CALIFORNIA STATE UNIVERSITY EAST BAY

ACADEMIC SENATE

http://www.csueastbay.edu/senate

INFORMATION TECHNOLOGY ADVISORY COMMITTEE

Designation Code: 2013-14 CAH 1amended
Friday, November 8, 2013

TO:	The Academic Senate
FROM:	The Information Technology Advisory Committee
SUBJECT:	13-14 CAH 1: Data Integrity Policy
PURPOSE:	Approval of the Academic Senate

ACTION REQUESTED:
That the Academic Senate approve the attached Data Integrity policy, effective Spring 2014.

BACKGROUND:
Beginning in academic year 2011-2, the Information Technology Advisory Committee (ITAC) has worked to develop a policy about data integrity. This was originally motivated by a catastrophic data loss when the learning management system (Blackboard) crashed and the backup was corrupted. Instructors' responses varied greatly. This proposed policy defines the rights and responsibilities of students, faculty, and staff in various scenarios in regard to "data loss" issues; this policy will be added to the catalog.

Student, Faculty, and University Responsibilities

to Ensure the Data Integrity of Academic Work

I. Purpose and Scope

The purpose of this policy is to establish the rights and responsibilities of students, faculty, and the university in regards to the loss, reattempt, and/or resubmission of coursework data in the event of verified data or service loss.

This policy applies to student and faculty interactions with academic systems or academic functions within more comprehensive systems and does not apply to administrative systems or functions.

II. Definitions of Data Loss

Catastrophic data loss is defined as the absolute corruption or destruction of data without any chance of recoverability on the part of its owner through data redundancy measures.

Data redundancy measures refer to the means and methods for saving and restoring copies of data prior to the point of its absolute corruption or destruction. This is more commonly known as making a *"backup"* of data.

Service loss is defined as the loss of services that interrupt and prevent the normal flow of academic work.

Examples of such services include the Learning Management System (LMS), other systems through which assignments are digitally submitted (for example, network drives), data housed on third-party applications such as Google, VoiceThread, or Pearson, or software provided by companies such as Wordpress.

III. Coursework Data

Coursework data is defined as digital products, materials, and works created, edited, and completed by the student or with which the student interacts as required by coursework specified by the instructor. Coursework data takes many forms, some of which include single data files (e.g. word processing files, presentation files, multimedia files), compressed archives (e.g. .zip files, .rar files), interactive coursework and assessments (e.g. online exams), and synchronous and asynchronous communication across multiple computing platforms (e.g. webinars, synchronous collaborative documents). While these examples represent a wide variety of the kinds of coursework data that may be required in a classroom, it is understood that the pace of change and innovation in technology introduces new and updated types of coursework data that may not be listed here but are also included as part of this policy.

IV. Responsibilities for the Prevention or Management of Data Loss

Multiple individual users and groups are responsible for the prevention and restoration of data and service, and the mitigation of damage when irreversible loss occurs. These include: the university, third-party vendors, and end users.

The University

Data and/or service loss resulting from university systems is known as *institutional data loss*. The university is responsible for ensuring the integrity of services it provides, either directly, if the data resides on university servers, or indirectly, if the data resides on servers operated by third-party vendors. To minimize the impact of university systems failure, appropriate university personnel will

- ensure that data is backed up on a regular schedule;
- restore lost data as quickly as possible; and
- communicate necessary information via Campus Announcements, including the appropriate requirements of this policy, and providing follow-up Campus Announcements regarding the status of services, as needed.

Third-party Vendors and Software

In the case of data or service loss by third-party vendors or the use of software not provided by the university, variations will occur depending on the stability and depth of the company providing data, services or software. Within its ability, the university will:

- ensure that provisions related to the prevention and restoration of data and/or services are included in contracts, and also requirements that the vendor back up data regularly and notify the university when data or service loss occurs;
- notify the third-party vendor of observable losses when noted at the university;
- work with the third-party vendor to ensure that data is restored from the last back-up and/or that service is restored as quickly as possible;
- ensure that the vendor provides appropriate communications to the university regarding the status of data and services; and
- receive and interpret vendor communications and/or communicate necessary information via a Campus Announcement, invoking the appropriate requirements of this policy, as appropriate; and provide follow-up Campus Announcements regarding the status of data and services, as needed.

Campus Announcements should stipulate

- the nature of the problem;
- the actions being taken to resolve the problem; and
- the anticipated recovery time, as soon as it is known.

While the university is indirectly responsible for working with third-party vendors and communicating appropriately to the user community, the university cannot be directly held responsible for third-party data losses. Further, should individual faculty, departments, or colleges contract with third-party vendors for data services without the knowledge, authorization, and

approval of the institution, the individual, department, or college will be responsible for ensuring data integrity and communicating with the group of users involved in those services.

Individual Users

Individual users (students and faculty) are responsible for preventing data loss by making backups of coursework data. The minimum recommended number of backups is two. Examples of backup methods include: flash drives, emailing documents to self, use of a third party service such as Carbonite, and backup to external drives. Regardless of the method chosen, backups should be conducted regularly and often, and individuals should "save" their work frequently throughout its creation.

It is also important to note that if an individual is working on a university computer (in offices, in the learning commons/library, or elsewhere on campus), the individual is responsible for making appropriate back-ups and saving often to ensure data integrity. Work being created by an individual during a computer crash is the responsibility of that individual. If back-ups are made sufficiently often, no or minimal loss should occur and restoration should be simple. The exception is if the data cannot be backed up regularly, e.g., during the taking of a test in BlackBoard.

V. Rights in the Case of Data Loss

In the case of data loss as a result of the failure of the university or third-party vendors, i.e., a loss that is not the responsibility of students or faculty, accommodations will be made to mitigate negative consequences that may result. Examples of system failures include:

- unscheduled downtime (a "crash"), where an assignment is due between the time of the crash and the last system backup or the last possible restoration point in the case of a failed backup. This could occur in the LMS or in a computer lab;
- unacceptable patterns of slowness/crash/partial recovery/full recovery occurring when assignments are due or online exams/quizzes/tests are underway, making it impossible for students to meet deadlines;
- third-party service interruption or stoppage where students are unable to complete assignments or work by deadlines; and
- power outages in computer labs during exams.

When possible, Information Technology will notify the university community of system failures, but not all will be immediately visible to a faculty member. If no Campus Announcement has been issued, faculty should verify any student-reported loss with the Information Technology Service Desk to determine if s/he should implement this policy.

It is understood that there are conditions that are beyond the control of an individual. As a result, faculty are advised to provide students with alternate means of submission in event of an application or browser failure or some other condition, and to include a description of these alternate means in their syllabi. Should data loss occur due to a student's not fulfilling his/her responsibility to back up data appropriately, however, the student is responsible for that failure.

VI. Policy Statements

When an institutional data loss or loss of service is verified by Information Technology Services (ITS) and noted on the learning management site (LMS), students will be allowed to resubmit coursework data and re-attempt tests within 72 hours of the implementation of data redundancy measures and the restoration of service by the institution as verified by ITS. If the window for completing coursework or tests is shorter than 72 hours, a new window (start-stop times) can be created by the faculty member, but a time frame of 72 hours takes into account the possibility that loss and restoration might occur over a weekend period.

For required third-party online sites, such as homework sites associated with publishers, the faculty member will post the method for notification of outages or malfunctions with his/her syllabus on Blackboard. Students shall be given at least 72 hours after restoration of service to complete assignments.

When data loss takes the form of a university computer lab failing during an examination period (for example, a blackout occurs during a midterm), the faculty member shall provide an appropriate accommodation for the resumption of the exam.

Beyond these conditions, students bear the sole responsibility for backing up their coursework data and ensuring data redundancy in the event of non-institutional data loss.

In addition to providing statements in their syllabi about accommodations in case of data loss, faculty should also provide a statement to explain students' responsibilities in regards to backing up their data. Suggesting phrasing is as follows:

> "Accommodations will be made for systems failures beyond students' control. These include:
>
> - [list accommodation information here]
>
> Accommodations will not be made for failure to complete an assignment or project because data has not been backed up.
>
> The 'golden rule' for data is that it does not exist unless you back up your data in two or more places on at least two different types of media and make sure that the backup is not in a temporary file that will disappear when you close the program or shut down your computer."