CGCC DATA SECURITY STATEMENT
Public Security Overview - 2017

The community entrusts Columbia Gorge Community College (CGCC) with their personal data, and CGCC makes it a high priority to take our patrons security and privacy concerns seriously. We strive to ensure that all data is handled securely and with highest level of confidentiality. CGCC uses a number of technology tools and practices for internal and external security. This statement is aimed at being transparent about our security infrastructure and practices, to help reassure you that your data is appropriately protected.

Physical Security
All of CGCC's information systems and infrastructure are housed in a state-of-the-art data center and secured distribution centers. All of these areas include the necessary physical security controls you would expect in a secured environment such as video monitoring and electronic key card door locks.

Administrative Security
CGCC's electronic data system access is designed and maintained with a need-to-know / least privilege philosophy. CGCC implements a robust user/group/application/location layered access model to help assure that only those that need to see your data get the correct access. Automated alert systems exist to notify personnel if there is inappropriate data access.

CGCC complies with all Family Educational Rights and Privacy Act (FERPA) laws.

Network Security
CGCC utilizes aggressive firewall rules for external access, complete internal network segmentation, physical connection limitations, as well as role-based access managed by authorized IT staff.

Vulnerability Management

- **Patching:** Latest security patches are applied to all operating systems, applications, and network infrastructure to mitigate exposure to vulnerabilities.
- **Third Party Scans:** Our environments are scanned using best of breed security tools. These tools are configured to perform application, file and network vulnerability assessments.
- **CGCC Personnel training**: CGCC personnel are trained and reminded on best security practices.

Handling of Security Breaches

Despite our best efforts, no method of electronic storage is perfectly secure. We cannot guarantee absolute security. However, if CGCC learns of a security breach, we will notify affected users so that they can take appropriate protective steps. Our breach notification procedures are consistent with our obligations under various state and federal laws and regulations, as well as any industry rules or standards that we adhere to. Notification procedures include providing email notices or posting a notice on our website if a breach occurs.

Your Responsibilities

Keeping your data secure also depends on you ensuring that you maintain the security of your account by using sufficiently complicated passwords and storing them safely. CGCC recommends you only share your student ID with known college personnel, and never share your CGCC password with anyone.