# [Agency Name]

# Acceptable Use Agreement

## Introduction

### Purpose and Applicability

This Acceptable Use Policy governs the use of all information technology (IT) resources at [Agency Name]. IT resources include, but are not limited to, computers, networks, hardware, software, electronic communication systems, and all forms of internet and intranet access. This policy applies to all [Agency Name] employees, contractors, and any other individuals who use or attempt to use IT resources owned, managed, or connected to the state SilverNet Network, whether legally or illegally.

### Responsibility of Users

As a user of these resources, you are required to read, understand, and comply with this policy. You hold the responsibility for all activities conducted under your user account or from your personal devices when connected to our network. IT resources are provided to support the mission of [Agency Name] and must be used in a manner that furthers departmental objectives and operational functions.

### Scope of IT Resources

IT resources within [Agency Name] encompass a broad range of technologies and digital platforms. This includes:

* Multi-user computer systems and networks.
* Single-user workstations and personal computing devices, whether free-standing or network-connected.
* Email applications provided or managed by [Agency Name].
* Access to the internet and intranet, including such access through personally owned devices.

### User Expectations

Users are expected to utilize IT resources efficiently, ethically, and lawfully, respecting the rights of other users and the integrity of the physical and system environments. [Agency Name] reserves the right to monitor all activities on its IT systems as permitted by law and to take necessary actions to preserve the security and proper use of its IT estate.

By accessing these resources, users agree to comply with this AUP and acknowledge that violating this policy may result in disciplinary action, including but not limited to, termination of access, disciplinary measures, legal action, and termination of employment or contracts.

## Acceptable/Unacceptable Use

### Responsibility and General Use

All users of [Agency Name] IT resources are required to protect the confidentiality, integrity, and availability of data and systems. This includes safeguarding sensitive information such as passwords, log-on IDs, network access data, and access codes from unauthorized access, alteration, destruction, or disclosure. Users are permitted to access and use [Agency Name] systems only when duly authorized and must adhere to all relevant [Agency Name] and state policies concerning data protection and information security.

#### 1. Personal Systems for Agency Business

* + Ownership and Control: When personal devices are used for agency business, [Agency Name] retains the right to any records or materials developed. Users must ensure these materials are safeguarded in line with [Agency Name]'s standards for virus protection, secure access, and data backups.
	+ Data Retention: Materials and data created or stored on personal systems for work purposes remain the property of [Agency Name] and should be managed as per the agency's data handling and privacy policies.

#### Prohibited Activities

Users must not engage in activities using [Agency Name] systems that:

* + Violate any local, state, or federal laws or regulations.
	+ Disrupt workplace harmony, offend others, or degrade morale.
	+ Constitute harassment or discrimination or contribute to a hostile work environment.
	+ Result in liability, embarrassment, or damage to [Agency Name]'s reputation.

#### 3. Data Integrity and Security

* + Users must introduce only data that serves legitimate business purposes to [Agency Name] systems.
	+ The acquisition, use, alteration, disposal, or destruction of data must be properly authorized.
	+ Data must be protected against unauthorized access, especially data communicated over public or internal networks.

#### 4. Personal Use Guidelines

[Agency Name] systems are primarily intended for business-related tasks; however, limited personal use is allowed if it:

* + Does not interfere with professional responsibilities or agency operations.
	+ Avoids activities involving non-approved business ventures or causes.
	+ Complies with all pertinent regulations and does not incur undue costs for [Agency Name].

#### 5. Software and Electronic Media Security

* + Prior to installation or use, all software, diskettes, CDs, and files acquired from external sources must be checked for viruses using approved detection tools.
	+ Only software that is approved and appropriately licensed by [Agency Name] may be installed and used on agency computers, aligning with software license agreements.

#### 6. Treatment of Nonpublic Information

* + Nonpublic information, data, or software that is stored, copied, or used on agency systems must be handled in accordance with stringent confidentiality standards and intellectual property laws.

#### 7. Termination of Access

* + Upon termination of their relationship with [Agency Name], individuals must cease using all agency IT resources and return all equipment, data, and access credentials.

#### 8. Email and Internet Use

The use of email and the internet must not involve:

* + Sending or forwarding inappropriate content such as discriminatory, offensive, or sexually explicit materials.
	+ Engaging in unauthorized activities like auctions, gambling, or dissemination of political materials unless expressly permitted by [Agency Name] or state regulations.
	+ Distribution of large personal files, chain letters, or any material that could impact network performance or violate policy.

#### 9. Monitoring and Enforcement

* + [Agency Name] reserves the right to monitor IT resource usage to ensure compliance with this policy. Violations may result in disciplinary action, including termination, legal action, and revocation of IT access privileges.

## Consequences

Any misuse or inappropriate use of [Agency Name]'s computer systems or information is subject to disciplinary action, up to and including dismissal. In the event of a violation, [Agency Name] will adhere to the State of Nevada's progressive disciplinary procedures, which are designed to ensure fair and consistent application of consequences.

## [Agency Name]Acceptable Use AgreementAcknowledgement

### Certification by User

I hereby certify that I have read and understood the [Agency Name] Acceptable Use Agreement. I agree to abide by the guidelines set forth within this policy. As an employee or business partner of [Agency Name], I acknowledge that I am personally responsible for my actions concerning the use of the agency’s computer systems and information. I understand that intentional misuse or abuse of these resources may result in disciplinary action against me, up to and including dismissal.

### Clarification and Questions

Should I have any questions about this policy, I will seek clarification from my supervisor or the [Agency Name] Information Security Officer (ISO).

### Non-Acknowledgement Procedure

If I refuse to sign this acknowledgement:

* + My supervisor will be notified and required to confirm that I have been provided time to read the policy and have had the opportunity to have questions answered.
	+ My supervisor will read this statement to me and will sign the form on my behalf to document that I have been informed of the policy.
	+ I am advised that refusal to acknowledge the policy may result in the denial of access to [Agency Name]'s computer systems, which could impact my ability to fulfill my job responsibilities.

### Documentation

This acknowledgement is part of my permanent employment record and serves as a testament to my commitment to adhere to [Agency Name]'s standards for the proper use of IT resources.

|  |  |
| --- | --- |
| 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.