Acceptable Use Policy

TABLE OF CONTENTS

PURPOSE **4**

SCOPE **4**

AUDIENCE **4**

COMPLIANCE & ENFORCEMENT **4**

POLICY STATEMENTS **5**

1. General *5*

2. Authorized Users *5*

3. Loss and Theft *5*

4. Illegal Activities *6*

5. Internet *6*

6. Electronic Communications *6*

7. Telecommunications *7*

8. Modems *7*

9. Software *8*

10. Portable Media *8*

11. Misuse Reporting *8*

12. Social Media *8*

13. Wireless *9*

14. Circumvention of Security *9*

15. Prohibited System and Network Activities *9*

16. Privacy of Stored Personal Information *10*

17. Privacy of Personal Electronic Communications *10*

18. Electronic Monitoring Areas *10*

19. Communications *10*

LEGAL CONFLICTS **10**

EXCEPTIONS **10**

COMMENTS **11**

RELATED DOCUMENTS **11**

REFERENCES **11**

MANDATES..... **11**

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

REVISION HISTORY..... **11**

Purpose

Saint Leo University recognizes that Saint Leo University personnel roles differ and that it can be challenging to define all acceptable and unacceptable behaviors related to the use of Saint Leo University technology. The purpose of the Acceptable Use Policy is to define the requirements for the acceptable use of information resources at Saint Leo University.

Scope

The scope of this Policy applies to all businesses within Saint Leo University globally.

Audience

The Policy applies to all Saint Leo University personnel, and contractors. The term "personnel" refers to all full-time, part-time, interns, and temporary employees hired directly by Saint Leo University and on the Saint Leo University payroll. The term “contractor” refers to anyone who is on another University’s payroll (contactors, 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. All Saint Leo University personnel are responsible for using Saint Leo University technology in an appropriate business manner.

1.2. Saint Leo University recognizes that its personnel and contractors may have an occasional need to use Saint Leo University technology for non-business-related purposes. However, Saint Leo University expects all personnel to abide by Saint Leo University Employee Handbook and to understand that Saint Leo University technology is intended primarily for business use.

1.3. It is never acceptable to use Saint Leo University resources to conduct illegal activities.

1.4. Use of Saint Leo University technology must comply with local, state, and federal laws related to issues such as copyright, trademark, insider trading, harassment, and discrimination.

1.5. All non-public information should never be sent or posted on the public Internet. The information we use and share within Saint Leo University is sensitive and confidential; the inappropriate disclosure of this information could damage the reputation of Saint Leo University, the reputation of its customers, and Saint Leo University relationship with its customers.

1.6. Saint Leo University reserves the right to revoke access from any Saint Leo University personnel regarding Saint Leo University technology, at any time, if the individual fails to use the Saint Leo University technology appropriately.

1.7. Saint Leo University reserves the right to audit and monitor activities that involve Saint Leo University technology including the monitoring of e-mail and Internet activity, and to restrict access to certain websites. Such monitoring and other activities are subject to, and compliant with, local legal and regulatory requirements.

2. Authorized Users

2.1. An authorized user is any person who has been granted authority by Saint Leo University to access its computing, network, information, or telephone systems. Unauthorized use is strictly prohibited.

2.2. Prior to accessing Saint Leo University network or using Saint Leo University-owned-/-leased equipment, Saint Leo University personnel must have completed a formal acknowledgement form agreeing to Saint Leo University Policies and Standards with respect to any such asset, as well as with respect to any information or communication stored, processed, or transmitted over such asset.

2.3. Whenever a user ceases being a Saint Leo University personnel, or if a user is assigned a new position and/or responsibilities, use of technology resources for which they are not specifically authorized in their new position or circumstances shall cease.

3. Loss and Theft

3.1. Lost or stolen equipment must immediately be reported to your supervisor and/or the Saint Leo Trane Stop.

3.2. Confidential information in physical or electronic format believed to be lost or stolen must be reported to your supervisor and Saint Leo University Technology Services.

4. Illegal Activities

4.1. 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.

5. Internet

5.1. Saint Leo University reserves the right to block certain non-business related websites, category of websites from time to time as deemed necessary and without notification to the Saint Leo University user community.

5.2. Risk of Use

5.2.1. There are risks involved with using the Internet. Saint Leo University cannot guarantee that users may not encounter language, images, or references that are objectionable, inappropriate, offensive, or illegal material. Any such encounter must be ended as soon as possible.

5.2.2. Users access the Internet with Saint Leo University equipment or facilities at their own risk.

5.2.3. Saint Leo University is not responsible for material viewed, downloaded, or received by users via the Internet. Responsible attitudes and appropriate behavior are essential in using this resource. To protect personal safety and privacy, Internet users should not give out personal information to others on public information systems, without taking into consideration the risks of doing so.

5.3. Web Browsing

5.3.1. Personal usage of Saint Leo University systems to access the Internet is permitted during, before, and after business hours, as long as such use follows pertinent policies and guidelines and does not have a detrimental effect on Saint Leo University, its customers, or on the user's job performance.

6. Electronic Communications

6.1. Personal use of Saint Leo University communications systems is permitted, as long as such usage does not negatively affect Saint Leo University and does not negatively affect the user's job performance.

6.2. Information that is considered Internal Use or Confidential by Saint Leo University should not be sent via email, regardless of the recipient, without proper authorization and technical controls.

6.3. The use of encryption to protect sensitive information during transmission is required to comply with Saint Leo University Policies, Standards, and applicable laws.

6.4. The Saint Leo University email system must not be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin.

6.5. Saint Leo University personnel must not create or disseminate defamatory, discriminatory, vilifying, sexist, racist, abusive, rude, annoying, insulting, threatening, obscene, or otherwise inappropriate messages or media.

6.6. Unless required for Saint Leo University business purposes, personnel must not send any of the following types of communications:

6.6.1. Broadcast email or voice-mail, without prior permission

6.6.2. Any form of harassment via email, telephone or other communications system, whether through language, frequency, or size of messages

6.6.3. Unauthorized use, or forging, of email header information

6.6.4. Creating or forwarding "chain letters" or "Ponzi" or other "pyramid" schemes of any type.

6.6.5. Attempting to impersonate any person by using forged headers or other identifying information is prohibited.

6.6.6. Solicitation of political, religious, or other personal causes or personal business ventures.

6.7. Saint Leo University email must not be automatically forwarded to an external destination.

6.8. Saint Leo University personnel must not open e-mail attachments received from unknown senders. These attachments may contain viruses, e-mail bombs, or Trojan horse code.

6.9. Saint Leo University personnel who receive unsolicited email or web requests for sensitive information are prohibited from sharing or disclosing any such information to any party outside of Saint Leo University.

7. Telecommunications

7.1. Personal usage of Saint Leo University telecommunications systems is permitted during, before, and after business hours, as long as such use follows pertinent policies and guidelines and does not have a detrimental effect on Saint Leo University, its customers, or on the user's job performance.

7.2. Saint Leo University personnel must not forward phone calls received by them to an outside number. This will prevent the misuse of the system to make unauthorized phone calls.

7.3. Voicemail

7.3.1. Voicemail boxes must be protected by a personal identification number (PIN).

7.3.2. Default voicemail PINs must be changed as soon as issued.

7.3.3. PINs must not be similar to the phone number.

8. Modems

8.1. Use of personal broadband modems is permitted if configured to prevent inbound access to Saint Leo University internal network and used for approved business purposes only.

8.2. Mobile broadband modems must not allow split tunneling when connected to the Saint Leo University network.

8.3. Traditional modems are only permitted when no other, more secure method is available to access the data or system and approved by the Saint Leo University Technology Services.

9. Software

9.1. No unapproved software is to be installed on Saint Leo University-owned information systems without approved by the Technical Support Services Team.

9.2. Peer-to-Peer ("P2P") networking and file sharing is not allowed on the Saint Leo University network or systems under any circumstances.

10. Portable Media

10.1. Files containing Confidential or Internal Use data may not be stored on mobile media or mobile devices unless protected by Saint Leo University approved encryption solutions.

10.2. Confidential or Internal Use data must never be stored on a personal mobile device unless it's covered by a Saint Leo University approved solution.

11. Misuse Reporting

11.1. Saint Leo University personnel should report actual or suspected misuse of Saint Leo University resources to the University Technology Services.

12. Social Media

12.1. Saint Leo University may block access to certain social networking sites, or provide only limited access for business purposes, as circumstances warrant. In addition, Saint Leo University reserves the right to review and remove comments that are deemed inappropriate from Saint Leo University sponsored social media.

12.2. Accessing social networking sites during work hours and/or when using Saint Leo University equipment should be primarily for business purposes and should not interfere with your job duties.

12.3. Excessive personal use of these sites during working hours may result in performance management and related discipline, up to and including termination, as appropriate. In other situations, activity that may itself not lead to disciplinary action can nonetheless create a customer or work situation that is harmful to Saint Leo University business or reputation, or be detrimental to your business reputation or marketability.

12.4. Saint Leo University reserves the right to retain information gathered on Internet usage.

12.5. Use of social media by Saint Leo University personnel is subject to the terms and restrictions set forth in this Policy.

12.6. The use of social media is allowed provided that:

12.6.1. Prior approval of management is obtained

12.6.2. It is part of the user's job responsibilities

12.6.3. It is done in a professional and responsible manner

12.6.4. Confidential information is not disclosed

12.6.5. It does not otherwise violate policies

12.6.6. It does not impact the user's job performance

12.6.7. It is not detrimental to the reputation, goodwill, or best interests of Saint Leo University and/or any of its personnel or stakeholders

12.7. The use of social media originating from Saint Leo University systems is also subject to monitoring

12.8. This Policy also applies to similar communications that are in any online form, such as tweeting, micro-blogging, texting, etc.

12.9. Saint Leo University personnel are prohibited from revealing any sensitive information when engaged in any public communications.

12.10. Saint Leo University personnel may also not attribute personal statements, opinions, or beliefs to Saint Leo University when engaged in the use of social media. If Saint Leo University personnel are expressing his or her beliefs and/or opinions using social media, the Saint Leo University personnel may not, expressly or implicitly, represent himself or herself as a Saint Leo University personnel or representative of Saint Leo University, unless for approved business.

12.11. Saint Leo University personnel assume all risk associated with personal use of social media.

13. Wireless

13.1. Care must be taken to maintain the security of communications while using wireless devices.

14. Circumvention of Security

14.1. Unless required for Saint Leo University business purposes and approved by University Technology Services, Saint Leo University personnel may not attempt to circumvent or subvert the security provisions of any Saint Leo University system.

14.2. Saint Leo University personnel must not acquire, possess, trade, or use hardware or software tools that could be employed to evaluate or compromise information systems security, unless specifically authorized by the Information Security Group.

15. Prohibited System and Network Activities

15.1. The following activities are strictly prohibited from Saint Leo University network, computing, and communications services, without documented approval from the Information Security team.

15.1.1. Effecting security breaches or disruptions of network communication for malicious purposes.

15.1.2. Introduction of malicious programs into the network or systems (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

15.1.3. Port scanning, security scanning, and password cracking are expressly prohibited.

15.1.4. Performing any form of network monitoring that intercepts data not specifically intended for the personnel's host.

15.1.5. Interfering with, or denying service to, any user (e.g., denial of service attack).

15.1.6. Using any program, script, or command, or sending messages of any kind, with the intent to interfere with, or disable, a user's working computer session, via any means, locally or via the Internet or network.

15.2. Users must not access, modify, or delete other users' files or system settings without express permission.

15.3. Tampering of any kind is strictly forbidden.

15.4. Deliberate attempts to tamper with or degrade the performance of a Saint Leo University computer system, telephone system, or network, or to deprive authorized users of access to or use of such resources are prohibited.

16. Privacy of Stored Personal Information

16.1. Saint Leo University personnel do not have any expectation of privacy in anything they store, send, or receive on Saint Leo University information systems.

16.2. Saint Leo University may monitor or review information system usage and files, including content, without prior notice.

16.3. Saint Leo University reserves the right to actively monitor, restrict, use, and dispose of email messages, other electronic communications, and/or personal stored files.

16.4. Saint Leo University personnel should exercise caution when storing and processing personal and sensitive information not directly related to Saint Leo University business.

17. Privacy of Personal Electronic Communications

17.1. Saint Leo University personnel do not have an expectation of privacy in anything they store, send, or receive on Saint Leo University information systems. All messages sent over Saint Leo University computer and communications systems are subject to monitoring and review in the interest of protecting the security of Saint Leo University information.

17.2. To properly maintain and manage the security of information resources, Saint Leo University reserves the right to examine all information stored in or transmitted by these information systems.

18. Electronic Monitoring Areas

18.1. Individuals are subject to electronic monitoring while on Saint Leo University premises and in secure areas. This monitoring is used to measure policy compliance as well as to protect Saint Leo University, its personnel, and others. In areas where there is a reasonable expectation of privacy, such as bathrooms, dressing rooms, and locker rooms, no visual or audio monitoring will be performed without the express consent of the leadership team and legal consultation.

19. Communications

19.1. Questions regarding this Policy should be directed to the Saint Leo University Security Team.

19.2. This policy shall be made available to all Saint Leo University personnel and contractors as applicable to their role and function within Saint Leo University.

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

- Payment Card Industry Data Security Standard

Revision History

Revision Level	Date
1.0	2012 January
1.1	2013 January