user is any member of the administration, staff, faculty, or student body who has been assigned a user account consisting of a valid user ID and password. Family members of people in one of the above groups who are assigned user accounts by Campus IT are also authorized to use the JUTN computing systems.

2. You must use only the computer account which has been authorized for your use. You may not use someone else's account. If you have trouble using your account or if you need more than one account, contact Campus IT.
3. You are responsible for the use of your computer account. You should take precautions against others obtaining access to your computing resources. Do not make your account available to others for any purpose.
4. Although JUTN does not make a practice of monitoring email, JUTN reserves the right to retrieve the contents from Johnson owned computers such as email messages for legitimate reasons, as to find lost messages, to comply with investigations of wrongful acts, to respond to subpoenas, to stop the spread of viruses, or to recover from system failure. Additionally, pornography, gambling, and violation of copyright laws are stumbling blocks for many Christians. In order to protect members of the JUTN community, JUTN blocks sites which the administration has deemed inappropriate for Christians, and students should not attempt to access such sites.
5. The following practices are unacceptable:
    - Attempting to circumvent the restrictions associated with your computer account.
    - Attempting to access files for which you do not have authorization or attempting to monitor others' network traffic without authorization.
    - Copying files or data belonging to the University without authorization. Written authorization from the Vice President for Student Life must be obtained before one can copy programs belonging to the University.
    - Using the network to illegally transfer copyrighted material or to permit others to illegally transfer copyrighted material. It is JUTN's policy to honor copyright restrictions and software licenses. Only software that has been legally obtained may be used on university computers.
    - Modifying system configurations on university-owned computers or network devices. Only Campus IT can perform or authorize such changes. Campus IT may remove personally owned hardware or software from university computers or network systems if they believe that it interferes with the computers' or network's operation.
    - Using the network to harass others. This includes, but is not limited to, the use of anonymous or forged email, spam, and other unsolicited messages. Port scanning of systems (campus or Internet) is prohibited and considered harassment.
    - Using the network to post vulgar, profane, obscene, libelous, false, or malicious content on social media, discussion groups, or other online forums hosted on either Johnson or off-campus servers.
6. To minimize the impact of your work on the work of others, do nothing that will prevent others' use of the facilities or deprive them of resources.
    - The use of peer-to-peer (P2P) file-sharing networks, such as Ares or Limewire, is prohibited. Such networks are used on a widespread basis to transfer pornography and to illegally transfer copyrighted material, and the use of such networks places an undue burden on the JUTN network. If you have any questions or concerns about this policy, please contact Campus IT. Legitimate BitTorrent downloads such as Linux disk images and game updates are permitted.
7. Students are responsible for making backups of their files and email account data.
8. Student workers should use departmentally assigned accounts when logging on to university staff computers. Students should not log on using their Student ID accounts unless directed to by Campus IT.