Technology Acceptable Use

LP 7.5

Policy Effective Date:
6/11/19

Last Revision Date:
6/11/19

Approved by Trustees:
6/11/19

Policy Owner:
Board of Trustees

Policy Administrator:
CIO

Affected Parties:
Faculty
Staff
Students

Table of Contents:

I Summary

This policy governs the use of Lander University's information technology resources ("university resources"). Lander University promotes the responsible use of these resources to support the academic, business, and public service activities of the institution, and the needs of the Lander community. Unauthorized use of university resources is prohibited. Lander University and its Information Technology Services (ITS) staff will take necessary action to protect the confidentiality, integrity, and availability of these resources.

II Scope

This policy applies to all users of Lander University resources, regardless of where or how the resources are accessed. All users are responsible for reading, understanding, and complying with this policy.

III Definitions

A. Authorized University Officials

Authorized University Officials are the Chief Information Officer (CIO) or designee, Human Resources Director or designee, and General Counsel.

B. Credentials

Usernames, passwords, and/or any other means of authenticating a user to grant access to university resources.

C. Data Custodians

Individuals who control access to specific sets of university information.

D. Information Security Incidents

Events that compromise the confidentiality, integrity, and/or availability of university resources.

E. Information Technology Resources ("University resources")

University-owned computer- and network-related hardware, software, services, accounts, credentials, and data.

F. Minimum Security Requirements

The baseline settings necessary for any device accessing university resources. The device must be free of detectable malicious software, have current and active antivirus software, and have current operating system and application updates (applied within 30 days of release).

Technology Acceptable Use

G. Personal Devices

Any computers, tablets, phones, or other appliances not owned or leased by Lander University that are used to access university resources.

H. Users

All faculty, staff, students, contractors, temporary employees, guests, and any other person or system accessing or having access to university resources.

IV Policy

A. General

1. University resources, including data, user accounts, and credentials, are the property of Lander University.
2. Use of university resources must comply with local, state, and federal laws, and all other university policies.
3. Users have a personal responsibility for the appropriate use and protection of university resources.
    a. Users must ensure that their actions do not compromise the confidentiality, integrity, and/or availability of university resources.
    b. Users are responsible for any activity initiated or conducted by their account or credentials, unless a violation is the result of an event beyond the user's control.
4. Any device, including personal devices, used to access university resources is also subject to this policy.
5. Users must immediately report the loss or theft of university resources to ITS or the Lander University Police Department.
6. The use of unauthorized external or third-party support, service, or repair for university resources is prohibited.
7. Users must utilize only authorized services to conduct official university business.
8. Limited personal use of university resources is acceptable as long as official university operations are not adversely affected. If necessary, individual departments may create personal use guidelines that are more restrictive.
9. Accessing or using university data for personal matters is prohibited.
10. Lander University is not responsible for technical support related to the personal use of university resources, including the recovery or transfer of personal data. Personal use and/or personal data issues will not take priority over support of official university activities.
11. Users should have no expectation of privacy when utilizing university resources. Lander University reserves the right to examine email messages, individual computer files, mobile devices, web browser cache files, and other information stored on or passing through university resources. Authorized university officials may conduct such examinations at any time and without prior notice to ensure compliance with internal policies, assist with internal

investigations, and assist with the management and protection of university resources. The university may be compelled to release such information in response to government or court-ordered legal actions.

12. Users are expected to behave in a reasonable, responsible, courteous, and professional manner when utilizing university resources. Prohibited conduct includes, but is not limited to, the following:
    a. Sending, storing, or accessing obscene messages or materials;
    b. Using any computer, device, account, credentials, and/or network to gain unauthorized access to any university system, service, or account;
    c. Using any university resource to gain unauthorized access to any non-university system or service;
    d. Using university resources for commercial activity outside of the Intellectual Property policy;[1]
    e. Illegally downloading, obtaining, or copying software or intellectual property protected by copyright;
    f. Using university resources for unauthorized fundraising, solicitations, political campaigning, or other activities inconsistent with the university's tax-exempt status.

    Failure of this policy to address specific inappropriate behavior does not imply that such behavior is sanctioned.
13. Data custodians are responsible for:
    a. Maintaining records of access granted to employees or other authorized users;
    b. Notifying ITS of any changes in employee duties so that access may be modified or terminated;
    c. Ensuring that any university data possessed by an employee or other authorized user is preserved prior to duty change or separation from the university.

B. Security

1. Full-time and part-time faculty and staff are required to complete annual security awareness training.
2. Users with access to sensitive university data must protect that information in accordance with any applicable state and federal privacy laws.[2]
3. Passwords used to access university resources must comply with the Lander Account Password policy.[3]
4. Users must protect passwords and any other account credentials used to access university resources.[4] Except in special circumstances, the sharing of passwords or other account credentials is prohibited.[5]
5. Users must lock their computer screen or sign out of any system before leaving it unattended.
6. When accessing university resources on a personal device, users must ensure that the device meets minimum security requirements.

7. Users are responsible for reporting to ITS any suspicious email/computer activity and any potential information security incidents.
8. Lander University is not responsible for any personal losses incurred as a result of a user's interaction with phishing/scam emails or malicious software.
9. Users may be held accountable and subject to disciplinary action if their interaction with phishing/scam emails or malicious software adversely affects Lander University.

C. System and network

1. Unauthorized access to university systems and/or networks is prohibited.
2. Users must not intentionally introduce malicious software (e.g., viruses, worms, and Trojan horses) into university systems or networks.
3. Users must not intentionally cause or contribute to network disruptions, including but not limited to network sniffing, packet spoofing, denial of service attacks, and other malicious activities.
4. Users are prohibited from conducting any form of network monitoring or scanning, unless such activity has been authorized for academic, ITS, or other official university purposes.
5. University storage media must only be used for storing authorized and appropriate university data. Storing personal or non-university data on university storage media is prohibited. Access permissions of university storage media must be consistent with the most restrictive access permissions of any stored data.

D. Email and communications

1. Official Lander University email accounts are created for all eligible faculty, staff, students, and other individuals as deemed necessary by university administration. Users provided with a university email account must use this account when communicating as a representative of the university and when conducting official university business. Users are prohibited from using any unauthorized third-party email accounts (including any associated services) to conduct university business.
2. Users must exercise extreme caution in using email to communicate confidential or sensitive matters. If sensitive information must be sent through email, the message must be secured by encryption.[6]
3. Users are prohibited from automatically forwarding university email to a third-party email account.
4. Misrepresenting, obscuring, suppressing, or replacing a user's identity is forbidden. The username, email address, organizational affiliation, and related information included with the message must reflect the actual originator of the communication.[7]
5. To assist the university in avoiding charges of libel, defamation of character, and other legal problems, uncivil communication is strictly prohibited whenever any affiliation with the university is included in an online message or posting. Uncivil communication includes, but is

not limited to, threats against another individual or organization and messages or materials intended to harass, annoy, or alarm another person.

6. Eligible users can participate in certain university-maintained mailing lists. The use of these mailing lists must be restricted to official university business communications. Messages sent to university-maintained mailing lists are subject to moderation.

V SANCTIONS

Failure to comply with this policy may result in sanctions including, but not limited to, temporary or permanent revocation of access to university resources and disciplinary action up to and including separation from the university. Reports of policy violations will be presented to all necessary parties (e.g., the Office of General Counsel, the Office of Academic Affairs, the Office of Student Affairs, and/or appropriate law enforcement agencies).

VI HISTORY

March 15, 2019: Revised to include the Email Use for Faculty and Staff policy, the Email Use for Students policy, and the Internet and Network Use policy.

---

[1] LP3.2: Intellectual Property: https://www.lander.edu/about/university-policies
[2] LP7.2: Student Information Security and Privacy: https://www.lander.edu/about/university-policies
[3] LP7.3: Lander Account Password: https://www.lander.edu/about/university-policies
[4] Password Creation and Protection Guidelines: https://www.lander.edu/about/information-technology-services/policies
[5] Departmental and System Accounts: https://www.lander.edu/about/information-technology-services/policies
[6] Email Encryption Instructions: https://www.lander.edu/about/information-technology-services/information-security/protecting-data
[7] Excludes approved "send on behalf of" email features and any information redacted for privacy law compliance.