

# Cold Room Policies

## I. Background to Policies

**Reactive Work:** Reactive work will be defined as all work that is done as a reaction to a system event or user need. Examples would be handling system problems, hardware failures, requests for changes in authorizations, accounts, application settings. Work that has a business need to happen in a rapid fashion, either to alleviate a problem with an existing process or system, or a change in configuration. Reactive work, in general, will be work that can be completed in under half an hour, or the process for determining the method of remedying the problem can be determined within a half hour.

**Proactive Work:** Proactive work is all work that can be scheduled for some future time. Work that needs to be done to maintain processes and systems in good functional and secure condition. Proactive work will be scheduled and will be a lower priority than reactive work.

## II. Change Management Process

All changes requests to supported systems will go through the UCAT Change Management system, so that they can be tracked. Some system changes will be deemed to be proactive work, and will be tracked in a different projects queue for ease of maintenance of the reactive work queues.

Requests for change will be acknowledged by the Change Management Committee, and a timeline suggested for those changes deemed to be proactive work.

UCAT Staff may need to wait for the next scheduled maintenance period to perform some change requests, due to system downtime requirements of the request.

Changes to monitoring, process, addition of new applications or machines, and modifications of configuration files will need to be approved by the Change Management Committee before they are put into place.

## III. Scheduled Maintenance Procedure

UCAT staff will set scheduled maintenance windows, and adhere to them for system changes which require system downtime. Currently this maintenance window is between 8 am and noon on Sundays. We will limit the systems downtimes as much as possible. Care will also be taken to not make changes that require a downtime to systems outside of the scheduled maintenance time period.

For each scheduled maintenance period, if a maintenance is going to be performed, an email will be sent to the mailing list of the affected system, system-announce or if it is just a particular application (for instance a restart of a system that is known to take a while to recover) system-application-announce. The announcement will contain the duration of the maintenance, and a general description of what is going to be done (including the brief description of any and all patches which are going to be installed).

## IV. Backup and Restore Procedure

Backups will be scheduled on a regular basis. Incremental backups will be done nightly. Full backups will be done approximately monthly. A copy of full backups will be stored in a different physical location within 2 days of the full backup.

Recoveries will be able to be done as needed, recently modified files (within the last 2 months) should be available within a normal reactive work schedule. Files deleted longer ago than 2 months may not be available as rapidly, but should be available within 3 business days.

The Cold Room will maintain backups for the documented necessary retention period for various legal requirements, currently this appears to be 6 years. Cold Room will maintain the necessary software to restore data from all archived tapes within this time period.

#### V. **Physical Access Policies**

Physical access to the Cold Room will be limited to those with operational need to enter the Cold Room. Access will be via key pad and biometric hand readers. Any personnel not part of the Cold Room staff will be monitored by a Cold Room staff member. Access to the Cold Room can be arranged as needed during normal business hours. Emergency access after hours will be accommodated, the method for starting the process of gaining access after hours will be to call the Cold Room phone line and leave a voice message with your name, contact phone number, and reason for needing access. A Cold Room staff member will return all calls within a reasonable time for after hours emergencies.

#### VI. **Firewall Modification Requests**

All requests to modify firewall rules must be formally submitted to the Network Analyst staff. Firewall modification requests must be within the general security models or they will not be completed. Requests for firewall modifications will be completed with 1 business day.

#### VII. **Hardware Requirement**

All new machines going into the Cold Room must be 1U or 2U rack mountable. All hosts will need to undergo a security scan or audit prior to being relocated into the Cold Room. Also, while the Cold Room provides increased network security, it is still necessary for hosts to take care of their own host-based security policies. Hosts in the Cold Room will be regularly scanned for vulnerabilities and those reports provided to the administrator(s) of the hosts.

All machines and hardware that will move into the Cold Room will need to be coordinated and scheduled with the Cold Room staff. As we grow the number of machines in the Cold Room, we will need to incrementally expand the infrastructure that supports the entire Cold Room. Sometimes this may mean a small delay in the deployment of hardware into the Cold Room until we have the appropriate infrastructure (including console, network, power, and rack space) for the hardware to be deployed

#### VIII. **Cold Room Equipment and Connection Provisioning**

All physical changes to equipment or connections in the Cold Room will be completed by the Telecom Facilities Staff at UCAT. NO ONE ELSE IS AUTHORIZED TO MAKE ANY PHYSICAL CHANGES IN THE COLD ROOM. Requests for changes in the Cold Room can come via Change Request or Cold Room Request forms.

#### IX. **Security Policies**

The Cold Room is a consolidated server room intended to provide a 24x7 high availability, redundant, and secure environment for those San Jose State machines which need a higher level of security than the rest of the San Jose State network can provide. Intended uses include meeting HIPAA requirements for servers, meeting California code requirements for privacy, as well as other servers that need high availability and increased security. The Cold Room design is intended to enable either the Cold Room systems administration staff, or the systems administrators of the servers housed in the Cold Room to be able to effectively manage their machines remotely and securely.

##### **Physical Access**

The Cold Room is intended as a limited physical access location for servers to reside . There will be remote network access to the servers via VPN for system administration access, and for other user access (researchers or programmers for example). Systems Administrators of machines which are housed in the Cold Room will have access to tools to assist in

the remote administration of their servers, however they should plan their servers as if they will only get physical access to them when it is necessary to perform hardware modifications or replacements. With this in mind, it is highly recommended that all servers be configured with administrative tools such as ssh servers, or Windows Terminal Services, in order to allow systems administrators to remotely maintain their servers. If you are unsure if you have these sorts of things set up for a server, a good test is to unplug the monitor or serial console (if either are present) and see if you can do all of your administration without needing to reconnect them.

