

ENTERPRISE IT SERVICES
ACCEPTABLE USE AGREEMENT

INTRODUCTION

This acceptable use agreement governs the use of computers, networks, and other information technology (IT) resources for Enterprise IT Services (EITS). This statement applies to all EITS employees and contractors, and all other persons who may legally or illegally use or attempt to use computer resources owned or managed by the department, and/or is connected by any means to the state SilverNet Network. As a user of these resources, you are responsible for reading and understanding this agreement.

IT resources within EITS are to be used in a manner that supports the mission of the department. IT resources refer to all equipment, hardware, software or network (including wireless networks) and includes computers, e-mail applications and state internet and intranet access (including when accessed through personally owned computers). The systems range from multi-user systems to single-user terminals and personal computers, whether free-standing or connected to networks.

ACCEPTABLE/UNACCEPTABLE USE

1. All users must safeguard the confidentiality, integrity, and availability of EITS systems, including password login, access codes, network access information and log-on IDs from improper access, alteration, destruction, or disclosure. Users shall only access or use EITS systems when authorized. Users must abide by EITS policies and other State policies regarding the protection of data and information stored on these systems.
2. When personally owned systems are used for EITS business, EITS retains the right to any EITS records or materials developed for EITS use. Also, any materials must be appropriately safeguarded according to applicable standards including, but not limited to, virus protection, protected access and backups.
3. Users must not use EITS systems to engage in activities that are unlawful or violate federal or state laws, State or EITS security policies or in ways that would:
 - a. Be disruptive, cause offense to others, or harm morale.
 - b. Be considered harassing or discriminatory, or create a hostile work environment.
 - c. Result in State or EITS liability, embarrassment, or loss of reputation.
4. Users must maintain the integrity of information and data stored on EITS systems by:
 - a. Only introducing data that serves a legitimate business purpose.
 - b. Only acquiring, using, altering, disposing of, or destroying data or information with proper authorization.
 - c. Protecting data and information stored on or communicated across EITS systems, and accessing appropriate data or information only when authorized.
 - d. Protecting data and information communicated over internal or public networks to avoid compromising or disclosing nonpublic information or communications.
5. While EITS systems are primarily intended for business purposes, limited (incidental and occasional) personal use may be permissible when authorized by management and it does not:
 - a. Interfere with work responsibilities or business operations.
 - b. Involve interests in personal outside business or other non-authorized organizations or activities (which may include, but are not limited to, selling personal property, soliciting for or promoting commercial ventures, or soliciting for or promoting charitable, religious, or political activities or causes).
 - c. Violate any of the federal or state laws or State or EITS security policies.
 - d. Lead to inappropriate cost to EITS functional units. Excessive non-work related surfing and utilizing streaming services such as listening to music or watching videos is prohibited.
 - e. External Internet based instant messaging is forbidden.
 - f. Peer-to-peer file sharing is specifically forbidden.
6. Users must check all electronic media, such as software, diskettes, CDs and files for viruses when acquired through public networks (e.g., internet sites) or from outside parties by using virus detection programs prior to installation or use. If users suspect a virus, the applicable system(s) or equipment must not be used until the virus is removed. The matter must be immediately reported to the applicable manager and the Chief

Information Security Officer (CISO) or Department of Administration Information Security Officer (ISO).

7. Only EITS approved and properly licensed software will be used or installed on EITS computers and will be used according to the applicable software license agreements.
8. Users must ensure that any nonpublic information, data or software that is stored, copied, or otherwise used on EITS systems is treated according to the State and EITS standards regarding nonpublic information and applicable agreements and intellectual property restrictions.
9. Whenever a user ceases to be an employee, contractor, or other authorized user of EITS computer systems, such user shall not use EITS facilities, accounts, access codes, privileges, or information for which he/she is no longer authorized. This includes the return of all EITS IT resources including hardware, software, data, and peripherals.
10. Inappropriate use of e-mail includes, but is not limited to, sending and forwarding:
 - a. Messages, including jokes or language, that may be considered discriminatory, harassing, unlawful, defamatory, obscene, offensive, insensitive, or otherwise inappropriate (for example, messages about age, race, gender, disability, sexual orientation, national origin or similar matters).
 - b. Pornographic or sexually explicit materials.
 - c. Chain letters.
 - d. Information related to religious materials, activities, or causes, including inspirational messages.
 - e. Charitable solicitations unless sanctioned by the State or Chief Information Officer (CIO).
 - f. Auction-related information or materials unless sanctioned by the State or CIO.
 - g. Software or copyrighted materials without a legitimate business or instructional purpose.
 - h. Large personal files containing graphics or audio files (such as photographs and music).
 - i. Materials related to personal commercial ventures or solicitations for personal gain.
 - j. Information related to political materials, activities, or causes unless sanctioned or permitted by the State or CIO.
 - k. Unauthorized or inappropriate mass distribution or communication.
 - l. Any other materials that would be improper under this policy or other State or EITS policy.
11. Inappropriate use of the internet includes, but is not limited to, accessing, sending, or forwarding information about, or downloading from:
 - a. Sexually explicit, harassing, or pornographic sites.
 - b. "Hate sites" or sites that can be considered offensive or insensitive.
 - c. Auction or gambling sites.
 - d. Games, software, audio, video, or other materials that EITS is not licensed or legally permitted to use or transmit, or that are inappropriate or not required by State or EITS business.
 - e. Offensive or insensitive materials, such as sexually or racially oriented topics.
 - f. Any other materials that would be improper under other State or EITS policies.
 - g. Intentional importation of viruses, keyloggers, Trojans, or any other software that could be classified as malware or spyware.

CONSEQUENCES

Any inappropriate use of EITS computer systems or information may be grounds for discipline up to, and including dismissal. Should disciplinary action be required, the State of Nevada, progressive disciplinary procedures will be followed.

ENTERPRISE IT SERVICES
ACCEPTABLE USE AGREEMENT
ACKNOWLEDGEMENT

This is to certify that I have read and agree to abide by the guidelines set forth within the EITS Acceptable Use Agreement. As an employee or business partner of EITS, I fully intend to comply with this policy realizing that I am personally liable for intentional misuse or abuse of the department's computer systems or information. If I have any questions about this policy, I understand that I need to ask my supervisor or Chief Information Security Officer (CISO) for clarification.

**If I refuse to sign this acknowledgement form, my supervisor will be asked to sign this form indicating that I have been given time to read and have had questions answered about this agreement. The supervisor will read this statement to me prior to signing the document and advise me that by not signing this document my rights to use the department's computer systems may be denied and may affect my ability to meet my job requirements.*

NAME (please print)	
SIGNATURE	
FUNCTIONAL UNIT	
DATE	

*SUPERVISOR SIGNATURE (if needed)	
SUPERVISOR COMMENTS	
DATE OF NEXT REVIEW AND AGREEMENT	

Date of next review should coincide with date of next Performance Evaluation.