CAROLINAS COLLEGE OF HEALTH SCIENCES
POLICY AND PROCEDURE

ADMINISTRATIVE

SUBJECT: DATA RETENTION, SECURITY, AND RECOVERY

REVIEWER(S): Director, Teaching, Learning and Technology*
Provost

POLICY

The College ensures the security and retention of its data through use of a back-up and retention procedures based on the location of the data and under the guidance and consultation of the system cybersecurity recommendations and officials.

For data that is located on Atrium servers, backups are performed by Atrium Health Information and Analytics Services (IAS) Department and staff under terms of a corporate services contract. Data that is hosted within cloud services such as through our Learning Management System (LMS) data will be maintained through back up methods offered by the third-party vendor as recommended. All users are responsible for data retention and security by following the policies for acceptable use from Atrium Health and the college.

Data security is maintained by all users taking data security seriously, never sharing passwords, being careful not to click on or interact with suspicious links, emails, or programs and reporting threats immediately to either IAS or the college technology support personnel. Teammates are also responsible for maintaining data by saving data in secure locations such as those provided by the system or college. College data should not be stored on personal devices or within personal accounts.

PROCEDURE

A. Teammates should follow Atrium policies to maintain data recoverability by saving data to the available data storage options – Shares Drives, OneDrive, or SharePoint. Saving items locally or on other locations puts data at risk of being lost or mishandled.
  I. Additional data and artifacts will be retained within the learning management system, Canvas. Additional information on student records retention can be found in the RECORDS: PRIVACY, RETENTION AND STORAGE
    i. Canvas by Instructure will maintain a weekly and monthly copy of production data that will reset every Saturday for weekly and on a designated date published by Instructure monthly in the beta and test instances respectively.
    ii. Previous courses will be maintained under past enrollments and accessible to end users for the length of our longest program plus one year. This data may be hidden from the end user for to prevent clutter after 1 year but can be requested for access from the Academic Support team by emailing – support@carolinascollege.edu
B. Data Stored in Atrium Servers
  I. This data will be backed up by the system per system policy IS.PHI 600.03
C. Data Recovery from the Cloud
  I. Usage of the cloud services, OneDrive and SharePoint, are highly recommended since this form of data storage allows for the currently safest method of maintaining and recovering data. Data stored on local devices are at risk of corruption so efforts should be made to maintain data in multiple locations.
D. Disaster Recovery for Shares Drive
  I. In the event that a "restore" of data is needed for our college wide folder, contact the Atrium Support Hotline at 704-446-6161. If a single folder or small subset of data is needed for recovery the Director of Teaching, Learning, and Technology should first be consulted and may be able to restore that content.
  II. For a larger full shares drive restoration, the support technician will contact the server administrator.

III. The Director of Teaching, Learning and Technology will consult with the server administrator to restore the necessary data.

IV. The necessary data will be un-encrypted and restored to the college server.

E. The Computerized Data Backup and Recovery policy and procedure will be reviewed bi-annually.

REFERENCES

Related Policies to Consult

    Carolinas College: ACADEMIC - Records: Privacy, Retention & Storage

    Atrium Health: IS.PHI 600.03 Information Services Security Policy

Related 2024 SACSCOC Standard

12.5 Student records