LUTHER COLLEGE

POLICIES AND PROCEDURES

| | |
|---|---|
| Department: | ITS |
| Subject: | Network Use Policy |
| Date Issued: | September 13, 2018 |
| Date Revised: | |
| Approved By: | Reviewed by Cabinet, Approved by President |

## I. Policy/Procedure

This document outlines the policy for network use of information technology solutions.

## II. Purpose

The purpose of this policy is to inform and educate the Luther College community of the rights and responsibilities associated with use of the College's data networks. This policy governs the use of Luther's data and data networks, and applies to students, faculty, staff and anyone else who is authorized to use these resources. The College reserves the right to modify this Policy at any time, with or without notice.

## III. Scope

This policy applies to all students, faculty, staff and anyone else who is authorized to use the Luther College network.

## IV. Procedures and Guidelines

A. Acceptable Use

- Luther College, as part of a continuing commitment to faculty, students, alumni, and staff, provides certain information technology resources, including telecommunications and computing equipment, and access services. These resources include centralized servers for email, Internet access, administrative applications, academic applications, and data; a fiber based campus network backbone as well as associated network hardware and software which distribute network resources to academic, administrative, and residential buildings; desktop resources such as computers, printers, and software; as well as access to campus and global information resources. These resources are to be used for education, research, and administrative purposes related to the mission of the College, and consistent with appropriate College policies and codes of conduct. It is expected that users of campus information technology resources will respect the priority of these purposes.
- As a Luther student, faculty, or staff member, you are encouraged to use these resources. By using these resources, you agree to abide by all policies and procedures of the College. Luther College expects ethical and responsible behavior. You are expected to conduct yourself as appropriate for any good citizen and you will not participate in any illegal activity, any for-profit commercial activity, or other conduct, communication, or activity that will negatively impact Luther College or other users of the College's information technology resources.

- Use of these resources is governed by and is subject to all applicable College policies. For student governance, see the Student Handbook for details of the Luther Code.
- For details on faculty or staff governance, see the respective handbook or other authorities that describe the Luther Code as it applies to faculty and staff.
- Failure to comply with these, or any other applicable policies, will result in sanctions as outlined in those policies and denial of access to the College's information technology resources.
- By using the information technology resource provided by the College, you are indicating your acceptance of this policy and your promise to abide by it.

B. Property Rights and Privacy
- The equipment, data network, and other technology resources provided by the College are the property of the College, and shall be used only for purposes consistent with the Acceptable Use policy. The College may monitor the use of its resources, including the Internet. Users shall have no expectation of privacy in the College technology resources or any materials within, including email and stored files.

C. Copyright
- Luther considers it the responsibility of each member of the College community to ensure that their academic or administrative work is in compliance with appropriate copyright law. This covers transmission, reproduction, storage, manipulation, and use of intellectual property.
- If using copyrighted works in academic or administrative endeavors, it should only be in "fair use" under copyright law. Information and guidance on "fair use" is available on the College's ITS website. Faculty are responsible for ensuring that all course materials used in their courses are being used appropriately with the proper permissions secured. Students are expected to complete assignments and work under "fair use" provisions or to arrange licensing in other cases.
- For Luther's full copyright and intellectual property policies, please see: http://www.luther.edu/copyright

D. Electronic Harassment and Social Media
- All content posted with the use of Luther College data networks, systems, or equipment (including posts accessed through a private user account over the College wireless network), and the use of social media to represent the College and members of the College community, are subject to all College policies and may not remain private or be limited to the user's intended audience. Luther College reserves the right to monitor all content transmitted or stored on its data networks, systems, or equipment. Luther College reserves the right to take appropriate action against students who improperly use Luther College's network, systems, and equipment, including harassment, eavesdropping, or other inappropriate behavior.
- In general, the following activities are considered disruptive to learning and/or a professional workplace environment, and an inappropriate use of the College's data network, systems, and equipment. Members of the College community engaged in inappropriate activities, including but not necessarily limited to the following, may be subject to discipline:
    - Any use of technology that creates, distributes, accesses, or transmits harassment, intimidation, threats, or otherwise takes advantage of peers or colleagues;
    - Any use of technology that violates the College's Bias Incident, Hate Act, Hate Crime, Discrimination, and Harassment Policy, or any other conduct policies applicable to students, faculty, or staff; or

- Any use of technology that creates, distributes, accesses, or transmits abusive, discriminatory, slanderous, libelous, or sexually explicit material.

- All College community members are reminded that use of social media such as Facebook, Twitter, Snap Chat, LinkedIn, etc. involves disclosure of personal information to others which can result in increased risk to you. Social media is increasingly being exploited for fraudulent and illegal activity including theft, blackmail, extortion, and slander. Luther strongly advises those who choose to participate on social media to exercise caution and to remain vigilant against individuals who seek to cause harm. Individuals who witness or learn about an incident of inappropriate use of social media within the College community are encouraged to immediately report such inappropriate use to College officials. The College will investigate reported incidents and will pursue sanctions against those in our College community who use these services for any illegal or inappropriate purpose.

E. File Sharing

- Peer-to-peer file sharing can be an efficient way to share files for which you have legal license to distribute or receive via computer networks. There are many software clients that enable file sharing operating on networks, for example, BitTorrent. Luther blocks access to peer-to-peer file sharing protocols in compliance with the Higher Education Opportunity Act of 2008.

- Receiving or transmitting files for which you do not have legal license to distribute (such as music or movies) is not permitted and is in many cases an illegal act punishable under criminal and/or civil law. Luther will contact any user found to be violating this policy with information regarding the claimed infringement. Failure to respond to and address the claimed infringement notice and associated activity may result in loss of network privileges and referral to the campus judicial system.
- The College has received infringement notifications that have resulted in the suspension of network privileges. If you are engaging in file sharing activity on Luther's network there are a number of issues that you should be aware of and consider:
    - All users of Luther's network resources are legally responsible for their own actions. Luther as an institution cannot, and will not, provide legal protection for online activities, and we will cooperate with any lawful legal action directed at users of our network.
    - Luther does not currently have any active processes to monitor the legality of traffic on our network. We believe users should be responsible for their actions and that it is not Luther's responsibility to police compliance.
    - Access to internet resources that are deemed to pose a threat are blocked to protect the security of the network. Additionally, we will shape and limit bandwidth to individual users to ensure a positive network experience for all.
    - People (and computers) are watching what you do online. If you are sharing files for which you do not own legal license to distribute, you run a good risk of being identified by copyright holders. When we are notified of fraudulent acts committed on our network, we track who was responsible for the activity and hold them accountable for that activity.
    - Installing and operating a personally-owned wireless access point attached to Luther's network is not permitted. Any community member that installs wireless access points on the Luther network may have their access to network resources disabled and will be held responsible for all activity that occurs on that access point. This includes anonymous use by others of your access point. In cases where file sharing or other illegal activity occurs over open access points, we have and will continue to pursue punitive measures against the owner and operator of the wireless access point.
- Luther encourages users who choose to acquire digital media to use legal and licensed services.

- For additional questions on Luther's file sharing policies, please contact helpdesk@luther.edu. For more information on your legal rights and responsibilities, please contact your legal advisor.

F. Granting and Removing Network Access

Granting Network Access

- The following individuals are issued credentials (Norse Keys) to access network-based services at Luther while they are active members of the Luther community:
    - Students (regardless of enrolled credit hours)
    - Faculty (regardless of course load or contract status, provided they receive compensation from Luther)
    - Administrative Staff (regardless of contract status, provided they receive compensation from Luther)
    - Contract Staff (regardless of contract status, provided they receive compensation through an authorized service contractor)
    - Employees with Emeritus Status (Faculty or Administrative Staff)
    - Alumni
- The following individuals are not automatically authorized to receive credentials (Norse Keys) to access network-based services at Luther. Requests for credentials to be issued to any individual within one of the groups below should be made in writing to the Executive Director of Information Technology Services:
    - Volunteers
    - Independent Contractors
- Generally, credentials are automatically generated through workflows established for students and employees. ITS requests that supervisors hiring new employees also complete our New Employee Setup Form available at:

  https://www.luther.edu/helpdesk/lisforms/newemployee/.

Removing Network Access

Graduating Students

- Seniors will be contacted by May 1st via email with a message from ITS regarding the transition of their accounts. Any student with a valid reason to keep their account active as a student will be directed to a web form. All other accounts will be transitioned to alumni accounts.
- Software Development will provide Network & Systems with a list of graduating seniors by June 1st.
- All graduating students will have their accounts transitioned from student accounts to alumni accounts on July 1st of their graduating year.
- Alumni will have access to the online alumni directory and alumni data via their Norse Key.
- Norse Apps will remain available to alumni.

Non-Graduating, Non-Enrolled Students

- Software Development will provide Network & Systems with a list by October 1st of students who:
    - did not graduate in the past year, and
    - did not enroll in any of the previous three fall/spring terms or in between.
- Students will be contacted by October 15th via email with a message from ITS regarding the transition of their accounts. Any student with a valid reason to keep their account active as a student will be directed to a web form.

- All non-graduating students who have not enrolled in courses for the fall semester will be transitioned either to an alumni account or an inactive account on November 1st of each year based on their individual criteria.
- For students qualifying as alumni, Norse Apps will remain available and alumni data will be accessible via the online alumni directory. For students not qualifying as alumni, Norse Apps accounts will be deleted November 1st.

Faculty

- Faculty accounts will expire on their employment end date.
- ITS will work with HR to acquire advance notice of these expirations. Notice will be made to ITS and distributed via KBOX to Network and Systems, Software Development, ITS Web Lead, KATIE Lead, Workstation Support Lead. The work order will include all date information, including any approved extensions.
- Faculty will be contacted by email with a message from ITS regarding the transition of their accounts. Faculty with a valid reason to retain an active faculty account will be directed to a web form where they can request a one month extension for their account to remain active. Any extensions longer than one month will require approval of the Dean of the College and the Executive Director of ITS.
- For faculty qualifying as alumni, they will retain their Norse Apps account and transition to an alumni account. Emeriti will retain their Norse Apps account indefinitely, unless a request is made to have it removed. For all other faculty, accounts will be initially disabled on their employment end date, and then deleted two months after their employment end date (or extended employment end date).
- Any college data stored on Luther servers (including H drive) will be retained for a period of two months after the account expiration, and then deleted. No requests for restores will be granted after that date.
- Voice services will be disabled/deleted on the employment end date (or extended employment end date).
- Faculty will be asked to meet with ITS staff to return/inventory all technology equipment.

Staff and Contract Staff

- Staff/Contract Staff accounts will expire on their employment end date.
- ITS will work with HR to acquire advance notice of these expiries. Notice will be made to ITS and distributed via KBOX to Network and Systems, Software Development, ITS Web Lead, KATIE Lead, Workstation Support Lead. The work order will include all date information, including any approved extensions.
- Staff and their immediate supervisors will be contacted by email with a message from ITS regarding the transition of their accounts. Staff with a valid reason to retain an active staff account will be directed to a web form where they can request a one month extension for their account to remain active. Any extensions longer than one month will require approval of their Vice President and the Executive Director of ITS.
- For staff qualifying as alumni, they will retain their Norse Apps account and transition to an alumni account. For all other staff, accounts will be initially disabled on their employment end date, and then deleted two months after their employment end date (or extended employment end date).
- Any college data stored on Luther servers (including H drive) will be retained for a period of two months after the account expiration, and then deleted. No requests for restores will be granted after that date.
- Voice services will be disabled/deleted on the employment end date (or extended employment end date).
- Staff will be asked to meet with ITS staff to return/inventory all technology equipment.

Death

- Upon the death of a student, ITS will work with the Dean for Student Life to determine how to transition digital content owned by the student prior to deletion, in accordance with applicable state and federal laws.
- Upon the death of a faculty member/staff/contract staff person, ITS will coordinate with the department head/supervisor to take control of and appropriately distribute any digital content owned by the individual prior to deletion.

Email Notices from ITS Regarding Removal of Network Access Includes:

- Summary of ITS Exit Policy with link to full text
- Reminder of Luther Policies on Intellectual Property and Ownership of Data
- Links to instructions for exporting or transferring email to another employee/service
- Links to instructions for exporting or transferring Norse Docs data
- Links to instructions for exporting or transferring KATIE content
- Links to instructions for exporting or transferring files stored on Luther servers
- Link to web form requesting special consideration
- Overview of timeline and deadlines
- Note to work with supervisor/colleagues to retain/transition critical data
- Notice to return any ITS/Library materials currently checked out to them (including interlibrary loan materials) and a link to review their circulation records.
- How to acquire lower-cost software/hardware (auction/academic pricing).

G. Norse Key Password Policy
Date Issued: September 12, 2007
Date Revised: November 7, 2016

I. Policy

In order to maintain appropriate network security, all users of Luther College networks and systems are required to use Google 2-Step Verification and periodically change their Norse Key password according to criteria established by Information Technology Services.

II. Purpose

Common security practice at institutions of higher education and businesses require regular changes of passwords to maintain secure access to resources.

III. Scope

Applies to all faculty, staff, students, and other users who have a Norse Key.

IV. Terms and Definitions

- Norse Key - A Norse Key is your gateway to most digital resources at Luther College. Specifically, it is your username and password that are used to log onto services such as your Luther email, My.Luther.edu, the campus directory and many others.
- Norse Key Accessible Services
  - Norse Mail and other Norse Apps
  - My.Luther log on
  - Lab computer log on
  - katie.luther.edu log on
  - Colleague (Ellucian/Datatel)
  - Academic H:, T: and departmental drives (students/faculty)
  - Administrative H:, T: and departmental drives (staff)

- Network registration (http://network.luther.edu)
- Workstation log on (Faculty, Staff, and Students)
- Help Desk Self Service (http://help.luther.edu)
- Campus directory log on (http://directory.luther.edu)
- Alumni directory log on (https://www.luther.edu/alumni/directory/)
- Qualtrics survey software (http://qualtrics.luther.edu)
- VoiceThread (http://luther.voicethread.com)
- Off-campus access to Library resources (e.g. Academic Search Premier, JSTOR, Project Muse, etc.)
- Interlibrary Loan (http://illiad.luther.edu)
- Citrix remote access system (http://citrix.luther.edu/)
- Slate Admissions customer relations management
- Content: ImageNow Document Imaging system

o Services Not Currently Accessible via Norse Key
- CBORD Odyssey PCS - Contact Technology Help Desk to synchronize Norse Key and PCS password.

V. Procedures and Guidelines

1. Policy Statements
   - All Norse Key passwords must be changed every 180 days.
   - Passwords must be at least 10 characters long.
   - Passwords must contain at least one number.
   - Passwords must contain at least one character.
   - Passwords cannot be blank and cannot contain any spaces or special characters.
   - Paper on which passwords are written must either be destroyed after use or stored in secure locations.
   - A password history will be retained and require users to use original passwords when updating them.
   - Users must review the college Statement of Responsibility and signify their compliance as a condition of changing their Norse Key and being granted access to the Luther College network.

2. Implementation
   - Colleague System User passwords are currently changed every 180 days.
   - Users will receive five notification/reminder messages prior to the expiration of their password. The first will be sent two weeks prior to expiration, the second one week prior to expiration, the third 3 days prior to expiration, the fourth 2 days prior to expiration, and the fifth 1 day prior to expiration. Users will be prompted to visit norsekey.luther.edu to change their Norse Key password.

VI. Confidentiality and Record

Information Technology Services is responsible for assuring the Norse Key passwords expire every 180 days.

H. Norse Key Security

College community members should not share or reveal their Norse Key credentials with anyone. In particular, ITS will never ask for your Norse Key via email. Requests for your login information received via email are invariably attempts to compromise your account.