UAA

UNIVERSITY *of* ALASKA
ANCHORAGE

Addendum to the Policies, Regulations, and Finances Review (PRFR) in response to the PRFR Panel's request for additional information for Standards 2.C.4 and 2.G.5.

Prepared for the Northwest Commission on Colleges and Universities

October 18, 2024

In response to the NWCCU PRFR Panel's initial review of UAA's Policies, Regulations, and Finances Review (PRFR) report, NWCCU requested follow up information about Standards 2.C.4 regarding backup and storage of electronic and paper records and 2.G.5. The below expands upon the responses to these Standards contained within UAA's PRFR report, submitted in August 2024.

2.C.4 - Provide evidence of policies and procedures for backing up of and storage of electronic and paper records.

Per University Regulation R05.08.022, which provides implementation guidance for Board of Regents' Policy P05.08.22, the UA System president "charges the chief records officer and the Office of Records and Information Management with the responsibility to oversee university compliance with state and federal laws and regulations relating to the preservation and destruction of records and information." As per the Records section of the UA System website, the office functions as the designated legal authority to develop records retention and disposition schedules; and to provide a timetable for maintaining information on all campuses, moving records to inactive storage or archiving them, and systematically disposing of records as appropriate. The work of the office is guided by Alaska Statute 45.48, the Alaska Personal Information Protection Act (APIPA). APIPA applies to entities that maintain personal information about Alaska residents in the course of their business.

Through the Office of Records and Information Management, the University of Alaska Records and Information Governance Program (RIM) guides university departments regarding the management of university records and information to comply with legal requirements, Board of Regents' Policy, and best practices for safeguarding records. It addresses the retention and disposition of records, and requires that vendors working with or for the university also meet the guidelines. The program follows the Generally Accepted Recordkeeping Principles developed by the Association of Records Managers and Administrators International (ARMA) that were developed from global best practices resources, including the US federal court case law, American national standards, and the international record management standards ISO 15489.1. These 8 principles include Protection (providing a reasonable level of protection to records and information that are private, confidential, privileged, secret, or essential to business continuity), Retention (maintaining records and information for an appropriate time, taking into account legal, regulatory, fiscal, operational, and historical requirements), and Disposition (providing secure and appropriate disposition for records that are no longer required to be maintained by applicable laws and the organization's policies).

Records Back Up. Records back up aligns with the principle of Protection, noted above. Because the institution has been moving toward electronic records, as per the June 28, 2019 Memorandum for Heads of Executive Departments and Agencies, posted on the UA System Office of Records and Information Management Policy and Regulations website, most records back up occurs in the electronic realm. Paper and other media are backed up per the Records Storage Guidelines. Though clearly dated, these guidelines do address security, as well as backing records up in another location.

The majority of student records are stored in Banner, DegreeWorks, or OnBase. These records are backed up according to the vendors' specific plans. For example, both Banner and DegreeWorks are Ellucian products. Ellucian manages their backup as part of its Managed Cloud Service. Attached is the Ellucian Cloud Backup Procedure Document.

Similarly, OnBase is a Hyland product. The technical aspects of its back-up program are provided in UAA's PRFR report, and repeated here for ease of access. The OnBase platform is hosted by the UA System Office of Information Technology (OIT) in the primary Data Center in Fairbanks. The Data Center is staffed 24/7 and all access is restricted, monitored, and audited. The OnBase system consists of an Oracle Database server and application servers. The Oracle database is monitored by Oracle Cloud Control and uses Oracle's Recovery Manager (RMAN) for backups. The database uses a combination of archive/redo logs and full backups so that recovery to any point in time is possible. The database data, archive logs, and full backups are stored on volumes on the primary enterprise storage array, a pair of NetApp FAS8300s. The volumes are encrypted and configured to replicate out to a paired NetApp Cloud Volumes OnTAP instance in AWS for offsite disaster recovery purposes. The full backups and offsite syncs are done weekly on Sundays and the status of the backups are monitored and alert on failure. The application servers are virtual machines that are backed up daily at 6:15 p.m. and 14 days' worth of backups are retained. The application servers or individual files can be restored from the backups using NetApp's SnapCenter plugin for VMWare vCenter.

For records kept locally, both the UAA Information Technology Services (ITS) and the UA System Office of Information Technology (OIT) back up all on-site critical systems and student records data held on premises on a regular basis (nightly). In addition, these backups are regularly backed up offsite (nightly). UAA ITS backs up critical systems with student records data at its on-site data center at University of Alaska Anchorage and is currently transitioning off-site backups from a third party-hosted data center in Portland, Oregon to using cloud services.

The system-level OIT backs up on-site systems at its data center in Fairbanks, Alaska, with offsite backups generally in Amazon Web Services (AWS). The backups for student data across the UA System Office of Information Technology (OIT) managed systems are handled through various back-up systems, depending on the specific application and the underlying hardware. For example, the newer infrastructure employs native snapshots and replication to AWS for offsite storage. In contrast, applications hosted on older physical servers rely on a mix of native snapshots from the newer enterprise storage system, and/or onsite tape storage via Dell EMC's Networker application, which is then backed up to AWS's virtual tape library for cloud storage. The exact backup method used varies from application to application. The most critical student data resides on the NetApp storage system. For these essential volumes, 26 daily snapshots are taken, with further redundancy provided via SnapMirror (NetApp Storage Systems). This level of volume protection is also applied to most databases containing student data, alongside Oracle DB-level backups. Backups are accessible via the Snap Center plugin in vCenter, which facilitates restoration of entire virtual machines or specific files. Additionally, backups are mirrored to Cloud Volumes ONTAP (NetApp Cloud Storage).

Another database that is broadly used is Maxient. This system is used for conduct, Title IX, and Care Team records. Maxient is supported through the system-level OIT. The vendor backs up all

UA records daily, and keeps 30 days' worth of back-ups. Further, for major decisions such as suspension or expulsion, printed records are also kept. These are stored in a secured area, as per the Dean of Students Office policy on Student Records.

Records Storage, Retention, and Disposition. The OnBase Enterprise Content Management (ECM) system is the official repository for records and official documents for the entire UA System. As designated by the individual retention and disposition schedules, OnBase is used for many student records, including for Admissions, the Registrar's Office, and Financial Aid. As noted above, the system-level Office of Records and Information Management provides Records Storage Guidelines that also address non-electronic records storage and back up.

Per University Regulation R05.08.022, the Office of Records and Information Management provides comprehensive guidance on the retention and disposition of all records, including for student records. These retention and disposition schedules are published on their Retention and Disposition Schedules website. Of particular relevance to Standard 2.C.4 is the very first schedule listed on the site, the Student Records Retention Schedule, titled the Student Enrollment Services Records Retention and Disposition Schedule on the website. This retention and disposition schedule includes records overseen by the Office of the Registrar, the Office of Admissions, the Office of Financial Aid, and Institutional Research. For each record type the schedule includes the record title, the minimum retention time, the custodian/location, as well as additional details as needed. The guidelines at the end of the document address topics such as the storage and back up of permanent records, which should be digitized and stored in an offsite location. As needed, reference is made to the sources of additional guidance, such as the American Association of Collegiate Registrars and Admissions Officers (AACRAO) or the Family Educational Rights and Privacy Act (FERPA).

The information contained in the general Student Records Retention Schedule described above is expanded upon by more detailed schedules for the particular areas, such as the Registrar Records Retention and Disposition Schedule, Financial Aid Retention and Disposition Schedule, and College Savings Plan and Scholarship Program Retention and Disposition Schedule. In addition to the record types, the minimum retention time, and the custodian location, these schedules identify OnBase as the official repository for these records, and provide additional guidance regarding the disposition of the records, referring to specific references, regulations, and best practices, as well as the state law that covers the disposal of records containing personal information, the Alaska Personal Information Protection Act (APIPA) AS 45.48, mentioned earlier.

Addendum Evidence for 2.C.4:
Policies and procedures for backing up of and storage of electronic and paper records Alaska Statute 45.48 - The Alaska Personal Information Protection Act (APIPA) Regents' Policy P05.08.022 - Records and Information Retention and Disposition University Regulation R05.08.022 **-** Records and Information Retention and Disposition

Addendum Evidence for 2.C.4:

UA System Office of Records and Information Management - Website

- Records – Website
- Records and Information Management (RIM) Governance Program - Website
- Retention and Disposition Schedules - Website
    - Student Records Retention Schedule
    - Registrar Records Retention and Disposition Schedule
    - Financial Aid Retention and Disposition Schedule
    - College Savings Plan and Scholarship Program Retention and Disposition Schedule
- Records Storage Guidelines - Website

UAA Student Conduct Records - Retention and Access - Website

2.G.5 - Recommend updating links to reflect most current student cohort loan default rates on institutional website.

UAA publishes the Cohort Default Rate in two places on the institution's website. These are linked to each other for ease of student navigation.

The most recent Cohort Default Rate reported to UAA by the US Department of Education on September 25, 2024 is 0.00%. It is published on the UAA Financial Aid Loans webpage, highlighted in the green box.

The Cohort Default Rate is published also on the UAA Student Consumer Information website under Student Financial Assistance, Tuition, and Fees. This site had not been updated at the time UAA submitted its PRFR report to NWCCU. UAA's Student Consumer Information page is now updated to match the UAA Financial Aid Loans webpage.

Addendum Evidence for 2.G.5:

Most current student cohort loan default rate published

UAA Office of Financial Aid - Loans - Website - Cohort Default Rate is at the end of the Federal Loan Programs section

UAA Student Consumer Information - Website - Cohort Default Rate is the first item under Student Financial Assistance, Tuition and Fees

Cloud Resources

Reference

May 9, 2024

Notices and Privacy

In preparing and providing this publication, Ellucian is not rendering legal, accounting, or other similar professional services. Ellucian makes no claims that an institution's use of this publication or the software for which it is provided will guarantee compliance with applicable federal or state laws, rules, or regulations. Each organization should seek legal, accounting, and other similar professional services from competent providers of the organization's own choosing.

Ellucian's Privacy Statement is available at: www.ellucian.com/privacy.

Ellucian shall have the right to (a) use, store, process, modify, reproduce, distribute and display customer data, and to grant sublicenses to third parties, for the sole purposes of providing the software, performing Ellucian's obligations under its agreements with customers and complying with applicable law or legal requirements; (b) use, store, process, modify and reproduce customer data for Ellucian's internal business purposes, including development, diagnostic, forecasting, planning, analysis and corrective purposes in connection with the software, and for otherwise improving and enhancing the software; and (c) use, store, process, modify, reproduce, display, perform, distribute, disclose and otherwise exploit in any manner Aggregated Data for Ellucian's business purposes, including disclosure within its public statements and marketing materials describing or promoting Ellucian or the software. “Aggregated Data” means any data obtained or generated by Ellucian, including data pertaining to the software, Ellucian's systems and software, and the use of any of the foregoing, and includes data derived from customer data, which in all instances (i) does not identify any individual and (ii) is not attributed or attributable to a specific customer. Aggregated Data includes data that has been combined into databases which include third party data.

Ellucian
2003 Edmund Halley Drive
Reston, VA 20191
United States of America

Contents

Backup services. 4

Backup services

Updated: February 27, 2023

Ellucian Cloud performs data and configuration file backups for customers as part of the Cloud service.

A backup is the process of saving the operational state, architecture and stored data of database software, into an archive file, at various points in time.

Database and configuration file backups provide protection from loss events, by allowing replication of the lost database and configuration files with the archived file or files.

This policy describes the following:

- **Backup Intervals and Retention Periods:** The frequency with which Ellucian captures backups and how long that information is saved.
- **Extended Data Retention Periods:** Requests that data be retained outside of standard guidelines.
- **Restoration Scenarios:** Reasons customers may need to request that Ellucian use backed up data to replicate a database.
- **Roles and Responsibilities (RACI Matrix):** The responsibilities of Ellucian and customers, while backing up and restoring data.

Backup Intervals and Retention Periods

Ellucian Cloud will conduct regular, point-in-time backups of all customer data. We separate the retention of this backup data into **Daily** and **Monthly** components.

Backups will adhere to Ellucian's internal backup controls.

The following table summarizes database backup retention periods by backup intervals for production environments.

Backup Interval	Production Minimum Retention Period
Daily	7 Days
Monthly	3 Months

Note: Customers may request ad hoc backups before significant system or configuration changes. Please contact your Cloud Service Delivery Manager (CSDM) to discuss ad hoc backup requests.

Extended Data Retention Periods

Ellucian does not retain backups beyond the periods above. At the end of these durations, we delete the oldest backups. Customers may request copies of database backups for archival purposes, when retention needs extend beyond defined Ellucian standards. Database backups may be requested up to one monthly.

Upon such request, Ellucian will make a copy of the database available to the customer for secure download for up to 30 days. Each database backup made available in this manner will replace the previously available backup. It is the customer's responsibility to retrieve and store its database backup in a timely manner.

Restoration Scenarios

When a customer's database or configuration files are lost (e.g., see below), Ellucian Cloud will use the data from the saved backup to restore the database in the Cloud environment.

The following scenarios outline a few reasons for which a backup restoration may be necessary:

- Data deleted in error.
- Table or record deleted or updated erroneously.
- Task schedule or Cron script modified erroneously.
- Log file removed or overwritten.

Roles and Responsibilities (RACI Matrix)

The following RACI matrix illustrates the key roles and responsibilities of Ellucian Cloud and customers.

- Responsible: The party or parties who execute the task.
- Accountable: The party or parties who provide approval for the task.
- Consulted: The party or parties who must receive the appropriate information to provide feedback needed to execute the task.
- Informed: The part or parties who must receive information regarding the ask.

Task	Responsible	Accountable	Consulted	Informed
Maintaining the accuracy of the customer data contained in the Cloud Software.	Customer	Customer	Ellucian	Ellucian
Deploy and maintain architecture for backup services.	Ellucian	Ellucian	N/A	N/A
Deploy and manage tooling that is needed to meet Ellucian Managed Cloud	Ellucian	Ellucian	N/A	N/A

Task	Responsible	Accountable	Consulted	Informed
backup, restoration, and retention standards.				
Validate backup runs as scheduled and troubleshoot any failures.	Ellucian	Ellucian	N/A	N/A
Take point-in-time daily production environment backups and retain for 7 days.	Ellucian	Ellucian	N/A	N/A
Provide instructions for submitting and accessing extended data retention requests.	Ellucian	Ellucian	N/A	Customer
Provide instructions for submitting requests for database or configuration file restoration.	Ellucian	Ellucian	N/A	Customer