Policy and Procedures on
Access Control and Password Security

Managed and secure access control is

- Vendor account passwords will be activated, disabled or changed only when needed. Vendors accessing College computers or software are to be accountable for their access;

- Default administrator accounts will be renamed, removed or disabled. Default passwords on any remaining administrator accounts will be changed. Where possible, these accounts should have user-IDs that do not indicate or suggest a level of privilege, such as supervisor, manager, or administrator;

- Authorized persons requiring access to operating system code, etc., will be provided a unique privileged account (user-ID) for his or her personal and sole use in conducting privileged activities. A second account will be provided for performing normal business activities;

- Privileged accounts will be subject to higher standards based upon the access provided:

    - Privileged accounts are only to be issued to individuals who are required to support the system at the level prescribed. Individuals provided access to privileged accounts will be specifically documented;

    - Use of privileged accounts will be strictly monitored and suspected misuse promptly investigated; and

    - Where possible, passwords to privileged accounts will be changed more often than normal user accounts.

- Temporary passwords will be the changed at the first logon;

- Passwords will not be included in any automated logon process, such as a macro or function key, web browser, or in application code;

- Access to systems and applications will be monitored, logged and analyzed to detect deviation from the access control policy;

- Automated techniques will be implemented that require re-authentication after a predetermined period of inactivity (e.g. password-protected screen savers, automated log-off processes, or re-authentication after a set time-out period);

- Passwords will only be transmitted and stored using secure mechanisms such that authentication information and access could not be intercepted or obtained by an unauthorized party; and

- Access to systems that contain private or sensitive information will not be allowed from unsecure devices or via unsecure environments unless appropriate security is used.

User Password Requirements

The following items govern the creation, use and maintenance of user passwords:

- System users are responsible for creating secure passwords and managing these effectively. Passwords must be a minimum length and include a mix of upper/lower case, numeric, and special characters as defined in the College's Policy on Password Creation Standards;

- Individuals are responsible for the protection of their passwords and protecting against unauthorized activities performed under his or her accounts;

- Individuals are not to share their passwords or grant permission to others to use their accounts without prior permission. Under emergency situations, individuals may request permission to allow another to use their account. If approved, the individual allowing access is responsible for any activity done under their password. New account passwords must be created after any shared use;

- Individuals are expected to change their passwords at regular intervals, as defined by the Policy on Password Creation Standards; and

- If an account or password is suspected to have been compromised, an individual must report the incident immediately to the Computer Center.

Password Security Check

Password cracking or guessing may be performed on a periodic or random basis by Computer and Information Systems. If a password is guessed or cracked during one of these scans, the user account will be disabled until the password has been reset.

Violations

Any individual found to have violated this Policy may be subject to disciplinary action, up to and including termination of employment. Violation of this policy may result in termination of contracts or commitments ludyment. Vc ngord bantfrys

T1d ( )Tj [(b)-10(e)35.95ubje-35.95ncedpu f* BT (uJ (P)Ta(c)4(i)-2(pl)-he)4(d unt)-2(i)- S policcmay