CCC DATA SECURITY STATEMENT

Information Security Overview

Clackamas Community College (CCC) is entrusted with the personally identifiable information (PII) of employees and students. Due to the sensitive nature of the PII entrusted, CCC makes it a high priority to take information security and privacy concerns seriously, and strives to ensure that all data is handled securely, and with highest level of confidentiality.
While the college uses a number of technology tools and practices for information security, CCC wants to be transparent about our security infrastructure and practices in order to reassure you that your data is appropriately protected.

Physical Security

All of CCC's information systems and infrastructure are housed in a data center that is secured physically, as well as technologically. The physical security includes the controls you would expect in a secured environment such as; video monitoring, and electronic door locks.

Administrative Security

CCC's system access is designed and maintained with the best practice need-to-know/least privilege philosophy. CCC implements a robust user/group/application layered access model to ensure that only those that need to see your data get the correct access. CCC also complies with all Family Educational Rights and Privacy Act (FERPA) laws.

Network Security

CCC utilizes next generation firewalls for external access, and internal network segmentation which also applies to the college's wireless network. Physical connections are administratively limited, with access managed by authorized IT staff.

Vulnerability Management

- **Patching:** Latest security patches are applied to all operating systems, applications, and network infrastructure on a regular basis to mitigate exposure to vulnerabilities.
- **Third Party Scans:** Our environments are periodically scanned for network vulnerability assessments by a third party.

Handling of Security Breaches

There is no method of electronic storage that is actually secure, so the college cannot guarantee absolute security. However, if CCC 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. Notification procedures will 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. Current National Institute of Standards and Technology (NIST) password recommendations are as follows:

NIST guidance recommends the following for passwords:

- An eight character minimum and 64 character maximum length
- The use of both upper-case and lower-case letters
- Use special characters such as @, #, $
- No sequential and repetitive characters (e.g. 12345 or aaaaaa)
- No passwords found in the user’s personal information (e.g. birthdate, SSN, etc.)
- No commonly used passwords (e.g. p@ssw0rd, etc.)
- No passwords obtained from previous breach corpuses

CCC recommends you only share your student ID only with known college personnel, and never share your CCC password with anyone, or let anyone use your computer while you are logged in.