Network Service Policy
TABLE OF CONTENTS

PURPOSE .................................................................................................................................................. 3

SCOPE .................................................................................................................................................. 3

AUDIENCE ............................................................................................................................................... 3

COMPLIANCE & ENFORCEMENT .......................................................................................................... 3

POLICY STATEMENTS .......................................................................................................................... 4

1. General ............................................................................................................................................... 4

2. Administrative Standards ................................................................................................................. 4

3. Network Use ..................................................................................................................................... 5

4. Monitoring/Altering Network Traffic ............................................................................................. 5

5. Guest/Temporary Network Use ....................................................................................................... 5

6. Technical Standards ........................................................................................................................ 5

LEGAL CONFLICTS ............................................................................................................................... 6

EXCEPTIONS .......................................................................................................................................... 6

COMMENTS .......................................................................................................................................... 6

RELATED DOCUMENTS ....................................................................................................................... 6

REFERENCES .......................................................................................................................................... 6

MANDATES ........................................................................................................................................... 6

DOCUMENT CONTROL INFORMATION .............................................................................................. ERROR! BOOKMARK NOT DEFINED.

REVISION HISTORY ............................................................................................................................... 6
Purpose
The University will provide the required infrastructure for enterprise-wide local area network services, (including wireless) and connections to the internet, internet-2 and other external networks to further the mission of the University. This policy is to assure that the integrity, security, availability and necessary resources of the University network is maintained.

Scope
The scope of this policy applies to all businesses entities within Saint Leo University globally.

Audience
The Policy applies to all Saint Leo University personnel, contractors, and visitors. The term "personnel" refers to all full-time, part-time, interns, students, temporary employees attending or hired directly by Saint Leo University and on the Saint Leo University payroll. Also, the term “contractor” refers to anyone who is on another University’s payroll (contractors, outsourcers, consultants, contingent workers, temporary agency workers, etc.).

Throughout this Policy, “Saint Leo University,” “Saint Leo,” “our,” “we,” and the “University” refer to Saint Leo University. “Personnel”, “contractor”, “you” and “yours” refer to you as an employee/representative of Saint Leo University.

This Policy applies to Saint Leo University, all wholly owned subsidiaries, subsidiaries in which Saint Leo University has a controlling interest.

Compliance & Enforcement
Compliance with this Policy is mandatory and applies to all Saint Leo University personnel and contractors globally including at any of its subsidiaries or units as well as authorized representatives.

Saint Leo University reserves the right to modify the Policy at its sole discretion.

All Saint Leo University personnel and contractors are responsible for complying with this Policy. A violation of this Policy may result in disciplinary action, up to and including termination. Violators may also be subject to legal action, including civil and/or criminal prosecution. Saint Leo University also reserves the right to take any other action it believes is appropriate based on the severity of the infraction.

This Policy also represents a statement of intent, any behavior or act violating the spirit of this Policy is also subject to disciplinary action in a fashion similar to a policy violation. Saint Leo University personnel and contractors should also note that with specific authorization and approval from senior management, there are some business programs or services which are exempt from portions of this Policy. Saint Leo University Personnel and contractors must contact their manager or supervisor if they do not understand this Policy, are unable to comply with this Policy, or have questions regarding Policy.
Policy Statements

1. General

1.1. Passwords to University accounts and devices must be kept confidential.

1.2. To preserve account integrity, the owner of the account should be the only person with knowledge of the password.

1.3. No user is required to share a University account password with another individual; including but not limited to managers, co-workers, or technical staff.

1.4. Notification of password expiration will be provided to account holders 7 days in advance and every day after until password expiration if you log into the Saint Leo portal.

1.5. Saint Leo University personal will “NEVER” ask for your password.

2. Administrative Standards

2.1. Network Configuration Authority

2.1.1. University Technology Service provides all network address assignments.

2.1.2. Unauthorized University network installations or modifications will not receive IP addresses for computing devices on the unauthorized network.

2.1.3. Such devices will be physically disconnected from the University network and the device's IP and/or MAC addresses will be blocked from University network access.

2.1.4. This includes wireless networks not connected to the University's enterprise network and/or private network devices operating within University facilities or University campuses.

2.2. Connecting to University and affiliated computing resources from outside the University network

2.2.1. All connections to these resources (servers, personal computing devices, networking equipment, etc.) must, except as noted, follow these standards:

2.2.2. Be via a secure and/or encrypted connection such as a VPN, secure HTTP, secure FTP, SSH, direct dial-in or other secure and/or encrypted method

2.2.3. Be configured so that a user account and password is required and be compliant with the policies and standards described in Acceptable Use

2.2.4. If the connection is by a contractor an Acceptable Use Agreement must be completed.

2.2.5. Connection interface (a VPN or dial-in vendor service line, for example) used for occasional connections should be disabled except during the periods when the connection capability is expected to be used.
3. Network Use

3.1. Under no circumstances is a Saint Leo University personnel authorized to engage in any activity that is illegal under local, state, or federal law while using Saint Leo University resources.

3.2. Faculty, staff and administrators with University LAN accounts usually receive secure personal drive space accessed via the LAN for individual use.

4. Monitoring/Altering Network Traffic

4.1. Users are expected to use end user applications such as network drive access, email and similar programs, as they are intended to be used on the University network.

4.2. Scanning of the network, "packet sniffing", packet interception/copying/decryption and any other means of reading, altering, spoofing or otherwise monitoring and/or changing network communications is forbidden without specific approval in writing from both the Information Security Officer and Network Group.

4.3. The University reserves the right to analyze network traffic at any time deemed necessary by either manual or automated means. For example, the University may specifically monitor network traffic if instructed by legal authorities or for the purpose of assessing system integrity, performance, management or possible policy violation.

5. Guest/Temporary Network Use

5.1. Guest access to the wired network requires faculty, staff or administrator account sponsorship.

5.2. Limited guest access to the wireless network is available for visitors of the University and may be requested by faculty or staff. Guest access will expire after one week.

6. Technical Standards

6.1. General

6.1.1. All enterprise level authentication requirements external to an application must be configured to use the University's Enterprise directory services. (Note: This also allows easier configuration of single sign-on abilities.

6.1.2. Full authenticated network access requires a secure wireless connection and client software that supports current University secure wireless standards.

6.2. Wireless

6.2.1. Full authenticated network access requires a secure wireless connection and client software that supports current University secure wireless standards.

6.2.2. A Wireless adapter card that fully supports 802.1x is required to access the network.

6.3. Voice
6.3.1. The University's Voice Networking (Voice Over Internet Protocol - VOIP) provided by Information Technology is based on FCC standards and specifications.

6.3.2. This consists of the telecommunications services, dial tones, telecommunications equipment, and specialized circuitry

6.3.3. All VOIP connections are maintained and provisioned by the UTS Department

Legal Conflicts
Saint Leo University policies were drafted to meet or exceed the protections found in existing laws and regulations, and any policy believed to be in conflict with existing laws or regulations must be promptly reported to the Saint Leo University Grand Counsel.

Exceptions
Exceptional circumstances occur from time to time. In these situations, consult Saint Leo University Security Team for guidance.

Comments
N/A

Related Documents

References

Mandates

Revision History

<table>
<thead>
<tr>
<th>Revision Level</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>2013 February</td>
</tr>
<tr>
<td>1.1</td>
<td>2013 February</td>
</tr>
</tbody>
</table>