ACCEPTABLE USE POLICY

Policy Statement

Information Security's intention for publishing an Acceptable Use Policy is not to impose restrictions contrary to University of Southern Mississippi established culture of openness, trust, and integrity. Information Security is committed to protecting Southern Miss faculty, staff, students, and partners from illegal or damaging actions by individuals, either knowingly or unknowingly. Internet/Intranet/Extranet-related systems — including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing — are the property of Southern Miss. Effective security is a team effort requiring the participation and support of every Southern Miss employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

Reason for Policy/Purpose

This policy is required for the effective communication of university policy regarding the acceptable use of computer equipment at Southern Miss. These rules are in place to protect faculty, staff, students, and the University of Southern Mississippi. Inappropriate use exposes Southern Miss to risks including virus attacks, compromise of network systems and services, and legal issues.

Who Needs to Know This Policy

This policy applies to faculty, staff, students, contractors, consultants, temporaries, and other workers at Southern Miss, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Southern Miss.

Website Address for this Policy

www.usm.edu/institutional-policies/policy-ACAF-IT-010
Definitions

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>spam</td>
<td>Unauthorized and/or unsolicited electronic messages</td>
</tr>
<tr>
<td>junk</td>
<td>Non-University business related email</td>
</tr>
<tr>
<td>FERPA</td>
<td>Family Educational Rights and Privacy Act</td>
</tr>
<tr>
<td>personally identifiable information</td>
<td>Information that can be directly tied to an individual</td>
</tr>
<tr>
<td>GLBA</td>
<td>Gramm-Leach-Bliley Act (Protection of banking information)</td>
</tr>
<tr>
<td>SOX</td>
<td>Sarbanes-Oxley Act (integrity of financial reporting)</td>
</tr>
</tbody>
</table>

Policy/Procedures

1.0 GENERAL USE AND OWNERSHIP

1.1 While Southern Miss's network administration desires to provide a reasonable level of integrity, users should be aware that the data/email they create/receive on university systems remain the property of Southern Miss and that no privacy can be expected while using these systems. Because of the need to protect the university's network, management cannot guarantee the confidentiality of information stored on any network device belonging to Southern Miss.

1.2 Faculty and staff are responsible for exercising good judgment regarding the reasonableness of personal use. Information Security recommends that any information which users consider sensitive or vulnerable be password protected.

1.3 For security and network maintenance purposes, authorized individuals within the Southern Miss iTech group may at any time analyze network utilization, traffic patterns and volumes related to Southern Miss systems/equipment and network.

1.4 Southern Miss' iTech Information Security Group reserves the right to audit networks and systems periodically to ensure compliance with this policy.

2.0 SECURED AND PROPRIETARY INFORMATION (PII, FERPA, GLBA, SOX, federal/state regulated.)

2.1 Faculty and staff should take all necessary steps to prevent unauthorized access to this information.
2.2 Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed quarterly. User level passwords should be changed every 90 days.

2.3 All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off (control-alt-delete for Win2K/XP users) when the system will be unattended.

2.4 Because information contained on portable computers is especially vulnerable, special care should be exercised to protect this data.

2.5 All Postings by employees from Southern Miss email addresses to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Southern Miss, unless posting is in the course of business duties.

2.6 All hosts used by the employee that are connected to the Southern Miss Internet/Intranet/Extranet, whether owned by the employee or by Southern Miss, shall be continuously execute approved virus-scanning software (http://www.usm.edu/infosec/antivirus.php) with a current virus database.

2.7 Employees must use extreme caution when opening email attachments received from unknown senders, which may contain viruses, email bombs, or Trojan horse code.

3.0 UNACCEPTABLE USE

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services). Under no circumstances are faculty, staff, and students of Southern Miss authorized to engage in any activity that is illegal under local, state, federal, or international law while utilizing Southern Miss-owned resources. The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

3.1 System and Network Activities – The following activities are strictly prohibited, without exception:

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Southern Miss.

- Collection, storage or distribution of pornography or material considered to be obscene in violation of this policy.

- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, copyrighted movies and the installation of any copyrighted software.
for which Southern Miss or the end user does not have an active license is strictly prohibited.

- Illegally exporting software, technical information, encryption software or technology in violation of international or regional export control laws.

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

- Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

- Using a Southern Miss computing asset to actively engage in procuring or transmitting material in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

- Making fraudulent offers of products, items, or services originating from any Southern Miss account.

- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, the following: Accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information.

- Port scanning or security scanning is expressly prohibited unless prior notification is given to Information Security and /or these processes are within the scope of regular duties.

- Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duties.

- Circumventing user authentication or security of any host, network, or account.

- Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

- Using any program/script/command, or sending messages of any kind, with the intent to interfere with or disable a user's terminal session, by any means, locally or via the Internet/Intranet/Extranet.

- Providing information about (or lists of) Southern Miss faculty, staff, or student protected/non-directory information to parties outside the university without the express written permission of the university administration.
• Any person found in violation of this policy will be notified immediately to cease and desist. The user will be given a time frame to comply or be disconnected from the Southern Miss network until they can prove the issue has been addressed.

3.2 Email and Communications Activities – The following activities are strictly prohibited, without exception:

• Sending email messages, including "junk mail/SPAM" or other advertising material, to individuals who did not specifically request such material (email spam).

• Any form of harassment via email, telephone, or paging; whether through language, frequency, or size of messages.

• Unauthorized use, or forging, of email header information in an attempt by an individual to misrepresent or hide his or her identity.

• Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

• Creating or forwarding chain letters or other pyramid schemes of any type.

• Use of unsolicited email originating from within Southern Miss's networks to advertise, any service not hosted by Southern Miss.

• Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

4.0 ENFORCEMENT

4.1 Faculty, Staff, and Students: Any faculty, staff, or student found to have violated this policy may be subject to disciplinary action, up to and including suspension, expulsion and/or termination of employment in accordance with procedures defined by USM administrative policies stated in the handbook governing that individual.

4.2 External Entities: Any external entity, contractor, consultant, or temporary worker found to have violated this policy may be held in breach of contract, and as such, may be subject to grievances or penalties allowed by such contract.

Review

The Chief Information Officer is responsible for the review of this policy every four years (or whenever circumstances require immediate review).

Forms/Instructions
Appendices

N/A

Related Information

N/A

History

1. 10/24/06 : Posted to website.
2. 11/15/06 : Added link to Peer-to-Peer Policy
3. 11/16/06 : Added link to Password Policy
4. 04/23/08 : Modified policies menu
5. 10/14/08 : Section UNACCEPTABLE USE modified
6. 11/01/11: Formatted for Institutional Policies website
6. 02/19/13: Formatted in new template. “Policy” section renumbered.

Amendments: Month, Day, Year – summary of changes
Authorization

ACCEPTABLE USE POLICY
ACAF-IT-000-010

As the Responsible Officer, I have reviewed this policy and believe it represents the current policy.

[Signature]
Responsible Officer

[Date]
04/16/13