EMPORIA STATE UNIVERSITY™

			11.3.1
Division:	Technology & Computing Services	Effective Date:	10/13/2009
Department	Information Security	Last Revised:	10/06/2009
Version:	FSB 09007	Next Annual Review:	01/15/2011
Approved By:	Faculty Senate and University President	Date Passed Senate:	10/06/2009
		Date of ESU President's Approval:	10/13/2009
Previous Action:	FSB 06025 Password Policy passed by Faculty Senate and approved by President 4/6/07		

Password Policy (Amendments to Password Policy; FSB 06025 approved by President 4/6/07; FSB 09007 approved by President 10/13/09)

Policy Objectives

A user ID and password is a key granting access to various systems and applications and the information assets they protect. As Emporia State University (ESU) is committed to protecting the confidentiality, integrity, and availability of the information it owns or controls, passwords must be created and protected in a manner that minimizes the likelihood of unauthorized access to such assets. If a password is shared, account holders can be held responsible for any activity performed with their account. Passwords should be unique and must not be shared.

Policy

Passwords created by any person granted access to ESU information assets must meet the following guidelines:

- Password must be at least eight (8) characters in length
- Passwords must be different than the user ID
- Passwords must not consist of familiar names (e.g., relatives, pets)
- Passwords must not be words found in a dictionary
- Passwords must be made using at least three of the following four groups of characters:
  - Uppercase alphabetic characters (A-Z)
  - Lowercase alphabetic characters (a-z)
  - Numbers (0-9)
  - Special Characters (i.e. #, &, *…)
- Passwords must be changed at least every 180 days
- Default account passwords that are included in many applications and systems must be changed immediately
- Initial passwords must be changed immediately upon first login
- Passwords must not be reused within a 12 month period

EMPORIA STATE UNIVERSITY™

			11.3.1
Division:	Technology & Computing Services	Effective Date:	10/13/2009
Department	Information Security	Last Revised:	10/06/2009
Version:	FSB 09007	Next Annual Review:	01/15/2011
Approved By:	Faculty Senate and University President	Date Passed Senate:	10/06/2009
		Date of ESU President's Approval:	10/13/2009
Previous Action:	FSB 06025 Password Policy passed by Faculty Senate and approved by President 4/6/07		

Responsibility

It is the responsibility of each account holder:

1) To create a password for each application as required by the application
2) To not share passwords
3) To protect passwords from unauthorized use
4) To change passwords at intervals specified by the policy or as required by the application
5) To immediately notify the Information Security Officer (ISO) if they believe their password has been compromised

It is the responsibility of System Administrators to keep the system administrator password secure, yet available in case of emergency. TCS System Administrators will refer to the System Password Procedures for systems managed by TCS.

Scope

This policy applies to any person granted access to an ESU information asset that requires a user ID and password.

Enforcement

The ISO is responsible for monitoring and reporting compliance with this policy.

In all cases, information will be disclosed as required by controlling law.

Exceptions

The President or designee must approve any exceptions to this policy.