SYSTEM ACCOUNTS APPLICATION

First Name_____ Middle Initial _____ Last Name_____

Home Address_____Birthdate_____

Principles - Academic freedom in teaching and research and the right of freedom of speech for faculty, staff and students are fundamental principles of the Nevada System of Higher Education. Nothing in these policies limits or removes the right of free speech or the academic freedom of faculty, staff, and students engaged in the learning process, nor relaxes their responsibilities as members of the NSHE community. This computer resources policy seeks to achieve objectives necessary for the legitimate and proper use of the NSHE computing resources. It is intended that these ends should be achieved in ways that maximally respect the legitimate interests and rights of all computer users. The NSHE acknowledges its responsibilities to respect and advance free academic inquiry, free expression, reasonable expectations of privacy, due process, equal protection of the law, and legitimate claims of ownership of intellectual property. Each institution within NSHE may adopt further computing resources policies congruent with these principles.

Use of Computing Resources - The computing resources of the Nevada System of Higher Education are the property of the NSHE and are intended for support of the instructional, research, and administrative activities of system institutions. Examples of computing resources are system and campus computing facilities and networks, electronic mail, Internet services, lab facilities, office workstations and NSHE data. Users of NSHE computing services, data and facilities are responsible for appropriate and legal use. Appropriate use of system computing resources means 1) respecting the rights of other computer users, 2) protecting the integrity of the physical and software facilities, 3) complying with all pertinent license and contractual agreements, and 4) never sharing your user accounts with others, 5) obeying all NSHE regulations and state and federal laws.

Students enrolled in kindergarten through twelfth grades using NSHE computing facilities and networks for K-12 classes and activities must abide by school district and NSHE policies. K-12 students enrolled in NSHE courses will be treated as NSHE students and therefore must abide by NSHE policies.

Inappropriate use of computing or networking resources, as defined in this policy, may result in the loss of computing privileges. If a violation of appropriate use occurs, a warning will first be given, notifying the individual that their action violates policy or law and that their access will be suspended if the action continues. All NSHE Code and campus by-laws shall be followed if the need to suspend computing privileges from faculty, staff, or students occurs. However, if the security and operation of the computing systems or networks are jeopardized, access may be immediately cancelled.

In congruence with NRS 281.481, NSHE employees shall not use the NSHE computer resources to benefit their personal or financial interest. However, in accordance with NRS 281.481(7), limited use for personal purposes is allowable if the use does not interfere with the performance of an employee's duties, the cost and value related to use is nominal, and the use does not create the appearance of impropriety or of NSHE endorsement. Personal use shall not interfere with official institutional use. An employee who intentionally or negligently damages NSHE computing resources shall be held responsible for the resultant expense. These policies also apply to NSHE students.

A NSHE account given to students, faculty, and staff is for the use only of the person to whom it is given. Unauthorized access or privileges are not allowed. In electronic communication such as mail, the user should not misrepresent his or her identity. No user should attempt to disrupt services of the computing and network systems, including the knowing propagation of computer viruses or the bombardment of individuals, groups, or the system with numerous repeated unwanted messages.

Privacy Issues - The NSHE provides security measures to protect the integrity and privacy of electronic information such as administrative data, individual data, personal files, and electronic mail. All FERPA (Family Educational Rights and Privacy Act) requirements are followed. Users must not circumvent security measures. While computing resources are system property and all rights are retained regarding them, these rights will be balanced with a reasonable and legitimate expectation that technical staff and administrators will not casually or routinely monitor traffic content or search files. The content of files shall only be examined when there is a reasonable suspicion of wrong doing or computer misconduct as determined by the institution president or his or her designee. Examination of files shall be limited to the matter under consideration. Disciplinary matters involving computer and network systems shall be handled in accordance with Chapter 6 of the NSHE Code. Within the limits of the capability of the computer system, NSHE shall protect the legitimate privacy interests of users and those about whom information is stored.

Software Management Responsibility - Users of NSHE computing resources are responsible for the legality of their software at all times. Data or software written or created by NSHE staff or students must not be copied or used without the author's permission. All commercial software must be licensed. Users must be aware of the license conditions and should never copy software without consulting the license agreement. Evidence of legal ownership is required. Individual employees and students are responsible for not installing illegal computer software on NSHE equipment. All NSHE institutions will enforce copyright laws and provide appropriate software management controls.

Internet Policy – You should be aware that the NSHE agreement with the provider for Internet access prohibits
1. attempted unauthorized access or destruction of any customers' information;
2. knowingly engaging in any activities that will cause a denial-of-service to any customers; and
3. Using products and services to interfere with the use of the network by other customers or authorized users, or in violation of the law or in aid of any unlawful act.

Legal Context - All federal and state laws, NSHE Code and regulations, and individual institutional policies are applicable to computer and network usage. Violation of NSHE Code provisions may result in disciplinary action. Violation of applicable laws may result in civil damages and criminal sanctions under state and federal law. Applicable statutes are summarized by System Computing Services and NSHE legal staff and can be found on the NSHE homepage on the World Wide Web. This list is by no means exhaustive, but it provides the individual user an overview of the provisions of these and other statutes as they relate to computer use.

Please sign below indicating you have read, understand, and will agree to the policies above.

_____   _____
Signature of Applicant   Date
NSHE does not accept electronic signatures

Submit application to respective department

FOR EMPLOYEE DEPARTMENT TO COMPLETE:

I: Employee Information

*Full Name: _____ *Title: _____

*Department: _____ *Contact Phone: _____

☐ Online   City:_____   Building: _____Room #:_____

PeopleSoft ID: _____   *Start Date: _____   **Term: _____

*Required for verifying employment **Only required for instructors*

EMPLOYEE TYPE:	ACADEMIC ONLY (INSTRUCTOR):	ADMIN OR CLASSIFIED
O Admin. O Classified O Academic	☐ Full-Time ☐ Part-Time	☐Full-Time ☐Part-Time ☐ Student Worker ☐ Facilitator ☐Lab Aid

II: Additional System Access

- ❖ *If additional access is NOT required please mark "No Additional Access"*
- ❖ *All instructors MUST have Peoplesoft Production access (allows access to class rosters and enter grades)*
- ❖ *All employees receive default access to OES (GBC Computer Login), email (Google) and Workday (HR)*
- ❖ *Shared network folders may be assigned by department Admin Assistant via Rapid Identity (ARMS)*
- ❖ *Special instructions may include "Needs same access as…" and/or "Only needs access to…"*

NONE:	PEOPLESOFT:	LEGACY:	Other:
☐ NO ADDITIONAL ACCESS	☐ Production ☐ TST	☐ Advantage ☐ Fin Data Warehouse ☐HRMS	☐ OnBase

Special Instructions :_____
_____

- ❖ *Expiration dates required for temporary positions and student workers with additional access*

Expires: _____

III: Signatures

This form must be completed with all relevant information. Failure to comply will result in a delay of an employee's complete computer access. This form may take 24-48 hours to be processed pending employee start date. If you have any questions, please contact the Peoplesoft Security Coordinator at 775-777-1810. Once signed and filled out completely, submit System Accounts Application to mailbox 12. Please DO NOT EMAIL any applications.

Supervisor Signature:_____Date_____

Supervisor Email: _____

-Internal Office Use Only-

AA Module Lead Signature: _____Date:_____

AD/CC Module Lead Signature: _____Date:_____

FA Module Lead Signature: _____ Date:_____

SF Module Lead Signature:_____Date:_____

SR Module Lead Signature: _____Date:_____

SACR Security Signature:_____Date:_____

OnBase Admin Signature:_____Date:_____

Project Lead Signature:_____Date:_____

VP Bus. Affairs Signature:_____Date:_____

Security Coordinator Signature:_____Date:_____