# MILES COLLEGE OFFICE OF INFORMATION TECHNOLOGY SERVICES POLICY MANUAL

## Access Control Policy

Access control procedures are used to authenticate all users who access each system. Such controls include, at a minimum, a login ID and a password for each user. All user accounts are required to change passwords periodically. The frequency is determined by the enforced length and complexity of the password combined with the sensitivity of the data protected following industry standards and guidelines. Authorized users are defined as any faculty, staff, or student at Miles College. Contractors, with the approval of the Chief Innovation Officer, may be provided a temporary user account to be used to access the Miles College network.

Access rights and privileges for all authorized users are maintained and managed user information. Confidential information is protected against unauthorized access regardless of form, computing environment, or location.

## Harassment

Harassment of any individual or group through email, websites, or any other online means is prohibited. Harassment takes many forms. In general, it creates an uncomfortable or hostile environment for the individual or group who is being harassed. If you send an email message to another person and make unwanted sexual advances, or if you send unwanted digital messages, or if you send many messages to another person, you are harassing that person. If you feel as if you are or have been harassed, please contact the Human Resources department at 205-929-1440.

## Cyber Bullying

A safe and civil environment is necessary for students to be successful in their educational pursuits. Cyberbullying or cyber harassment by any member of the Miles College community (student, faculty, staff, etc.) toward another individual constitutes conduct that disrupts the educational environment of the College. Examples of cyberbullying and cyber harassment include, but are not limited to, harsh text messages or emails, rumors sent by email or posted on social networking sites, and embarrassing pictures, videos, websites, or fake profiles.

Cyberbullying and cyber harassment are prohibited by many state laws, by various federal laws, and many jurisdictions throughout the international community.

Miles College will not tolerate lewd, intimidating or other disorderly conduct by or toward members of its community. The following are examples of instances where social media can cause harm to the College or a member of the Miles College community or may violate policies:

A Miles College student establishes a Twitter account that encourages others to submit negative anonymous messages to an account that will be redistributed by the account holder.

A member of the College community establishes a fake account under the name of an official College official or department and uses the name and trademark to post vicious comments or other content.

A member of the College faculty or staff uses his or her blog or social media account to berate or otherwise discuss engagement with or judgment of a student's work or other information considered confidential or proprietary by FERPA or HIPPA.

All other members of the College community are likewise prohibited from engaging in cyberbullying or cyber harassment, and instances will be adjudicated through the proper established channels.

Students who feel that they are being bullied or harassed through electronic technology should immediately report it to the Human Resources department at 205-929-1440.

## AWARENESS & TRAINING CONTROL

### Faculty and Staff Access and Training in the use of Technology

The Miles College faculty and staff have desktop computers and are provided with training in the use of applications. The College maintains technology appropriate to meeting the learning outcomes of its programs as well as to ensure faculty and staff access to technology.

### Security Assessment and Authorization

- Shutting Off Computers – Users have the responsibility to sign off the computer after using the computer or whenever they need to leave the computer for an extended period. When leaving a computer unattended, the user should lock/log off the computer.
- Virus Scan – Disks, removable media, and drives from any outside source have to be scanned for viruses prior to opening the contents on the disk/removable media/drives.
- Laptops – Laptops need to have virus software updated regularly.

### Monitoring and Enforcement

The Miles College Office of Information Technology Services (ITS) actively monitors the network and network resources. Monitoring activities are done regularly, and allow the ITS staff to detect, diagnose, and fix the normal day-to-day problems associated with operating a complex network. Monitoring also ensures that the network is used for its intended purpose-academics and academic support-and safeguards the College against legal risk.

When Miles College believes that technology, resources are being:

- Misused
- Inappropriately used
- Illegally used
- Used in a way that compromises or threatens the functioning of the system

- Used in conflict with College policies or local, state, federal, or international law

Miles College reserves the right to investigate and to take whatever action is necessary to maintain system integrity and security.

Miles College may review individual ITS records to the extent necessary to assess the problem and determine responsibility. Miles College also reserves the right to delete files, programs, network connections, and/or user accounts.

Both network and individual user log\s may be examined. This includes the logs on personal computers or servers that are attached to the College network, whether they are owned by the College or by other parties.

Abuse of technology privileges may result in appropriate disciplinary action. In many cases, the user is given a warning. Incidents involving students may be referred to the Dean of Students. If the user violates our policies more than once, then this may result in the loss of network and computer privileges.

In cases of illegal activity, the College may refer these matters to law enforcement authorities. The College reserves the right to respond to legally mandated requests for technology records. For example, if a law enforcement agency is investigating allegations of copying and distribution of copyrighted material and serves a court-approved search warrant upon the College, the College is obligated to permit the search.

- Unauthorized Access – Gaining unauthorized access to electronic information and communication systems.
- Inappropriate Websites – Accessing websites including but not limited to pornography, gambling, music file downloading, chain letters, and etc.

## Management and Access Controls

- Each ITS resource has a designee who is responsible for its security and management. Each authorized user of a system has a unique login ID. Any ID which is used to access a system and does not provide a unique user identification has access only to specific, limited system resources. Access to services and/or resources are suspended, and the appropriate account deleted when there is no longer a business or academic need for access. Employees are required to remove any personal data from Miles College computer systems before their last day at Miles College. The deprovisioning of the account is performed in a manner proportionate to the level of risk posed by such access, including immediate suspension of access and privileges and deletion of the report if necessary.
- When an employee is terminated, that responsibility falls upon the department and the user's supervisor to report termination. Information Technology Services, upon an employee's termination and departmental request, stores files on a network drive and makes it available to the new departmental data owner for a period of one (1) year, unless a request is otherwise made, at the end of which the files are purged from the system. Upon

notification from the Human Resources Director, ITS will disable the user account and email.
- When a student graduates from Miles College, their email account is deleted 6 months after graduation.

## BACKUP AND RETENTION POLICY

The goal of this policy is to ensure that Miles College has recovery plans against any kind of natural disaster, man-made disaster and/or system corruption. This policy focuses on the backing up of data, and the length of time backups are retained. Miles College retrieval time frame for data through backup is established and discussed.

### Backup Policy

Backing up data is a vital part of Miles College's defense to prevent against the loss of valuable information. Backups restore systems to the most recent backup performed and stored in case of a system failure or accidental deleting of a file. Back-ups are stored off-site in cloud-based locations.

### Retention Policy

Retention Policy refers to how long backup data files are stored. Miles College Office of Information Technology Services staff performs daily backups that are kept on tape or stored in the cloud for seven days. The weekly backups are kept up to two months on tape or cloud storage.

### System File and Log Retention Policy

System files and logs are kept for a year.

### System Maintenance

### Hardware (Including hardware issued and used offsite)

- Installing and Removing Hardware – Users are not authorized to attach/detach or install/uninstall any computer components without authorization from their Division Chair or Supervisor and involvement of ITS staff. This includes keyboard, mouse, printer, monitor, internal boards, or components. The Office of Information Technology Services is responsible for assigning computer components to specific computers.
- Storing Data – Users with the need for an extraordinary amount of data storage should notify their Division Chair or Supervisor, who will then work with the ITS staff to meet the user's needs. If portable media containing electronically protected information, the user must take the responsibility to store the media in a secured, locked location and dispose of the media per the media disposal guidelines when no longer needed.

- Acquiring and Disposing of Computer Hardware – The purchase of any computer hardware or the disposal of old computer hardware is made only with the approval of the Chief Innovation Officer and the involvement of ITS staff. Please check with the ITS staff on proper disposal of removable media (CDs or removable media) containing confidential information.

## Software

- Installing Software – It is the responsibility of the Office of Information Technology Services to install any software on Miles College computers. Users must submit a help desk request to have any program installed on any Miles College equipment by the ITS staff.
- Unauthorized Downloadable Software – The use of illegal downloadable software is prohibited. Downloadable software such as freeware, shareware, program demos, surveys, advertising, training, Internet browsers, copyrighted data, fonts, personal digital images, graphics, and private photos should not be downloaded without prior approval.
- Software Licensing Compliance – Violation of any software licensing agreement, copyright, or other intellectual property rights of third parties is strictly prohibited. This includes, but not limited to, computer software/data or related manuals and materials. Contact the Office of Information Technology for more information about software licensing agreements.

## Maintenance Time

All hardware and software maintenance times are typically performed after business hours, excluding the week of midterms and finals'. If hardware and software require disabling all faculty, staff, and students are notified 24 hours before, by Miles College official email.

## Internet and Email

- Email accounts are created only for Miles College faculty, staff, and students.
- Internet and Email Usage – The computer system, Internet, and email system are to be used for college business purposes only; however, the organization realizes that occasionally it is necessary for employees to use the Internet for critical personal issues, but such usage must be kept to a minimum. All computer use rules must be followed. Some examples of limited personal use may be to access other email accounts, bank accounts, and to verify travel plans.
- Your email account is the only official means of communication from the College, including administrators, faculty, staff, and students. You are expected to check it regularly.
- All restricted information must be approved, encrypted, and password protected.
- Mass emails should only be used for official college events or communications. The mass email system should not be used for private marketing, solicitation, etc. without prior approval.
- It is prohibited to use the Miles College email system to create, forward, and/or distribute any material that is disparaging or otherwise offensive.
- Viruses – The ITS network or any computer resources cannot be used to download or distribute pirated software or data, or to propagate any virus or variant thereof. Instant

messaging/chat rooms and the like are expressly prohibited to all employees unless specifically authorized otherwise.

**System Security**

- Shutting Off Computers – Users have the responsibility to sign off the computer after using the computer or whenever they need to leave the computer for an extended period. When leaving a computer unattended, the user should lock/log off the computer.
- Virus Scan – Disks, removable media, and drives from any outside source have to be scanned for viruses prior to opening the contents on the disk/removable media/drives.
- Laptops – Laptops need to have virus software updated regularly. The Office of Information Technology Services will provide users with practical avenues to accommodate anti-virus software updates.

**Spam Prevention**

It is the responsibility of each computer user to take steps to safeguard against increasing the amount of spam that comes into the College. The Office of Information Technology Services provides guidance to the user on the type of sites, emails, and email addresses that are safe and unsafe to use.

Questions on the above policy can be sent to its@miles.edu.

## INFORMATION SECURITY POLICY

Miles College Office of Information Technology Services has security policies in place for safeguarding data and information in its workstations, servers, mobile computing devices, storage devices, network, and communication devices. These policies also ensure that there is no theft of sensitive data, exposure of critical information, and theft, or damage to the College's devices. Any use of Miles College information technology systems contrary to this policy may lead to a withdrawal of access.

**Risk Assessment**

Miles College Office of Information Technology Services staff regularly assess unauthorized use of network; risk to network security; unauthorized access to information; unauthorized request for information; and third-party unauthorized transfer of information; systems corruption; a breach of integrity. In addition, these risk assessments are done to ensure the protection of our student information. Risk assessments are conducted consistent with system criticality and are performed by ITS staff on a yearly basis. Cybersecurity tests are performed bi-annually and network penetration is tested twice a year to identify breaches in security.

**Password Security**

- Never disclose your password to others, in person, either by phone, or by email.
- Never leave your password at the default. Change it immediately.

- Make your password eight or more characters.
- Use a combination of upper and lower case letters, numbers, and special characters like @!&[*
- Never use all numbers or all letters.
- Never use personal information someone could easily guess or discover. For example, your pet or hometown, etc.
- Never use any word found in a dictionary or the name of a sports team.
- If you must write down your password, keep it in a locked location.
- Change your password frequently, at least every 90 days.
- Miles College ITS staff will never ask for your password via email or telephone.

**Desktop Security**

- When you leave your desk, log off or lock your workstation with Ctrl+Alt+Delete or Windows Key + L
- At the end of day, logoff or restart your computer.
- Do not download or install a screensaver to your workstation, choose a pre-installed screen saver.
- Do not install software-commercial, shareware, or freeware-borrowed or purchased from another user.
- The use of peer-to-peer applications to share copyrighted materials, such as music or movies, is a direct violation of copyright laws. Do not do it!

**Laptop Security**

- Your laptop is easy access for identity theft. Protect it like your purse or wallet.
- When traveling, lock your laptop in the trunk of your car.
- Password protect or encrypt any sensitive information stored on the laptop.
- When you are away, lock it in a drawer, overhead bin, cabinet, or office.
- Never leave your laptop unattended in a public place, even for “just a minute.”
- Never check your laptop as luggage when you travel.
- Never leave your laptop in a car in plain view on the seat or the floor.
- Never leave your laptop in a car overnight.
- Never use your business card as a luggage tag to identify your laptop case.
- Encrypt your hard drive if it is possible to do so.

**Spyware**

Spyware is used by the advertising industry and by hackers. Spyware and Adware are software, when installed on your computer, may send you pop-up ads, redirect your browser to certain web sites or monitor web sites you visit. Extremely invasive versions of spyware may track exactly what keys you type to steal username and password information.

- The installation of an anti-spyware/anti-virus package is encouraged to fight spyware and other malicious software.

- Other tips to fight malicious software: do not click on links with pop-up windows, choose “no” when you are asked unexpected questions, be wary of free, downloadable software, and never follow email links.
- If you believe you have spyware on your system, please contact ITS personnel for assistance in having it removed.

### Voice Mail

- The minimum password length is set to four digits.
- To create a strong voicemail password, use five or more digits.
- Do not set your password to the same as your phone extension or employee number.

### Viruses, Worms and Trojans, Malware

Viruses are computer programs designed to cause trouble to your computer. Worms are programs that replicate themselves and look for holes in networks or send themselves via email to infect as many other computers as they can. Trojans are programs that carry hidden, malicious programs.

- Fight malicious software by installing an anti-spyware/anti-virus package.
- Do not open email files from anyone you do not know.
- Do not open email attachments containing executable or movie files.
- Some files extensions to avoid include: .EXE .COM .CMD .PIF .SCR .VBS .WMF .ASF

### Emails and Spam

- Always password protect your email account.
- Do not use your personal email account to send or receive sensitive information (credit card numbers, bank account information, SSNs, etc.)
- Do not send or forward email messages such as chain letters, jokes, and news containing lewd, harassing, or offensive information.
- Be wary of unsolicited attachments, even from people you know. Viruses travel incognito, using legitimate email addresses to trick their way into users’ machines.
- Do not click a link in an email. Even if the link says one thing, it may send you somewhere else.
- Report other email abuses by calling 205.929.1498.

### Phone/Mobiles Device Security Tips

- Set a password or PIN on your phone to prevent unauthorized use and make it more difficult to hack if stolen or lost.
- If your phone has Bluetooth functions, disable them until they are needed, and then set visibility settings to “hidden” so your device cannot be scanned for other Bluetooth devices.
- Limit the amount of sensitive or personal information, such as passwords and account information, stored on your mobile device.

- Consider purchasing anti-virus software for your phone, and make sure it is frequently updated.
- Download ringtones, games, and other personalized content only from trusted, classified sites.
- Treat mobile devices as you would your wallet, keys, or laptop. Do not leave them in plain sight and keep them close to you at all times.

**USB Drives/Thumb Drives/Jump Drives and other Mass Storage Devices**

These drives are a very convenient and commonly used method to hold personal files and schoolwork. Unfortunately, the small physical size of these devices makes them easy to lose or to steal.

- If you use a mass storage device to store any critical or sensitive data-class work, research data, personal files, etc.-make sure that the data is protected.
- Many modern mass storage devices come with a security utility that can encrypt sensitive files.
- If you do not have encryption on your mass storage device, do not keep sensitive information on it.

**Response to Incident**

Miles College Office of Information Technology Services requires notification of incidents of unauthorized usage, access, and activity.

**External Vendors**

External vendors providing service to Miles College and those who have access to data information have to maintain the integrity of that data and information and safeguard it against security leaks. Other College units using external vendors for technology needs have to forward the contracts to ITS for review of the arrangements. External vendors are not provided an email address.

If you suspect that you have been a victim of a computer crime or abuse while at Miles College, please report the incident by contacting the ITS help desk at helpdesk@miles.edu. Give as many details as possible: Who, What, When, and Where.

Questions on the above policy can be sent to helpdesk@miles.edu.

*Last Updated: September 2021*

## INFORMATION TECHNOLOGY SUPPORT POLICY

The goal of this policy is to establish service expectations and inform faculty, staff, and students at Miles College of the method by which requests are prioritized and the expected resolution timeline. All Helpdesk requests will be resolved within 24-48 hours. The Helpdesk is the first and single point of contact for technology support for all Miles College faculty, staff, and students. Information Technology (ITS) provides technology assistance primarily by email (helpdesk@miles.edu) or through web-based portal (ITS), and walk-in requests for technical support. Walk-in requests for support are only handled Monday-Friday, 8 a.m. – 5 p.m. The Office of Information Technology Services uses ITS help desk to record and track all technology requests. Technology problems and requests for service are resolved in an efficient and timely manner.

The Office of Information Technology Services staff is committed to providing hardware, software, network, telephone, cable TV, media, event, and lab support for Miles College faculty, staff, and students during business hours and all other approved times. A standard process and single point of contact for all technical problems are necessary to eliminate confusion over whom to call for an issue. The Office of Information Technology Services is comprised of a team of support technicians and server/network support personnel who are available to provide faculty, staff, and students and in special cases approved guests of Miles College support for technical problems or questions submitted via email or the online self-service process. Roles and responsibilities in the Office of Information Technology Services are to maintain a courteous and professional manner at all times when interacting with the college faculty, staff, and students.

The Office of Information Technology Services staff who receive calls directly, rather than through the ITS portal should advise the caller to place a ticket in ITS or email the Helpdesk. The caller is informed that calls made directly to technician staff are subject to delays, missed calls, and delayed resolution of problems. If a trouble ticket requires escalation, the ITS staff is to maintain ownership of the problem and escalation process. Users are to be advised that they will be contacted by an ITS support staff. The staff is to follow up to ensure resolution is achieved, and the ticket is updated.

When entering or updating tickets, the technician is to describe the problem accurately and include details. Generalizations such as “Broken” or “Fixed” are not sufficient to communicate worthwhile information. The ITS support staff in charge of resolution is responsible for updating tickets so that when a user asks for status updates, essential status updates can be provided. The ITS staff is responsible for conferring with each other and deescalate problems, to management, that they cannot fix within a reasonable timeframe.

The ITS Help Desk administrator monitors ITS to make appropriate determinations as to resources required. Problems and requests within a specific priority category are handled on a first-come first-served basis. All Service Outage Event Notifications are posted promptly by email or by direct contact.

**Procedures**

To report a problem, the user must provide the following:

- Name
- Student/Employee ID number
- Email Address
- Telephone Number
- Location
- Problem Type
- Problem Description

This information serves to verify identity and contact information and identifies equipment location, if applicable.

- Email: helpdesk@miles.edu Include Name, Student ID number, Email Address, Telephone Number, Location, Problem Type, Problem Description, and all necessary details.
- Enter a self-service web ticket at the following URL: http://itsupport.miles.edu
- To schedule support for a campus event, email helpdesk@miles.edu. For more information, contact Director of Building Operations or Director of Student Activities

*Last Updated: September 2021*

## HARDWARE/SOFTWARE PURCHASE POLICY

This policy applies to any purchase of hardware or software using institutional, federal, or grant funds. The requesting department is responsible for providing the funds to purchase software and hardware using their budget. ITS makes purchases with its funds in the event the software and hardware benefit the entire campus or multiple departments. This decision is made on a case-by-case basis.

**ITS Involvement:**

1. **Software purchases require ITS involvement if any of the following are true:**
    1. Assistance will be required to install or implement the software.
    2. Software or data used by the software will be stored on an internal server.
    3. Software will use and/or store data stored in the Student Information System (SIS).
    4. Software or hardware will require campus credentials (Active Directory or Single Sign On) for authentication.
    5. Software or hardware will be made generally available to students and/or employees.
    6. Integration with other campus systems is required.
    7. Ongoing support from ITS is expected.
2. **Purchases of the following hardware require ITS involvement:**
    1. Desktop or laptop computers.
    2. Tablets.
    3. Any individual piece of hardware with a purchase price greater than $500.
    4. These items may not be paid through expense reimbursement to an individual. If paid by check request, the check must be paid to the vendor selling the hardware.
    5. ITS involvement is not required for hardware that will change ownership prior to use/activation and will not be used for conducting College business (e.g. a tablet to be given away in a drawing).
3. Purchases of permanently mounted hardware require ITS involvement.
4. Purchases of peripherals (hard drives, adapters, mice, keyboards, etc) require ITS involvement if there is an expectation of future support. ITS involvement is always recommended to ensure device compatibility and best pricing.
5. **As needed, ITS will draft a statement of work that outlines:**
    1. Requirements for implementation of the hardware or software.
    2. Expected milestones and timelines.
    3. Levels and expectations for post implementation support.
6. ITS does not support hardware and software purchased without ITS involvement. Support for such systems would be best effort and only as time allows.

2. **Accessibility:**
    1. Software and non-peripheral hardware purchased by the college should consider accessibility as a factor in purchasing decisions.
    2. **Hardware or software purchased by the college should comply with one or more of the following standards as evidence of accessibility:**

    1. Section 508 of the Rehabilitation Act
    2. W3C Web Content Accessibility Guidelines (WCAG) 2.0
3. **As part of the purchasing process, the vendor should supply:**
    1. A valid Voluntary Product Accessibility Template (VPAT)
    2. Another statement by the vendor that provides an evaluation of the product's accessibility.
4. **The office making the purchase will provide to ITS:**
    1. Documentation regarding accessibility supplied by the vendor.
    2. A list of any exceptions to the above accessibility standards identified in the vendor documentation.
5. In the event that no suitable product is found that meets minimum accessibility requirements, a description of the reason the product was selected should be submitted to ITS. ITS will store this documentation for the duration the product is in use.

**Hardware Upgrade Policy**
As there is need and as the campus hardware budget allows, Information Technology Services (ITS) aims to upgrade campus faculty and staff computers with improved machines every 3-4 years to help maintain maximum computing efficiency and productivity. ITS will be responsible for evaluating need and determining the best upgrade option. Though ITS routinely monitors the performance of all faculty and staff computers, please report all computer performance issues to the ITS Help Desk.

Staff members currently using a desktop and requiring an upgrade to a laptop are requested to give written justification including specific reasons for their portability needs and have approval from their department head and Vice President of Academic Affairs. ITS will carefully review all requests. In all situations where portability is not critical to job function, users will be required to use a desktop PC. If the user's request for a laptop is granted, the user's laptop will be swapped for their desktop PC. The advantages of a desktop PC are savings in purchase and support costs, improved performance and reliability, larger screen size, and good ergonomics. Faculty members currently using laptops issued by the college, who do not have a need for portability, are also encouraged to switch to a desktop. If the laptop becomes damaged or unrepairable, ITS reserves the right not to issue the faculty member another laptop in favor of switching them to a desktop computer.

**New Computer Request Policy**
Computer requests for new hires and or special projects should be submitted during the onboarding process or via the ITS help desk. If the campus hardware budget is exhausted, departments necessitating additional hardware may be required to pay for the expense out of their available budget, pending approval from the Comptroller's Office and ITS. All equipment must be purchased by ITS, meeting Miles College standard hardware specifications. You will be asked to return any computer equipment not purchased through ITS.

**New Employees/Change of Position and/or Office**
All Miles College employees are to be given an email address, user login, and a computer/laptop (if applicable). Email addresses and user login will be created after completion of the onboarding

form located on the ITS help desk and approval from the Human Resources Director. User account creation can take up to 3 business days to complete. It is the desire of ITS to deploy hardware for new employees prior to the employee's arrival to campus. However, this is dependent on the availability of ITS staff and other pressing issues that may arise.

Any changes in job position or office location that require moving or upgrading hardware should be initiated by the department head. The department head should send a request to the ITS help desk.

*Last Updated: September 2021*

## GOLF CART POLICY & PROCEDURE

The following policy and procedures applies to anyone operating a golf cart on college owned or leased property. The purpose of this policy and procedure is to help ensure the safe operation of golf and other utility cart vehicles on campus.

Any individual operating a golf or utility cart on college owned or leased property must adhere to the following policies and procedures. Any violation of these rules may result in disciplinary action:

- Carts are to be operated with the utmost courtesy, care and consideration for the safety of the operator, passengers, pedestrians and College property. Pedestrians shall be given the right-of-way at all times.
- Carts are provided to facilitate performance of work duties.
- Carts are to be properly equipped and utilized appropriately and safely.
- Per NH RSA 215-A carts are prohibited from operating on "off campus" public roadways except when crossing onto other College owned or leased property. When crossing a public roadway the cart operator must do so at a 90 degree angle and must yield to traffic.
- Procedures and details for operating carts on campus are specified in the section below:

### General Operation

- Vehicles shall not be operated in a manner that may endanger drivers, passengers or other individuals (pedestrians), or harm College property. Dialing and/or texting on mobile phones or manipulating other devices is prohibited while operating a golf cart.
- Golf cart operators (drivers) should be limited to employees (including student employees), authorized lessees and/or contractors. Passengers may include campers being shuttled by camp employees or lessees, athletes being shuttled by event personnel or athletic trainers, guests being shuttled for college events, and CS community members being shuttled by Campus Safety.

### Passenger Limit/Load Capacity

- Do not exceed the passenger limit, seating designation, capacity, or load capacity designated by the vehicle's manufacturer.

**Parking**

- Do not block any access or egress (natural flow of traffic) to entrance areas to buildings, stairways, access ramps, or main thoroughfares.
- Park carts in a single row so they do not block or interfere with the normal flow and path of pedestrians or other carts.
- Cart operators are responsible for the security of ignition keys during the time that a cart is assigned to them. Any time a cart is unattended; the ignition shall be turned off, the key removed from the ignition, and in the possession of the authorized operator.

**Driving Rules**

- No one under the age of eighteen (18) is allowed to operate a cart.
- A valid driver's license is required to drive a cart on campus.
- Carts will be driven in compliance with the common "rules of the road," adhering to all traffic laws and regulations, regardless of whether they are being operated on service drives, sidewalks or roadways.
- Pedestrians have the right of way. Cart operators must reduce speed on walkways when pedestrians are present and space is limited. Maintain safe distance between golf cart and pedestrian. Drive on the right side of sidewalks/paths similar to street driving rules.
- When walkways are crowded (between classes), golf cart operators must either stop, proceed around pedestrians at a very slow pace, or if ground conditions are dry may temporarily proceed around a group of pedestrians on the turf/grass.
- All occupants in the golf cart shall keep hands, arms, legs and feet within the confines of the golf cart at all times when the cart is in motion.
- Never back up without first making sure there is no person or obstructions behind the cart.
- Reduce speed to compensate for inclines, corners, bumps/rough terrain, pedestrians, and especially on wet/icy conditions.
- Avoid abrupt stops (skidding), high speed turns and any form of horseplay.
- Avoid driving over sprinkler heads, drain covers and avoid turf (grass) during wet conditions.
- Do not jump curbs or other obstacles that may damage the cart.
- Be certain to set the brake whenever stopping and leaving the cart.
- Drivers and passengers must remain seated whenever the vehicle is moving. Do not stand on or ride on the bumpers, fenders or club storage area. Drivers should stop cart when looking or scanning beyond a 90-degree field of vision (stop before turning your head to view something behind you – 180 degrees).

**Checking out golf carts**

- Authorization for use of golf carts originates with the Information Technology Services (ITS) Department.

- The Admissions Office and ITS are the primary users of the golf carts. Outside requests for use of the golf carts is prioritized by need and function. We encourage requests for use of the golf carts be submitted at least 2 business days in advance.
- If request for use of golf cart is approved, the individual will need to report to the ITS to be issued a key. If there are no available carts at the ITS officer, the individual will need to go under the bleachers at the football stadium to get a cart. The key must be returned after use of the golf cart is complete.

**Accidents**

- Drivers involved in an accident must immediately report the incident to their supervisor and to Campus Safety, regardless of whether property damage or personal injury occurred.
- Accidents involving injury must be reported to Campus Safety, the injured employee's immediate supervisor, and Human Resources.

**Enforcement**

- Golf cart operators violating these procedures may be prohibited from operating a golf cart by their Department Head, Information Technology Services, and/or the Director of Campus Safety