POLICY 2.65: ACCOUNT RETENTION

This policy establishes the retention, management and deactivation processes for student and employee accounts within Sandburg for information systems. The policy ensures compliance with applicable laws, including the Family Educational Rights and Privacy Act (FERPA), Illinois Local Records Act, data-privacy regulations and institutional record-retention requirements.

The policy applies to all college-issued accounts used to access email, LMS platforms, administrative systems, cloud storage, collaboration tools and any associated digital services.

Student accounts

Retention period

ACTIVE STUDENTS

Accounts remain active for the duration of the student's enrollment, as defined by the registrar.

GRADUATED STUDENTS

Accounts remain active for 12 months following graduation.

WITHDRAWN OR INACTIVE STUDENTS

Accounts remain active for six months following the last date of attendance (LDA).

Notification

Students will receive three notifications 90 days, 30 days and seven days before account deactivation. Notifications will include instructions for backing up or exporting personal data.

Data backup responsibilities

Students are responsible for saving or exporting any personal data before account deactivation. IT will guidance upon request via support@helpdesk.com.

Account deactivation and data handling

- After the retention period expires, student access will be terminated.
- Account contents will be retained in a recoverable state for **30 days**, exclusively for institutional record-keeping purposes.
- Data constituting **student educational records** — including submissions within the LMS — will be retained and managed according to the college's official record-retention schedules and FERPA requirements.

- Student email accounts may be permanently deleted after the 30-day recoverable window, as record copies of any required FERPA-governed communications will be retained by faculty and staff recipients.

Exceptions

Extensions of student email access for alumni engagement may be approved jointly by Student Development and IT. Access extensions do **not** extend institutional obligations for record retention.

Employee account retention

Retention period

ACTIVE EMPLOYEES

Accounts remain active for the duration of employment.

SEPARATION (VOLUNTARY OR INVOLUNTARY)

Employee access to all college systems and email will be terminated immediately upon separation. This aligns with legal guidance to prevent unauthorized access, use, modification or removal of institutional data.

RETIRED EMPLOYEES

Access to core systems is terminated at retirement. Limited continued access (e.g., to retiree benefits platforms) will be provided only through personal credentials established by the employee with the third-party provider.

Data preservation and backup

- Employees may transfer personal (non-college) data prior to separation.
- Upon separation, supervisors must identify institutional data that must be preserved and coordinate with IT to ensure transfer to the college prior to access removal.
- No data — email, documents, files or messages — may be deleted or removed by the employee after separation.
- All employee account contents constitute college property and are retained in accordance with the Local Records Act and College record-retention schedules.

Account deactivation and data handling

- Access is immediately disabled upon separation.
- The account and its contents will remain in a secure, recoverable administrative state for **60 days** to support operational continuity and record-retention evaluation.
- Data will be preserved or disposed of only in accordance with the Illinois Local Records Act and approved destruction processes.

Access transfer

Supervisors must work with IT prior to separation to ensure all critical institutional data (email, shared storage, project documents, etc.) is transferred to designated personnel or repositories.

Exceptions

Extended access for project continuity or transitional needs may be granted only when approved jointly by HR and IT and must not conflict with legal requirements or institutional security controls.

Compliance and review

This policy complies with FERPA, the Illinois Local Records Act, GDPR (where applicable) and all institutional data-governance standards. The policy will be reviewed annually by IT in collaboration with Student Development and Human Resources.

Original: 12/25