* ***Password Management Policy***

**Purpose:** The purpose of this policy is to ensure that security practices are introduced and maintained by all employees with respect to password-protected information infrastructure.

***Policy: -***

(1)Passwords should not be inserted into email messages or other forms of electronic communication.

(2) If a password is suspected of being compromised, it should be changed immediately and the incident reported to the University Help Desk.

(3) Passwords may be not visible on a screen, hardcopy printouts, or any other output device

(4) The same password should not be used for access needs external to Montclair State (e.g., online banking)

(5) It is recommended that passwords be changed at least every six months. Passwords for various systems and applications may have an “aging” feature that mandates a password change after a certain number of days or months after the last password change.

*[Note: - Password aging is a mechanism you can use to force users to periodically change their passwords. ]*

(6) Passwords should not be shared with anyone, including administrative assistants or IT administrators. Necessary exceptions may be allowed with the written consent of the Information Technology Division and must have a primary responsible contact person. Shared passwords used to protect network devices require a designated individual to be responsible for the maintenance of those passwords, and that individual will ensure that only appropriately authorized employees have access to the passwords.

(7) Password cracking or guessing may be performed on a periodic or random basis by IT Security or its delegates with the cooperation and support from the appropriate system administrator. If a password is guessed or cracked during one of these scans, the password owner will be required to change it immediately.

(8) Screen-saver password must be enabled after 10 minutes of inactivity of the user. Users must not be allowed to change the inactivity time.

(9) Lockout policy must be implemented for unsuccessful login attempts. As a good practice, a maximum of 3 login attempts should be allowed. The auto-lock policy for locked accounts must be released after 24 hours only.

(10) Password accounts not used for 90 days will be disabled and reviewed for possible deletion. Accounts disabled for 60 days will be deleted.

(11) Vendor or service accounts will be removed from computer systems prior to deployment and new passwords are to be implemented on all systems immediately upon installation at XXX facilities.

(12) Passwords may not be embedded in automated programs, utilities, or applications, such as autoexec.bat files, batch job files, terminal hotkeys.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*