Stockbridge-Munsee Community	
Policy: Computer Use Policy	**Tribal Council Approved:** 10/6/09
Department: MIS	**Revision Approved:** 12/1/09
Pages: 6	

The Stockbridge-Munsee Community ("SMC") provides computer hardware, software, peripherals, network and internet access ("computers") to elected officials and employees to facilitate the business functions of the organization. Volunteers and consultants/contractors may be provided limited access in some circumstances. Elected officials, employees, volunteers and consultants/contractors ("Users") are responsible for the appropriate use of computers. All users of SMC computers are subject to the provisions of this policy.

Tribal Property and Privacy – In addition to computer hardware and software, ***all information stored on SMC computers constitutes business records and is the property of SMC. Because all information is the property of SMC, users should not expect that it is private.*** Users should also be aware that deleted files may be retrieved. SMC reserves the right to retrieve, monitor and review any use of and information on its computers and may disclose such information for any purpose without notice to the user and without seeking permission from the user.

Persons requiring access to another user's computer for audit purposes must provide a written request to the MIS Department. The reason for the request must be related to productivity, performance, security or employer liability as determined by the SMC Human Resources Department and Legal Office. In addition, appropriate access will be provided to facilitate tribal operations, including for audit purposes, as part of authorized investigations, and to ensure compliance with contractual requirements and applicable laws and policies.

Confidential or Proprietary Information – Copying, downloading, sending or uploading of confidential or proprietary information to unauthorized individuals is prohibited. For purposes of this policy, proprietary information includes licensed materials, copyrighted materials, trade secrets, financial information or similar materials. Users shall not attempt to modify the source code of software licensed by the SMC.

Confidentiality – All user information stored on SMC computers, other than information specifically made publicly available over the internet, is considered confidential. Accessing or attempting to access confidential information unrelated to job responsibilities is strictly prohibited. Confidential information should only be used for its intended purpose.

Authorized persons may access and review information at any time when requested in writing as specified in the ***Tribal Property and Privacy*** section above. For computers that may contain confidential or protected information including, but not limited to, health, employee, financial, child protection or legal information, this review will be done by a person authorized to have access to such information.

All persons participating in the review process shall maintain the confidentiality of all information that they may become aware of as part of fulfilling their duties under this policy. Information that remains on a user's computer after the user has left SMC may be reviewed by the user's supervisor or other authorized person before the information is purged.

Security –Users are responsible for maintaining the security of their own computer account user name and password. Sharing account user names and passwords with others is discouraged. In the event that a user shares their account user name and password with another person or allows an unauthorized person to use their SMC computer, the user is responsible for the actions of that person. Passwords may be disclosed to the MIS Department for purposes of troubleshooting technical issues, but should be changed by the user immediately after resolution. Users are encouraged to change account passwords frequently. No user is to keep an unsecured written record of his or her password, either on paper or in an electronic file. Whenever possible, the MIS Department will implement network policies to enforce password protection and other security measures based on industry standards.

It is important that users take extra care with information stored on SMC computers. The following are inappropriate under any circumstances when dealing with confidential information:

- Leaving your computer containing confidential information unattended and logged in.
- Leaving computer disks or USB drives with confidential information unattended and in easy to access places.
- Sending confidential information over the Internet or other unsecured communication lines unless such use is required to complete normal job responsibilities.
- Giving out passwords or any information about SMC proprietary information or computer systems to unauthorized persons or outside entities.

If you observe a document at a shared printer, or any other location, do not read it without permission. If you accidentally identify a new way to access information that you are not authorized to access, report it to your supervisor and the MIS Department.

Obtaining or trying to obtain other users' passwords or using programs that compromise security in any way are prohibited. Users are responsible for reporting inappropriate use of SMC computers and breaches of computer security and assisting in resolving such matters. If you observe an unauthorized person accessing an SMC computer, report it to your supervisor.

Using hacker programs and trying to access computer systems using hacker techniques is prohibited. Trying to hack into third party computer systems using SMC computers is prohibited and will be reported to the local authorities.

Users are required to log off or shut down their computer at the end of the day and utilize the locking function within the operating system when not in use for an extended period of time or while left unattended. This will help to prevent computer security breaches. Users must take all reasonable precautions to prevent unauthorized access to SMC computers.

Backing Up Computer Information – The MIS Department will implement procedures and educate users on the proper use and storage of computers and information. Users are responsible for ensuring these procedures are followed to prevent loss or damage of computer information and equipment. Users working at networked facilities will be provided a file storage area on the central file server for automatic daily backups. Users at remote facilities must perform manual backups of computer hard drives in order to backup critical SMC information. Backups may be used to restore information in case of computer hardware failure and data loss.

File Management – In order to keep SMC computer systems running efficiently and to mitigate liability, users should delete unnecessary files stored on SMC computers. Files should not be saved for an extended period unless required as part of SMC's record retention policy.

Business Use – Use of SMC computers must be primarily job-related and for business purposes. Limited, occasional or incidental use of SMC computers for personal use is acceptable if done in a professional manner that does not interfere with business functions or consume computer or network resources. Prohibited activities include, but are not limited to, computer games, personal software and hardware or running a personal business. Using SMC computers to store or transmit inappropriate jokes, junk mail and chain letters is prohibited. Personal files stored on SMC computers will be treated the same as business files and therefore considered to be tribal property with no employee privacy.

Business Form – Users are expected to conduct themselves in a professional manner when using SMC computers. **Users should keep in mind that electronic files are subject to discovery and may subsequently be used in litigation involving SMC or the user.** Therefore, it is expected that use of and files created and stored on SMC computers will reflect favorably on SMC and the user.

Solicitation – Users may not utilize SMC computers to solicit for commercial ventures or charitable, religious or political organizations or other causes without prior authorization from their supervisor. Solicitation by users acting in the capacity of their job responsibilities is acceptable.

Anti-Harassment and Anti-Discrimination Policies Applicable – SMC employment policies, including those prohibiting sexual or other harassment and discriminatory conduct, are applicable to SMC computer systems. Files containing foul, inappropriate, or offensive language, those containing racial or ethnic slurs, sexual innuendo, pornography or defamation are prohibited.

Unacceptable Use – Unacceptable use of SMC computers includes, but is not limited to, the following:

- Using or allowing another to use for fraudulent or criminal purposes.
- Using for personal purposes for activities that cause significant congestion or disruption of the SMC computer network or jeopardize the security of SMC computers.
- Using to interfere with the ability of others to conduct business.
- Using to buy and sell personal goods and services or for personal gain.
- Creating or distributing material which others may find offensive or disruptive.
- Using or allowing another to use in any way that violates the employee manual, tribal policies, tribal ordinances, applicable state or federal laws.

Internet Use – Internet resources will be provided to users in order to fulfill job responsibilities. Limited, occasional or incidental use of internet resources for personal use is acceptable if done in a professional manner that does not interfere with business functions or consume computer or network resources. Users are required to use common sense and exercise good judgment while using internet resources. The MIS Department will ensure that appropriate routers and firewalls are in place to technically support access requirements. Connectivity to the internet through separate analog lines and modems is prohibited.

Files downloaded from the internet may contain viruses or malware. Downloading and installing files from the internet by users other than updates to authorized software is strictly prohibited. Users must make a request to the MIS Department to install software and only software needed to perform job functions will be installed on SMC computers.

Use of social networking sites to conduct business on behalf of SMC or to disclose confidential information is prohibited unless such use is required to complete normal job responsibilities. Users may not post SMC e-mail addresses or information that will harass or negatively impact SMC employees or the SMC on social networking sites.

Filtering and reporting systems are in place to track usage of internet resources. The MIS Department will monitor usage and block sites and site categories that propose a threat, report high usage or that are causing significant congestion to the SMC computer network and do not serve a valid business purpose. Authorized persons will be provided with internet usage reports when requested in writing as specified in the ***Tribal Property and Privacy*** section above.

Unauthorized Changes to SMC Computers – Installing software and making changes to computer hardware, software and system configurations are prohibited. Only MIS personnel are authorized to perform these functions. Users will not violate any licensing agreements. All software installed on SMC computers must be used in compliance with all applicable licenses, notices, contracts and agreements. The MIS Department is responsible for monitoring and uninstalling any unapproved hardware or software from SMC computers and unauthorized changes will be reported to the user's supervisor. Users will not have administrator rights to SMC computers unless it is required for their job functions.

Use of Personal Hardware and Software – No SMC information shall be stored on personal computers. Other than proper remote e-mail access, all business conducted for the operation of SMC must be performed on a computer owned by SMC. Use of personal computer hardware, software and peripherals in the workplace is prohibited. Software purchased by SMC will not be installed on personal computers.

Portable Devices and Media – All portable devices including laptops, LCD projectors, smart phones and storage media will be monitored and tracked to minimize the risk that equipment or confidential information is lost, damaged or disclosed. Portable devices may not be taken off SMC premises without proper authorization. Family members or friends are not permitted to use SMC computers or portable devices. The use of media storage such as USB drives is permitted for work related functions but removal of confidential information from SMC premises without authorization is prohibited.

Virus/Malware Protection – The MIS Department will install authorized anti-virus and anti-malware protection on all SMC computers. This software must be active, scheduled to perform regular virus checks and have its virus definition files kept up-to-date. Users should report potentially infected computers to the MIS Department immediately. Users should not attempt to remove viruses or malware themselves.

Software downloaded from the internet and e-mail attachments have been identified as a means for spreading computer viruses that cause the loss of information or even a complete shutdown of the system. Downloading and installing software from the internet is strictly prohibited. Attachments to e-mails should not be opened unless the e-mail originates from a known source. Viruses can also come from other sources such as portable media (USB drives, computer disks, etc). Scan all portable media for viruses before using in SMC computers. Any activities related to the creation and/or distribution of malicious programs is prohibited.

Purchasing Computer Equipment and Software – All computer hardware, software and peripheral purchases must be coordinated with and approved by the MIS Department to ensure pre-established quality requirements, competitive pricing and compatibility with other SMC computer equipment and software. The MIS Department will maintain a record of all computer purchases. See the approved purchasing policies and computer replacement policies for further information.

Suspension or Termination of Employment – Users are prohibited from accessing SMC computers when their employment by the SMC has been suspended or terminated. Deleting, altering, or sharing confidential, proprietary, or any other information upon termination without management authorization is prohibited. All computers must be returned to SMC along with any other appropriate information necessary for SMC to continue using the computer and information stored on it, uninterrupted. Accessing SMC computers or taking files, data, programs or computer equipment upon termination is prohibited and could be prosecuted to the fullest extent of the law.

Failure to Comply – Supervisors are responsible for ensuring that users are trained on the proper use of SMC computers and that they have been provided with and understand this policy. Violations of this policy will be reported to the user’s supervisor. Failure to comply with this policy may result in the revocation of the user’s computer and further disciplinary action as documented in the employee manual.

Your signature indicates that you have read and understand the Computer Use Policy approved by Tribal Council on 12/1/09.

User’s Printed Name

User’s Signature **Date**

Supervisor’s Signature **Date**