User Guidelines for UCScienceNet (UCSN)

UCScienceNet (UCSN) is a dedicated research network providing 10 Gb/s end-to-end data transfer capability to specific research locations, culminating in an aggregate 100 Gb/s network to Internet2 and other National Research Networks (NRENs).

The policies found on the Information Security website: http://www.uc.edu/infosec/policies.html should be followed by all users of UCSN.

FAQs

Q: How do I get “on” the research network?
A: UCScienceNet is available to any faculty member conducting research at UC. If your department has dedicated resources, contact your department IT representative for an account. If not, contact UCIT R&D via our website: http://www.uc.edu/ucit/services/research-development.html

Q: Is there a cost involved?
A: There may be some startup costs involved depending on your location and specific needs. These costs can include network interface cards, cabling, switches, etc. There are currently 8 locations that researchers can connect to. Installation for additional nodes of UCSN is unique, thus there is no flat-rate cost. Some factors that influence cost include: proximity of node room to research computers; cost of fiber cabling from node room to nearest UCSN hub; and cost to install new dedicated CAT6A cabling.

Q: Does anyone track my usage?
A: All access to Internet2 must be done from defined endpoints. That is, you can’t just “surf” to see what is out there. Connections are logged but not tracked in real time.

Q: Do I have to pass some sort of security review?
A: While there may be a requirement to obtain security clearances from grants, etc. There is no review required by UCIT to use UCSN. However, it is important that access to the network be physically and logically secure to prevent security breaches. This means locked rooms with limited access and requiring all users of machines that access UCSN to have separate accounts. Grant awards may have other security requirements. The UC Information Security Protection Guidelines can be found at: http://www.uc.edu/content/dam/uc/infosec/docs/Guidelines/Checklist_for_Protecting_Information_Guideline.pdf

Q: Who manages my servers?
A: If they are co-located in our data centers the center staff can manage your servers. Otherwise you are responsible for installing updates, backing up your data, etc. Note that there are minimum standards for

1 Need more information? Contact us at ucitresearch@ucmail.uc.edu or brett.kottmann@uc.edu
operating secure servers. These can be found at the UCIT policies page:
http://www.uc.edu/infosec/policies.html

Q: What kind of equipment do I need?
A: Needs vary according to your compute, storage, etc. requirements. Contact UCIT for an evaluation of your needs via the contact information at the end of this document.

Q: Can I be connected to the regular network and high-speed network at the same time?
A: No. Only one network connection can be active at a time.

Q: How do I connect my computer?
A: Your equipment will need a high-speed network interface card (NIC) to connect to UCSN. Most machines/servers do not come with this card as a default, so you will have to request an upgraded NIC that can handle at least 10Gb/second. As of September, 2017, an upgraded NIC costs about $175 as a separate item. If you do not have a high-speed connection in your office/lab one will have to be installed.

Q: How do I reach other sites through the high-speed network?
A: The security of UCSN depends in part on known endpoints. That is, we know what machine you are using and what specific site (URL or IP address) you are visiting. This information allows us to route you through the high-speed network. That is why we require your MAC address and the destination IP. Changes and additions must be submitted to UCIT for processing. See contact information at the end of this document.

Q: Is there a checklist I can use to make sure I am following the correct procedures?
A: For users on UCSN you may use the following checklist:

- Secure (locked) room with limited access
- All users have separate accounts
- All users made aware of security restrictions/implications
- (College/dept issue) Grant or project restrictions (if any) are implemented
- (College/dept issue) Implement Information Security Protection Guidelines as needed for FISMA, HIPAA, etc. data:
  http://www.uc.edu/content/dam/uc/infosec/docs/Guidelines/Checklist_for_Protecting_Information_Guideline.pdf

*As noted above, network equipment (switches, etc.) have a higher security standard.

2 Need more information? Contact us at ucitresearch@ucmail.uc.edu or brett.kottmann@uc.edu