

### **Section 3.11: High Risk Information Confidentiality and Disclosure Policy**

Western State College of Colorado collects information from prospective and enrolled students and parents, employees and dependents, alumna and donors for administrative, management or business purposes. This policy establishes restrictions on the access, use and distribution of high-risk confidential information.

High-risk confidential information (HRCI) is defined as any combination of full name, SSN, date of birth, permanent address, driver's license number/passport/other government-issued identification number, credit/debit card number, bank information, personal medical information and academic records. This information, if maliciously obtained and misused, carries a high risk of causing personal, financial or reputational damage to its owner.

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 College policy and state and federal statute and is not permitted.

Employees whose job responsibilities require access to HRCI must follow these acceptable use guidelines:

1. Use of such data shall be limited to the purpose required to perform college business.
2. Users must respect the confidentiality and privacy of individuals whose records they access, handle HRCI ethically, and abide by applicable laws with respect to accessing, using, or disclosing information.
3. Users must comply with all state and federal laws relating to information security and privacy.
4. HRCI may only be disclosed to individuals or entities on a need-to-know basis.
5. HRCI must be protected to prevent loss, theft, unauthorized access, unauthorized modification, unauthorized destruction, and/or unauthorized disclosure. Please refer to the policy on Data Protection and Security.

Through the course of legitimate business practices, HRCI may need to be disclosed and/or transferred to outside entities. Employees responsible for this disclosure or transfer of HRCI must follow the guidelines specified in Transmittal of Confidential Data. Contact the Information Technology Services department for information on these guidelines.

Employees whose position requires access to HRCI are required, as a condition of employment, to sign a confidentiality agreement or provide a signed acknowledgment of this policy.

Employees must immediately report to their supervisor any violations to this policy or incidents of misuse of HRCI.

### **Section 3.12: Data Protection and Security Policy**

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

High-risk confidential information (HRCI) is defined as any combination of full name, SSN, date of birth, permanent address, driver's license number/passport/other government-issued identification number, credit/debit card number, bank information, personal medical information and academic records. This information, if maliciously obtained and misused, carries a high risk of causing personal, financial or reputational damage to its owner.

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 College 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 out of the office.
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 out of the office. 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.
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.

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 president's cabinet prior to implementation.

Employees must immediately report to their supervisor any violations to this policy or incidents of misuse of HRCI.

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