Computer Exception Form

Chemistry & Chemical Biology (CCB)

PURPOSE: To request a wired network connection for self-supported devices.

NOTE: If your networking needs are fulfilled using Cornell's wireless network (RedRover, eduroam), this form is not required. That network permits self-registration and requires no jack activations.

Chemistry IT is available to assist in filling out this form, or clarifying your options and the trade-offs. We welcome you to contact us:

ChemIT@cornell.edu
250 Baker Lab
607-255-6278

Network Options

1. RedRover wireless, by Cornell IT (CIT)
Cornell's wireless network, including eduroam, RedRover, and Visitor. (Physical wall jack not used.)

2. Chemistry network, by Chemistry IT
Default wired network. Remote access to fixed IPs with VPN.

3. AccessNet, by Cornell IT (CIT)
A wired network with RedRover-like access, such as self-registering and no remote access.

4. RedNet, by Chemistry IT
Chemistry's wired network. Direct remote access to fixed IPs, less protected network.

Required by CCB's Computing Committee

This application requires that the group's faculty member acknowledge and accept that:

- Chemistry IT will not be expected to provide IT support for these devices. Chemistry IT is not responsible for troubleshooting, for example.
- Chemistry IT's billing to the group will still be charged.
- The faculty member, or group designate(s), serves as the Local Support Provider, as defined within University policy. Review page 3.
- The faculty member will assume responsibility to ensure that University policies are being followed on this device.
- Routers and printers are discouraged and generally unnecessary on CCB RedNet. If still deemed necessary, register such devices with Chemistry IT by filling out page 2.

Faculty member signature: _____

Date: _____

Required by Chemistry IT to enable network connections

Port jack number(s) to activate or convert to a non-Chemistry IT network (e.g. AccessNet or RedNet):

Please submit this form to Chemistry IT.

Optional: Only fill out if AccessNet is not sufficient

If CIT's AccessNet will not meet the needs of a research group, CCB's **RedNet** is available. This wired network will only contain self-managed devices, not devices managed by Chemistry IT.

To request access to this segregated, more open access, less protected network, please complete the requested information below.

Required by CCB's Computing Committee

In addition to the acknowledgements on the first page, the faculty member affirms that CCB's RedNet is required because (check one or more):

- ❑ The faculty and/or other group member(s) requires remotely accessing their device(s) and they don't want to, or cannot, use a VPN to get to their system.
- ❑ Other reason(s):

Routers and printers are discouraged on RedNet, and wireless routers are problematic because they can interfere with Cornell's RedRover/ eduroam wireless network. If you still intend to use these devices, please list them here:

Required by Chemistry IT to enable network connections and for device inventory

Ensure desired port jack number(s) are entered on page 1, as well as:

MAC address of wired Ethernet adapter card (required by CIT) Ask Chemistry IT for assistance, if desired.	DNS prefix** (optional)	Local Support Provider's name and NetID (if not faculty member)	System info: serial number	System info: Manufacture and model	Cornell system or private?

**DNS name convention (for the A record) is <DNSprefix.groupname.chem.cornell.edu>. Please contact Chemistry IT if this naming convention represents a problem.

Excerpts from University Policy 5.4.1

Security of Information Technology Resources

Local Support Provider

DEFINITION: An individual with principal responsibility for the installation, configuration, security, and ongoing maintenance of an IT device (e.g., system administrator or network administrator).

RESPONSIBILITIES: Maintain knowledge of information technology (IT) devices under his or her control through identification and understanding of their usage. Follow safe security practices when administering IT devices under his or her control. Follow electronic security incident reporting requirements in accordance with University Policy 5.4.2, Reporting Electronic Security Incidents.

User

DEFINITION: Any individual who uses an IT device such as a computer.

RESPONSIBILITIES: Comply with the current policies, requirements, guidelines, procedures, and protocols concerning the security of the university's electronic networks and devices. Protect IT resources under his or her control with measures such as the responsible use of secure passwords, appropriately establishing an administrator password, and timely antivirus updates. Assist in the performance of remediation steps in the event of a detected vulnerability or compromise. Comply with directives of university officials, such as the security officer and his or her delegates, to maintain secure devices attached to the network regarding software patches and/or virus protection. **Take note of circumstances in which he or she may assume the responsibilities of a local support provider**, e.g., by attaching a personal computer to the Cornell network or working remotely from home. Follow electronic security incident reporting requirements in accordance with University Policy 5.4.2, Reporting Electronic Security Incidents.

University IT Policies

- https://www.dfa.cornell.edu/tools-library?tab=policy_library
- http://www.it.cornell.edu/policies/university/security/index.cfm

University IT security policies at the above pages include, but are not limited to, the following:

Security of Information Technology Resources, Policy 5.4.1

- http://www.it.cornell.edu/policies/university/security/securityitr.cfm

Information Security, Policy 5.10

- http://www.it.cornell.edu/services/guides/data_discovery/policy_details.cfm

Reporting Electronic Security Incidents, Policy 5.4.2

- http://www.it.cornell.edu/policies/university/security/electronicsecurityreport.cfm