

Date Passed Senate: October 6, 2009

Date of ESU President's Approval: October 13, 2009

FSB 09007

AMENDMENTS TO THE PASSWORD POLICY

Date of First Reading: September 15, 2006

Date of Second Reading: October 6, 2009

Senate Sponsor: Academic Affairs Committee
Ann O'Neill, Chair of Academic Affairs

- I. **Purpose:** To amend the password policy to reflect changes recommended by the Legislative Division of Post Audit.
- II. **Previous Senate Action:** FSB 06025 Password Policy passed by Faculty Senate and approved by President 4/6/07
- III. **Rationale (optional):** In 2008 Emporia State University was audited by the Legislative Division of Post Audit. After consultation with the University General Counsel, the Academic Affairs committee and the University Information Security Officer, Cheryl O'Dell, CISSP (Certified Information System Security Professional), has drafted the changes to the password policy to reflect the expectations of the audit findings.
- IV. **Guidance (optional):** Revise the policy. ~~Existing text to be changed is struck through.~~ **Text intended to replace existing text is bold and underlined.**

FSB 09007

Amendment to Password Policy

1
2
3
4
5
6
7
8
9
10
11

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.

12 Policy

13

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

- 16 • Passwords ~~should~~ **must** be at least ~~six~~**eight (68)** characters in length
- 17 • Passwords must be different than the user ID
- 18 • Passwords ~~should~~ **must** not consist of familiar names (e.g., relatives, pets)
- 19 • Passwords must not be words found in ~~the~~ **a** dictionary
- 20 • Passwords ~~should~~ **must** be made using at least ~~two~~**three** of the following
21 ~~three~~**four** groups of characters:
 - 22 ○ **Uppercase** ~~A~~alphabetic characters (A-Z, ~~a-z~~)
 - 23 ○ **Lowercase alphabetic characters (a-z)**
 - 24 ○ Numbers (0-9)
 - 25 ○ Special Characters (i.e. #, &, *...)
- 26 • Passwords must be changed at ~~intervals as specified by the procedures for the~~
27 ~~application in which they are used~~ **least every 180 days**
- 28 • ~~All policies regarding protection from unauthorized access apply to passwords~~
29 ~~written or otherwise listed elsewhere~~
- 30 • Default account passwords that are included in many applications **and systems**
31 ~~must be changed~~ **immediately** ~~prior to deploying that application into the~~
32 ~~network, and must follow the same guidelines as user account passwords.~~
- 33 • Initial passwords must be changed immediately upon first log-in.
- 34 • **Passwords must not be reused within a 12 month period**

35

36 Further, it is the responsibility of each account holder:

- 37 • ~~To create a password for each application as required by the software vendor~~
- 38 • ~~To not share passwords with anyone~~
- 39 • ~~To protect passwords from unauthorized use~~
- 40 • ~~To change passwords at intervals specified in application's procedures~~
- 41 • ~~To immediately notify the Information Security Officer (ISO) if they believe~~
42 ~~their password has been compromised~~
- 43 • ~~Password protection policy applies to any person granted access to an ESU~~
44 ~~information asset that requires a user ID and password.~~
- 45 • ~~The Information Security Officer is responsible for monitoring and reporting~~
46 ~~compliance with this policy.~~
- 47 • ~~In all cases, controlling law will govern the disclosure of information.~~
- 48 • ~~The University President or designee must approve any exceptions to~~
49 ~~password policy.~~

50

51 **Responsibility**

52

53 **It is the responsibility of account holders:**

- 54 1) **To create a password for each application as required by the application**
- 55 2) **To not share passwords**
- 56 3) **To protect passwords from unauthorized use**

- 57 4) **To change passwords at intervals specified by the policy or as required by**
58 **the application**
59 5) **To immediately notify the Information Security Officer (ISO) if they believe**
60 **their password has been compromised**

61
62 **It is the responsibility of System Administrators to keep the system administrator**
63 **password secure, yet available in case of emergency. TCS System Administrators**
64 **will refer to the System Password Procedures for systems managed by TCS.**

65

66 **Scope**

67

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

70

71 **Enforcement**

72

73 **The ISO is responsible for monitoring and reporting compliance with this policy.**
74 **In all cases, information will be disclosed as required by controlling law.**

75

76 **Exceptions**

77

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

79

80

Provide comments about this bill to your department's senator or Faculty President Carol Russell at crussell@emporia.edu.