Data Privacy, Safety and Security Plan	Plans
	Effective Date: July 1, 2019
	Board Review Date: September 24, 2019

(1) Data Privacy.
  (a) Student academic records are maintained in the Northstar information system. Access to the system is controlled by the Vice President of College Services and the Registrar, and the information is password protected. All staff undergo yearly FERPA training.
  (b) Employee personnel files are stored on a separate drive from other college records, and are only accessible by authorized personnel. Payroll and other financial records are likewise stored on a separate drive or off-site, and are password protected.

(2) Data Safety.
  (a) The IT team maintains a Disaster Recovery Plan and Procedures to recover from disasters affecting its production operations. In the event of a disaster at the College that results in loss of data processing equipment or the data that it contains, the following procedures outline methods to recover the data and access to it. This document will address total loss of equipment and data. Obviously, only the portions of this document that apply to the equipment/data lost need to be addressed.
    (i) Obtain and replace any defective equipment (see list of vendors below)
    (ii) Connect/configure network hardware as required
    (iii) Load Operating System/software as required
    (iv) Restore data from backup appliance (see Backup Procedure document-attached)
    (v) Contact technical support as required (see list of support vendors below)
  (b) Backup Procedures. All server backups are done on a Simplivity VMWare Appliance. A secondary appliance is located at the UETN DC and is used as an offsite backup location. All the backup data is replicated and synchronized on both devices after the nightly backups are executed. Backups are retained as follows:
    (i) Full backups – 3 Years
    (ii) Incremental backups – 1 Year
  (c) Disaster Recovery Procedure. In the event of a disaster at the College that results in loss of data processing equipment or the data that it contains, the following procedures outline methods to recover the data and access to it.
    (i) Obtain and replace any defective equipment
    (ii) Connect/configure network hardware as required
    (iii) Load Operating System/software as required
    (iv) Restore data from backup appliance

(3) Data Security.
  (a) Internet and infrastructure backbone connectivity is provided by the Utah Education and Telehealth Network (UETN) data network, is maintained by the UETN, and is contracted throughout the state. The UETN network:
    (i) Provides and maintains the wide area broadband; Internet access; network support and security monitoring; and broadcast.
    (ii) Carries high speed data and real-time applications, including video to communities throughout the state.
    (iii) Support personnel continuously track, report, and manage Internet, data, and video traffic for the College.
    (iv) Security detects attacks on the network, identifies miscreant tools and trends, and mitigates infrastructure vulnerabilities.

(b) The College employs competent Information Systems personnel that provide ongoing analysis, planning, maintenance, and security of the LAN/WAN operations.
(c) Student academic records are maintained in the Northstar information system. Access to the system is controlled by the Vice President of College Services and the Registrar, and the information is password protected.
(d) Employee personnel files are stored on a separate drive from other college records, and are only accessible by authorized personnel. Payroll and other financial records are likewise stored on a separate drive or off-site, and are password protected.
(e) Servers housed at the College are located behind secure doors, with limited access.
(f) Hardware and software firewalls are configured to block access to the Intranet from the outside. Antivirus and antispyware Software is used on all servers and workstations.
(g) Users are required to change their password every 90 days and must maintain at least six passwords.

(4) Annotations. See COE Check Sheets (2018), Standard 6, No. 16.