DATA PROTECTION AND SECURITY POLICY

(*Excerpted from Section 3.12 of the Western Employee Handbook for Professional Employees*)

Western Colorado University collects information from prospective and enrolled students and parents, employees and their dependents, alumna, and donors for administrative, management, or business purposes. This policy establishes requirements on data security and protection of high-risk confidential information.

The same definition of HRCI as set forth in Section 3.11, applies in this Section 3.12.

Access to HRCI must be limited to only those employees whose job responsibilities require it. HRCI is to remain confidential and must not be revealed to anyone who does not have the right to view or know the information. Unauthorized access to and use of HRCI violates University policy, and state and federal statute, and is not permitted.

Employees whose job responsibilities require access to and use of HRCI must take steps to physically secure this information and must follow these guidelines:

1. Employees must take all steps necessary to ensure that HRCI displayed on computer monitors is not subject to unauthorized viewing by others. Such steps include, but are not limited to, minimizing application windows while in the office, locking the Desktop, closing applications, and logging out of computers when not working.
2. Employees must ensure physical protection for all devices storing HRCI. When not directly in use, office and suite doors must be locked and any easily transportable devices not in the possession of the employee should be secured in locked cabinets or drawers.
3. Employees must limit the production of hard-copy documents containing HRCI to the extent practical. Hard copy documents containing HRCI must remain in secured locations on campus unless otherwise authorized by the President or overseeing vice president.
4. Employees must secure hard copy documents containing HRCI by maintaining a clean desk and locking such documents in secure, designated areas (such as a locked desk or file cabinet) when they are not working. If no locking storage areas are available, documents must be removed from plain sight.
5. Employees should supervise and protect incoming and outgoing mail collection points and fax machines so that unauthorized individuals do not pick up documents containing HRCI.
6. Employees must immediately retrieve documents containing HRCI from printers or retrieve such documents at the printer using a password.

HRCI kept in electronic format should be stored exclusively in secured network drives and databases (e.g., Banner, document management system). Storage of HRCI data on any device, including but not limited to, desktop hard drive, laptops, PDAs, phones, USB Drives, CD/DVD, and diskettes is prohibited unless otherwise authorized by the President or overseeing vice president.

Devices with access to stored HRCI data must be password protected and locked or logged off when unattended. Employees must follow these guidelines for password protection:

1. Employees accessing password protected computing resources are required to use strong passwords that are difficult to guess or crack, including a combination of alpha, numeric, and other characters.
2. Passwords are not to be posted on, under or around a computer or in the workplace.
3. Employees must never provide their password to anyone else and never let anyone else use their computer account.
4. Passwords must be changed when there is reason to believe the password has been compromised.

5. All campus departments whose business practices require access to and use of HRCI must develop policies surrounding the retention and disposal of information that are consistent with state or federal law. All policies must be approved by the Cabinet prior to implementation.
6. Employees must immediately report to their supervisor any violations to this policy or incidents of misuse of HRCI.

The University shall regularly conduct, or cause to conduct, assessments of data risk to improve the policies and procedures related to data protection.

.