Luther Seminary Faculty and Staff Account Deletion Policy

I. Rationale:

Data security and integrity are critically important in the maintenance of Luther Seminary's information systems. When a faculty or staff member is no longer employed by the seminary, his or her access to all electronic resources will be immediately interrupted. This access includes (but is not limited to) LutherNet account and voicemail services. This process describes this interruption and the steps toward permanently closing IT accounts.

There are two main scenarios this policy covers: voluntary and involuntary terminations. In addition, a process for faculty and staff who are also students is noted below.

II. Definitions

Disabling an account – Changing the account password which prevents future logins.

Active logins – An open session to IT systems that exists from a prior login.

III. Voluntary Termination:

This document considers a voluntary termination when a faculty or staff member has made arrangements to end their affiliation with Luther at a designated future date. This process is initiated when IT is informed by Human Resources or the Dean's Office of the departure plans. In the case of a rapid voluntary termination the process will follow the involuntary termination steps.

IT Responsibilities:

- The Liaison for Computing will assist the employee in archiving any personal electronic files, personal emails, or personal contacts if the employee desires.
- The Liaison will work with the employee's supervisor or faculty's department chair to move any Seminary files out of the employee's personal file space.
- The Liaison will work with the employee's supervisor or faculty's department chair to retrieve any Seminary equipment, such as a laptop, per the Human Resources termination procedures.
- The Liaison will disable LutherNet account at the end of business on the designated day unless other arrangements have been made; with approval from Human Resources. Any active logins will also be closed. Any other arrangements must be approved by an IT Director and the employee's supervisor or faculty's department chair.
- The Liaison will reset the voicemail password at the end of business as well.
- The LutherNet account should be deleted within 7 business days of the employment end date. If the account is not to be deleted within 7 business days the Liaison must note the date for deletion in the account notes field.
- The voicemail box should be deleted within 7 business days of the employment end date.
- The phone extension should then be relabeled as *available* in the phone system.

Employee Responsibilities

- Employee must select and pass on any email communication important for continuing work to employee's supervisor (or supervisor's designate). Emails can be passed on by means such as forwarding, archiving or similar. The Liaison can assist with the process.
- If the employee wants to retain any personal files, personal emails, or personal contacts they must contact their Liaison before their employment end date if they require assistance.

IV. Involuntary Termination:

This document considers an involuntary termination when a faculty or staff member's affiliation with Luther is ended immediately. This process is initiated when IT is informed by Human Resources or the Dean's Office of the departure plans. Human Resources or the Dean's Office must contact an IT Director in the case of Involuntary Terminations; an IT Director will determine the appropriate IT staff resources to complete the IT Responsibilities.

IT Responsibilities:

- The former employee's account will be disabled immediately and any active logins closed immediately.
- The former employee's voicemail box password will be reset immediately as well.
- The account should be deleted within 7 business days of the employment end date. If the account is not to be deleted within 7 business days the designated IT staff must note the date for such action in the account notes field.
- The voicemail box should be deleted within 7 business days of the employment end date.
- The phone extension should then be relabeled as *available* in the phone system.
- If the supervisor (or designate) requires work-related emails from the former employee's account the process will take one of two forms.
    - Designated IT staff will meet with supervisor (or designate) and perform a subject line only scan to determine which messages should be passed on.
    - Failing (1) being feasible, the request is referred to the Director of IT or the CIO.
- The email forwarding and bounceback policy will also be followed.
- If the supervisor (or designate) requires work-related files from the former employee's storage locations (i.e. network storage, computer storage) designated IT staff will make those files available in a secure location.
- If the former employee requires any personal files, emails, or contacts they must arrange this retrieval with their Liaison in consultation with employee's former supervisor or faculty's former department chair. This retrieval will take one of two forms.
    1. The former employee will meet with the Liaison on campus and will request which items are to be retrieved. The Liaison will produce a CD/DVD free of charge with the files, emails or contacts and give the CD/DVD to the former employee.
    2. The former employee will request which items are to be retrieved. The Liaison will produce a CD/DVD free of charge with the files, emails or contacts. The former employee will make arrangements to pick up the CD/DVD from Human Resources.

V. Employees who are also students:
In the case that an employee departs who also a current student, the access to student resources needs to be retained.

IT Responsibilities

- The student employee account will follow the above procedures as a separate student-only account should exist already.

Employee Responsibilities

- As the account will only be moved, not deleted, all personal files, personal emails and personal contacts will be retained in the account.

VI. Deletion Review:
A monthly review is required to be performed by either the Director of Information Technology or their designated representative to ensure that all flagged accounts have been removed and/or disabled if retention of the account is required for legal or other reasons.

Revision History

Revision	Change	Date
1.0	Original Version	1/15/2019
1.1	Procedures updated	1/25/2019