'Ts	Responsibility
✓	Users are required to choose strong password.	Users
✓	Active directory user passwords must not be less than eight characters.	Users
✓	A new user must be set to change password at first logon.	Users
✓	Passwords must be a combination of alphabets, numbers and special characters.	IT Administrator
✓	Passwords must not be same as username or of the reverse order.	IT Administrator
✓	Passwords must not be based on common character patterns e.g. 1234567, abcdefg, asdfghjkl.	IT Administrator
✓	User passwords must be enforced to be changed every (45) days.	IT Administrator
✓	New password should not be repeated from the past used for any user	IT Administrator

✓	User password reset must be done only on the request of the user or respective manager.	IT Administrator
✓	Critical network equipment including servers, firewall, storage systems, switches, telephony devices and other special devices must have highly complex passwords with access exclusively to Technical Director and IT Administrator.	IT Administrator
✓	Critical online services including email and other web services must have highly complex passwords with access exclusively to the Technical Director and IT Administrator	IT Administrator
✓	IT Department who configures new systems and setup services are to ensure that all passwords' settings are changed from their default settings before changing operating system/application.	IT Administrator
✓	Choose password that it easily remembered so there is no need to write it down.	IT Administrator
✓	Immediately change your password if you think that it has been revealed to anyone else or compromised;	IT Administrator
✓	Confidential Information is not allowed for copying unless otherwise user give rights to this information.	Users
✓	Whenever there is a change in responsibility/ transfer of user/ separation the above list is updated after due authorization.	IT Administrator
✓	When there is no activity for 05 Min the system will automatically locked.	IT Administrator
✗	Don't use any information about you that is easily obtainable, such as the month, your car registration number, your birthday, your child or pets name, your favourite holiday destination or your favourite sports team or hobby.	User & IT Administrator
✗	Don't use your surname or given name in any form.	User & IT Administrator

✗	Don’t use the ‘Remember Password’ ‘Save Password’ feature of applications.	User & IT Administrator
✓	IT Department has rights to change anyone’s password, to secure the information.	IT Administrator

Records

Nil

Effective Measures

No. of deviations with respect to above acceptable usage quarterly.