

**The Texas A&M University System**  
**Facilities Planning & Construction Department**  
**IMPACT System Access**  
**(User/Consultant Details)**

*PLEASE FILL IN With PC the information below (2<sup>nd</sup> thru 5<sup>th</sup> pages do not have to be resubmitted when adding new projects to your previously submitted documents).*

**First Name:**

**Last Name:**

**Company Web Site:**

**Company Name:**

**Company Address:**

**Title:**

**Fax:**

**Work Phone:**

**Home Phone (Optional):**

**Mobile Phone:**

**Email Address:**

If you are a consultant or subcontractor, please name the **other** firm \_\_\_\_\_

TAMUS Project No.	Project Name(s)	Role(s)

Each person needing access to the TAMUS IMPACT Project Management system must fill in, sign and forward as an email attachment these PAPER forms (click on each page if needed to see fillable blanks). If needed, a FREE Adobe Reader at <http://get.adobe.com/reader/> can be downloaded and used for filling these forms. Please email as an attachment to Ben Polasek ([ben-polasek@tamus.edu](mailto:ben-polasek@tamus.edu)) and cc: James Davidson ([jm-davidson@tamus.edu](mailto:jm-davidson@tamus.edu)).

This file of 5 pages includes a User/Consultant Details page and 4 pages of SOR form ("Dept. Head Signature" will be added by TAMUS FP&C). If available, a Business Card should be attached below prior to scanning. Once setup in IMPACT, you will receive an email providing details for logging into the TAMUS IMPACT system.

**[Tape your Business Card HERE prior to Scanning]**



**Business Computing Services**

A&M System Building, 301 Tarrow • College Station, Texas 77840-7896  
Phone 979.458.6300 • Fax 979.458.6299 • Campus Mailstop 1124 • Web tamus.edu

**Software/Hardware/Network Statement of Responsibility**

*With few exceptions, you have the right to request, receive, review and correct information about yourself collected using this form.*

I understand that I will be violating A&M System Policy, A&M System Offices (SO) rules, and state and federal law if I gain, or help others gain unauthorized access to the SO computer network. I acknowledge that neither I nor anyone else possesses the authority to allow anyone to use my ID or password.

I also understand that if I violate state and federal laws by gaining or helping others gain unauthorized access to the SO network, I will be subject to criminal prosecution to the full extent of the law (Chapter 33, Section 1, Title 7 of the Texas Penal Code).

By logging on to any of the SO network computers, I acknowledge my responsibility for strictly adhering to The Texas A&M University System Policy concerning network access, the SO Information Resource Acceptable Use Standards (attached) and state and federal law. I am also aware that penalties exist for unauthorized access, unauthorized use or unauthorized distribution of information from SO computers.

I agree further not to attempt to circumvent the computer security system by using or attempting to use any transactions, software or resources I am not authorized to use.

***User Information***

_____	_____	_____
Name (First Middle Last)	Nickname (if any)	Official Position or Title
_____	_____	_____
UIN		Department
_____	_____	_____
Email Address		Agency/Institution
_____	_____	_____
Office Phone Number		
_____	_____	_____
User Signature		Date
_____	_____	_____

For Official Use Only: <a href="http://www.tamus.edu/offices/computing/support/forms/Statement-of-Responsibility-for-Non-SO-Employees.pdf">http://www.tamus.edu/offices/computing/support/forms/Statement-of-Responsibility-for-Non-SO-Employees.pdf</a> Rev. Jun. 01, 2009 \\sago-file\work\mcns\administration\so policy\Statement-of-Responsibility-for-Non-SO-Employees.docx				
_____	_____	_____	_____	_____
Username	Date Added	Initials	Date Deleted	Initials

**The Texas A&M University System Offices**  
**INFORMATION RESOURCES ACCEPTABLE USE STANDARDS**

Rev. June 01, 2009

The A&M System Offices (SO) rely on networked computers and the data contained within those systems to achieve its mission. These Acceptable Use Standards are to protect these resources in accordance with A&M System Policy, SO rules, and federal and state law. These Standards do not supersede any state or federal laws or any other agency policies regarding confidentiality, information dissemination, or standards of conduct. All individuals granted access to A&M System Offices Information Resources must follow the Acceptable Use Standards below:

<b>General</b>	<ul style="list-style-type: none"> <li>• A&amp;M System Offices (SO) Information Resources are provided for the express purpose of conducting the business and mission of The Texas A&amp;M University System Offices; however, brief and occasional personal use (i.e., surfing, browsing, email, instant messaging (IM)) is allowed if the following Acceptable Use Standards are followed. Personal use should not impede the conduct of state business; only incidental amounts of employee time—time periods comparable to reasonable coffee breaks during the day—should be used to attend to personal matters.</li> <li>• All users of state networks and systems should be aware that when sending an e-mail message or other electronic transmission of a personal nature, there is the danger of the employee's words being interpreted as official agency policy or opinion. Therefore, when an employee sends a personal e-mail, especially if the content of the e-mail could be interpreted as an official agency statement, the employee should use the following disclaimer at the end of the message: "This message contains the thoughts and opinions of [employee name] and does not represent official A&amp;M System Office policy."</li> <li>• SO Information Resources must not be used to: engage in acts against the mission and purposes of the A&amp;M System or any A&amp;M System member, intimidate or harass, degrade performance, deprive access to a SO resource, obtain extra resources beyond those allocated, or to circumvent computer security measures.</li> <li>• Intentionally accessing, viewing, creating, storing, downloading, uploading, transmitting, printing, copying, posting, or sharing any racist, sexist, threatening, sexually explicit, obscene or otherwise objectionable material (i.e., visual, textual, or auditory entity) is strictly prohibited.</li> <li>• Information Resources must not be used to conduct a personal business or for any personal monetary interests or gain or used for the exclusive benefit of individuals or organizations that are not part of the A&amp;M System. Any exceptions must be in support of the SO missions and require the prior written approval of an Executive Officer of the SO.</li> <li>• Users must not copy, reproduce or download any illegal and/or unauthorized copyrighted content or licensed software except as expressly permitted by the software license, use unauthorized copies on SO-owned computers or use software known to cause problems on SO-owned computers.</li> </ul>
<b>Ownership and Privacy</b>	<ul style="list-style-type: none"> <li>• Internet, instant messaging, and peer-to-peer usage (P2P), electronic files or e-mail created, sent, received, transmitted or stored on Information Resources owned, leased, administered, or otherwise under the custody and control of SO are the property of SO, are not private, and are subject to the Texas Public Information Act, and may be accessed at any time by SO IT employees or other appropriate personnel without knowledge of the Information Resources user or owner in accordance with the provisions and safeguards provided in the Texas Administrative Code 202, Information Resource Standards.</li> <li>• Information concerning SO business is subject to the Texas Public Information Act regardless of where this information is stored. These storage locations include external email accounts (Hotmail, Gmail, etc.), a home computer, BlackBerry or other handheld mobile device or personal storage device such as a thumb drive.</li> </ul>
<b>Data Protection</b>	<ul style="list-style-type: none"> <li>• Data will be accessed on a need to know basis. Users of SO information systems must not attempt to access data or programs contained on systems for which they do not have authorization or consent.</li> <li>• All critical SO data (electronic files) will be saved on network servers to ensure backup of the data. All data should be backed up for disaster recovery reasons.</li> <li>• All records (electronic or paper) will be maintained in accordance with the SO Records Retention Policy.</li> </ul>
<b>Virus and Software Protection</b>	<ul style="list-style-type: none"> <li>• All computers connecting to the SO network, including dial-up or VPN, must run current and authorized virus prevention software and be updated with the latest software security patches. Virus protection software must not be disabled or bypassed except as required by the temporary installation of software or for other special circumstance. Computers found to be infected with a virus or other malicious code will be disconnected from the SO network until deemed safe by Microcomputers and Network Support (MCNS).</li> </ul>
<b>Instant Messaging</b>	<ul style="list-style-type: none"> <li>• Employees will not download/install any Instant Messaging (IM) software without specific authorization.</li> <li>• If authorized for usage on state systems, IM may be used for any routine official business communication that is not normally filed for recordkeeping, such as a communication that is temporarily needed only for an employee to complete an action.</li> <li>• IM may not be used to conduct state business that would require the content to be saved as a state record.</li> <li>• IM may not be used to document a statutory obligation or agency decision, and IM should not be used when the resulting record would normally be retained for recordkeeping purposes.</li> </ul>
<b>Peer-to-Peer</b>	<ul style="list-style-type: none"> <li>• If authorized for usage on state systems, Peer-to-Peer (P2P) may be used for any routine official business communication that is not normally filed for recordkeeping, such as a communication that is temporarily needed only for an employee to complete an action.</li> <li>• Users of state computers or networks shall not download/install any P2P software onto state computers, networks, or mobile computing device (PDA) without specific authorization.</li> </ul>

<p><b>Electronic Mail</b></p>	<ul style="list-style-type: none"> <li>• The following electronic mail (email) activities are prohibited: <ul style="list-style-type: none"> <li>- Using email for purposes of political lobbying or campaigning except as permitted by the A&amp;M System Policy and Regulations.</li> <li>- Posing as anyone other than oneself when sending email, except when authorized to do so by the owner of the email account.</li> <li>- Reading another user's email unless authorized to do so by the owner of the email account, or as authorized by policy for investigation, or as necessary to maintain services.</li> <li>- Use of email software that poses a significant security risk to other users on the SO network.</li> <li>- Sending or forwarding "chain" letters.</li> <li>- Sending unsolicited messages to large groups except as required to conduct SO business.</li> <li>- Sending excessively large messages or attachments unless in performance of official SO business.</li> <li>- Sending or forwarding email that is likely to contain computer viruses.</li> <li>- Violating copyright laws by inappropriately distributing protected works.</li> <li>- Subscribing to mailing lists or mail services strictly for personal use.</li> </ul> </li> <li>• Individuals must not send, forward or receive confidential or sensitive agency information through non-agency e-mail accounts (e.g., Yahoo!, AOL, or any other e-mail service belonging to an Internet service provider).</li> <li>• Delivery of electronic mail is not guaranteed.</li> </ul>
<p><b>Confidential or Protected Information</b></p>	<ul style="list-style-type: none"> <li>• Confidential or protected information must not be transmitted unless approved transmission protocols and security techniques are utilized.</li> <li>• Confidential or protected information must not be sent, forwarded or transmitted through email.</li> <li>• All confidential or protected information stored on a laptop, PDA or other portable storage media must be encrypted.</li> </ul>
<p><b>Incidental Use of Information Resources</b></p>	<ul style="list-style-type: none"> <li>• Incidental personal use of electronic mail, IM, P2P, and internet access is permitted by SO Standards, but is restricted to employees (it does not extend to family members or other acquaintances). It must not interfere with normal performance of an employee's duties, must not result in direct costs to SO, and must not expose the SO to unnecessary risks.</li> <li>• Storage of any non-work related email messages; voice messages, files and documents within the SO email system must be nominal (less than 5% of a User's allocated mailbox space).</li> <li>• Non-work related information may not be stored on network file servers.</li> <li>• All messages, files and documents stored on SO computing resources, including personal messages, files and documents, are owned by the SO and are subject to SO review.</li> <li>• Any files, messages or documents residing on SO computers may be subject to public information requests. Therefore, a SO email account should not be used for personal email correspondence that is confidential.</li> </ul>
<p><b>Internet Use</b></p>	<ul style="list-style-type: none"> <li>• Software for browsing the Internet is provided to authorized users for business and research purposes only.</li> <li>• Due to network maintenance, performance monitoring and to ensure compliance with applicable laws and policies, all user activity may be subject to logging and review.</li> <li>• Email or postings by users of SO network resources to news groups, "chat rooms" or "listservs" must not give the impression that they are representing, giving opinions, or making statements on behalf of SO, unless authorized.</li> <li>• Personal commercial advertising must not be posted on SO web sites.</li> <li>• Non-business related purchases made over the internet are prohibited. Business related purchases are subject to A&amp;M System Disbursement of Funds Guidelines.</li> <li>• All authorized users of state networks or systems must use the Internet facilities in ways that do not disable, impair, or overload performance of any other computer system or network, or circumvent any system intended to protect the privacy or security of another user.</li> <li>• Downloading entertainment software, games or any other non-business related software or files, such as music or movies is prohibited.</li> <li>• Streaming media, such as internet radio or videos, is prohibited unless there is a business need.</li> <li>• No files or documents may be sent or received that may cause legal liability for or embarrassment to the SO.</li> </ul>
<p><b>Passwords</b></p>	<ul style="list-style-type: none"> <li>• Every SO computer/network account, password, any personal identification number (PIN), digital certificate, security token (i.e. Smartcard), or any other similar information or device used for identification and authorization purposes must not be shared. Each user of SO resources is responsible for all activities conducted using his or her account(s).</li> <li>• Digital certificate passwords used for digital signatures must never be divulged to anyone.</li> <li>• Users must not circumvent password entry through use of auto logon, application "remember password" features, embedded scripts or hard-coded passwords in client software. Exceptions may be made for specific applications (like automated backup) with the approval of the SO Information Security Officer (ISO). Any exception situation must include a procedure to change the passwords and must adhere to security policies for password construction. (For more information, see the SO's Password Guidelines.)</li> <li>• Unattended computing devices must be secured from unauthorized access. Physical security options include barriers such as locked doors or security cables. Logical security options include screen saver passwords and automatic session time-outs.</li> </ul>

<b>Portable and Remote Computing</b>	<ul style="list-style-type: none"> <li>• All computers, portable-computing devices and portable storage devices using SO information resources, especially those which process, store, or transmit confidential information, must be password protected using the “strong” password standard adopted by SO. At a minimum, such passwords are to be changed at least annually, or immediately if there is suspicion that the password has been compromised.</li> <li>• Employees accessing the SO network from a remote computer must conform to SO Information Security Standards that apply to access from within the local area network. Remote computers are subject to the same rules and security related requirements that apply to SO-owned computers.</li> <li>• Unattended portable computing devices must be physically secure.</li> <li>• If it is determined that required security related software is not installed on a remote computer or that a remote computer has a virus, is party to a cyber attack or in some way endangers the security of the SO, the account and/or network connection will be disabled. Access will be re-established once the computer is determined to be safe by MCNS.</li> <li>• Users must not divulge SO dialup or modem phone numbers to anyone unless they have a business need.</li> <li>• All remote access (e.g., dial in services, cable/DSL modem, etc.) to confidential information from a portable computing device shall utilize encryption techniques, such as Virtual Private Network (VPN), secure File Transfer Protocol (FTP), or Secure Sockets Layers (SSL).</li> <li>• If critical SO data is stored on portable computing devices it must be backed up to a network server for recovery in the event of a disaster or loss of information.</li> <li>• Any confidential information stored on portable computing or storage device shall be encrypted with an appropriate encryption technique. Special care (such as file encryptions, file level password protection, etc.) should be taken to protect information stored on portable computing or storage devices, and in protecting such devices from theft.</li> <li>• Confidential information shall not be transmitted via wireless connection to, or from, a portable computing device unless encryption methods that appropriately secure wireless transmissions, such as Virtual Private Network (VPN), Wi-Fi Protected Access (WPA) or other secure encryption protocols are utilized.</li> <li>• Unattended portable computing or storage devices, containing confidential information, shall be kept physically secure using means appropriately commensurate with the associated risk.</li> <li>• Where appropriate, keep portable computing devices patched/updated, and install anti-virus software and a personal firewall.</li> </ul>
--------------------------------------	---

<b>Security</b>	<ul style="list-style-type: none"> <li>• Security programs or utilities that reveal or exploit weaknesses in the security of a system or that reveal data by circumventing established authorization procedures and systems should not be downloaded and/or used, except as authorized by MCNS. For example, password cracking programs, packet sniffers, or port scanners on SO information resources shall not be used.</li> <li>• Where technically feasible, all PC’s, laptops, personal digital appliance (PDA) devices and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less to prevent unauthorized access to the device.</li> <li>• Users must report any weaknesses in SO computer security, any incidents of possible misuse or violation of this agreement to the proper authorities by contacting the immediate supervisor, department head, or the SO ISO.</li> </ul>
-----------------	---

**User Acknowledgment**

If you have questions about the above standards and procedures, address them to the SO Microcomputer and Network Support (MCNS) group before signing the following agreement.

I acknowledge that I have received and read the A&M System Offices Information Resources Acceptable Use Standards. I understand that I must comply with these Standards when accessing and using Information Resources and my failure to comply with these Standards may result in appropriate disciplinary action and/or action by law enforcement authorities.

Signature: \_\_\_\_\_ Date: \_\_\_\_\_

Print Name: \_\_\_\_\_