

COLLEGE POLICY DOCUMENT

Policy Name	Password Policy	Version	1.2
Review Date	9/1/2015	Next Review Date	8/31/2016
Author	Arun	Effective Date	11/1/2015

INTRODUCTION

Passwords are an important aspect of computer security and are the first line of defense for user accounts. A poorly chosen password may result in unauthorized access and/or exploitation of MEC's resources. All users, including contractors and vendors with access to MEC systems, are responsible for taking the appropriate steps to select and secure their passwords.

PURPOSE

This policy defines the requirements for establishing the password configuration settings and managing fixed passwords used on any MEC computer and communications system.

AUDIENCE

The MEC Password policy applies equally to all individuals granted access privileges to any MEC Information Resources.

DEFINITION

Partner – Any non-employee of MEC who is contractually bound to provide some form of service to MEC.

Password – An arbitrary string of characters chosen by a user that is used to authenticate the user when he attempts to log on, in order to prevent unauthorized access to his account.

System Administrator – An employee or partner who is responsible for managing a MEC multi-user computing environment. The responsibilities of the system administrator typically include installing and configuring system hardware and software, establishing and managing user accounts, upgrading software and backup and recovery tasks.

User - Any MEC employee or partner who has been authorized to access any MEC electronic information resource.



POLICY STATEMENT

- Don't use dictionary words as passwords. - Avoid using any words, words in foreign languages, swear words, slang, names, nicknames, etc.
- Avoid use of family names, friends and partners, anniversary dates, car registrations, usernames and telephone numbers. Instead try to pick acronyms, mnemonics, random letters or insert non-alphabetic characters in the middle of the word, replace letters with numbers ('o' to zero, I to 1, E to 3).
- Use a **mIxTuRe** of UPPER and lower case on case sensitive systems - Unix and Linux.
- You must include a number (0-9) somewhere within the password. Include a symbol (£\$ %&^*+=) somewhere in the password.
- Change password completely, rather than partially.
- Never allow anyone to login as you. Never tell anyone your password, for example on the telephone.
- Avoid letting other people watch you key your password in. Choose something that is not easy to guess from watching, like "qwerty12345".
- All system-level passwords (e.g. root, enable, Windows admin, application administration accounts, etc.) and user-level passwords (e.g. email, web, desktop computer, etc.) must be changed at least on a quarterly basis.

DISCIPLINARY ACTION

Violation of this policy may result in disciplinary action which may include warning, termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or warning, suspension or expulsion in the case of students. MEC reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity.

REFERENCE (OPTIONAL)