SDSC Data Center Reference Guide

I. PURPOSE:

The purpose of this document is to serve as reference material for campus personnel and customers participating in co-location at the San Diego Supercomputer Center. Revisions to this document will be made as necessary to maintain its accuracy.

II. TECHNICAL STANDARDS:

SDSC Data Center Attributes:

- 19,000 sq. ft. of space
- 4 Megawatts of current datacenter power, with total on-site capacity of 13 Megawatts
    - 208V distribution currently available (30 Amp standard up to 100 Amp available per circuit)

Equipment Racks:

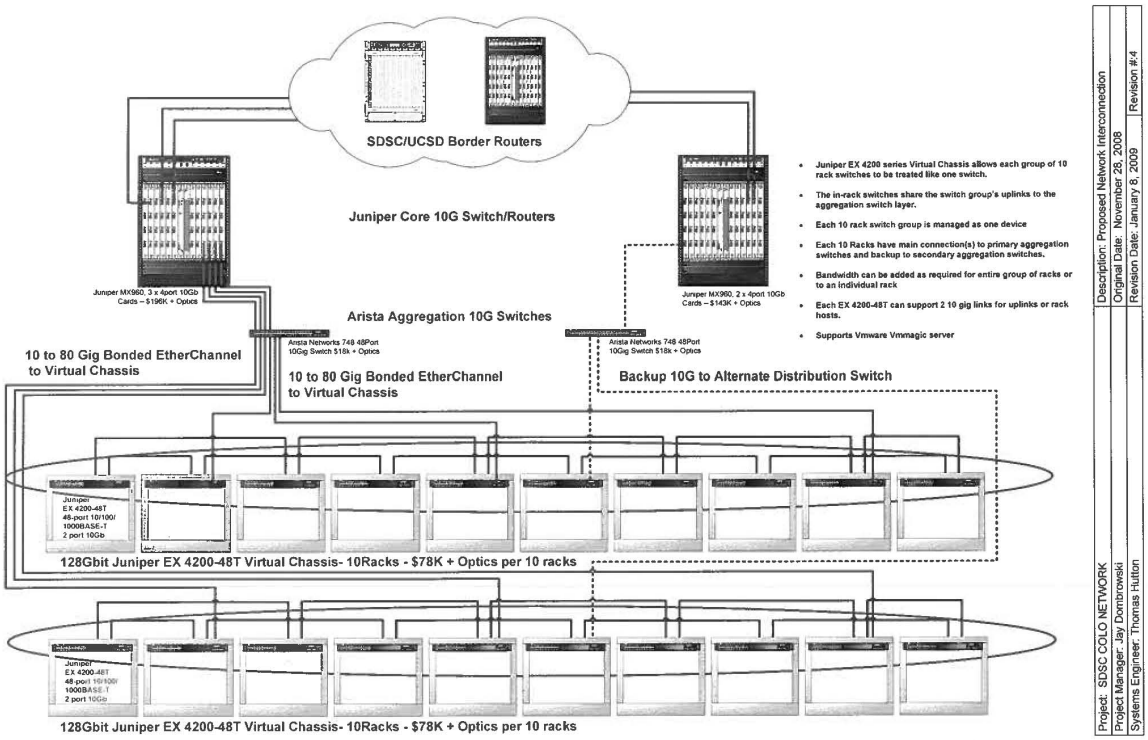
The racks to be used and provided in the SDSC datacenters are APC AR3300s in the West Datacenter and Liebert/Knurr Miracel 600mm width, 1200mm depth, 41U racks in the East Datacenter. All racks are labeled front and rear at the top with their data center coordinates. The racks will include overhead cable troughs and thermal containment systems.

- http://www.apc.com/resource/inhttp://www.apc.com/resource/include/techspec_index.cfm?base_sku=AR3300clude/techspec_index.cfm?base_sku=AR3100
- http://www.knuerr.com/web/zip-pdf/en/IT-Special-Catalog/IT-Special-Catalog-Miracel.pdf

Networking:

The design of the SDSC colocation network fabric provides a stable, flexible infrastructure that has high performance and reliability. All backbone trunks currently utilize 10g links, in some cases using more than one bonded together for increased throughput. The Layer 2/3 colo fabric will include Juniper core and Arista aggregation switches. The design will support thousands of 1G ports and hundreds of 10g ports with hundreds of vlans available. Vlans will conveniently allow a virtual space in the network devoted to a customer's IP address space. Customers may require local data and management vlans assigned to a customer going to the same or different racks. This will allow several different options depending how a customer wants to use their rack space.

Below is the agreed upon SDSC network infrastructure to support scalable colocation:



Here are examples of common connectivity configurations:

- NGN connectivity (for UCSD customers):
    - Based on NGN coverage some or all of the customer's connectivity will be provided free of charge. This is reviewed on a case-by-case basis.
- In-rack switches:
    - Prior to any customer network device (e.g. switch, firewall, etc.) being installed in the data centers, SDSC networking staff must review and approve the configuration(s). Configuring network devices to meet SDSC networking standards is usually provided free of charge.
    - SDSC can purchase an already approved switch (currently Juniper EX4200) on behalf of the customer. The switch is recharged to the campus up-front with an annual maintenance cost charged for maintenance and the depreciation of the upstream fabric. Switches can be connected to the network with any number of 1Gb or 10Gb connections. These ports are leased on an annual basis, recouping the depreciation costs of their share of the upstream fabric.
    - Hosts are connected to one or two 1G copper ports or to a 10Gb port on the in-rack switch.
- 10Gb links:
    - SDSC typically uses SFP+ optics and SR fiber optic cable.
    - For higher-bandwidth needs or other special circumstances 10Gb links can be provided.
    - These 10Gb ports are leased on an annual basis, recouping the depreciation costs of their share of the upstream fabric.

- 1Gb and 10Gb links directly into the core switch fabric:
    - These ports are leased on an annual basis, recouping the depreciation costs of their share of the upstream fabric.
    - These connections minimize the number of hops within the SDSC network fabric.
- Direct fiber connections to other providers:
    - SDSC is home to the San Diego Network Access Point (SDNAP) providing flexible and cost effective connectivity to a number of member networks. These include but are not limited to Internet2, ESnet, NLR, and others. Please visit the SDNAP site for further information: http://www.sdsc.edu/sdnap/

Special configurations are available on a case-by-case basis as agreed to by SDSC, UCSD networking representatives, and/or the customer(s). These might include the capability for customers to have unique BGP peer point(s), dedicated 10G L2/L3 path(s) to CENIC, or other WAN configurations.

If using SDSC address space, IP addressing is managed by SDSC's network group. Each campus would be provided subnets and VLANs as needed to support their networking needs, with the allocated amount of IPs charged for at current rates. DNS services within SDSC's address space are included in the per-IP costs. In some (but not all) cases, DNS services may be able to be delegated to the participating campus. Alternately, campus-delegated address space would be completely managed by the participating campus and not incur any per-IP costs.

Additional services include:

- Time supplied by SDSC servers.
- SNMP stats on a colocation web server of VLAN usage or port usage at the head switch in a rack.
- Performance testing NDT servers online for local or remote testing of bandwidth.
- Troubleshooting/configurations assistance at current hourly rates.

Prohibited activities include:

- NAT IP addressing for data access (VPN access is permitted).
- Span or mirror ports in the fabric switches without coordination with SDSC networking staff.
- Excessive performance testing through fabric.

Rack Power:

- SDSC will provide two NEMA L6-30, 30 amp, single phase, 208v power connections to all standard racks. If additional power is required, alternate arrangements should be made with SDSC. Time and materials cost between standard and non-standard configuration is passed on to the customer in the first billing cycle.
- Conditioned power could be available but is not guaranteed.

Seismic Protection:

- All equipment (i.e. racks, mainframes, clusters, etc.) placed in the SDSC Data Center will need to be installed on top of Iso-Base seismic platforms. This is an additional level of protection in the event of an earthquake or other major catastrophe.
    - http://www.worksafetech.com/pages/isobase.html

Aisle Containment:

- SDSC utilizes aisle containment to maximize life and efficiency of data center equipment. Equipment hosted at the SDSC data center must have an airflow orientation from front to back. Exceptions will be made on a case-by-case basis.

III. DATA CENTER INFRASTRUCTURE:

HVAC:

- West Data Center:
    - The San Diego Supercomputer Center utilizes Liebert air handling units for data center cooling. In the West data center (WDC) there are multiple 30 and 40 ton cooling units placed throughout the room to deliver conditioned air. Delivery of air is through adjustable perforated floor tiles inserted in the 2 foot raised floor. The ceiling above acts as the return plenum, sending the exhausted hot air back to the CRAH (computer room air handling) units. The CRAH units receive water by the UCSD central pump station through a chilled water loop. If pump station service is interrupted, a local chilled water loop at SDSC can supply supplemental cooling during the outage. The controls are adaptively controlled by an Opto22 system that is monitored in real-time in the SDSC NOC.
- East Data Center:
    - The air handling units are installed one level below the data center and are ducted into the supply plenum. The return plenum is above the ceiling like the WDC. The temperature is controlled by Johnson Controls Metasys system and monitored in real-time inside the SDSC NOC.

Fire Suppression:

- Detection:
    - The detection system is a combination of in room and under floor particle detection devices.
- Water Suppression:
    - Like most building facilities the SDSC data center is equipped with a wet fire extinction system. It is a “dry” system, meaning the pipes are not filled with water until initial particle detection. It takes a minimum of two separate detections to energize this system. Actual discharge will take place if the wicks located at the nozzles reach a critical temperature.

    - A false positive can occur if one of the nozzles recessed in the ceiling is damaged or tampered with. This will fill the system with water but not lead to a discharge. Safety guidelines should be followed all times in the SDSC data center.
- West Data Center Clean Agent (Halon):
    - The detectors are similar to the ones used in the water system however they are underneath the floor. The particle detection underneath the floor is possible because the particulates would be cycled through the room by the CRAC units. Two detections are required to discharge the system.
    - There is an abort button physically located in the Data Center that can prevent discharge if pressed before the second detection.
- East Data Center HFC-125 (FM-200 Clean Agent type):
    - Detection devices are mounted to the ceiling and inside the aisle containment but not underneath the floor. All other operations of this system are similar to the Halon system. Like the Halon system, there is an abort button located near the main entrance to the Data Center next to the EPO button.
- Once the fire suppression system energizes (either water or Halon), the room will EPO (emergency power off) all equipment except for the lights (for safety purposes). There are 6 EPO buttons (4 in the WDC and 2 more in the EDC) can also be manually pushed in the event of an emergency.

Power & Electricity:

- Utility Supply:
    - SDSC currently has two utility feeders that supply electricity to the building and data centers. With the completion of a current electrical upgrade, these systems total ~13,000 kW.
- Distribution:
    - SDSC has multiple transformers and power distribution units (PDU) that will supply 10+ MW of power to the data centers. Distribution voltages range from 110 to 480.
- Uninterruptable Power Supply (UPS):
    - The data centers have a combination of MGE and Mitsubishi UPS systems. These UPS' primarily keep core infrastructure and critical systems running in the event of a power compromise or loss. Critical systems include but are not limited to the SDSC NOC, mechanical systems, core networking equipment, and the San Diego Network Access Point (SDNAP).
- Generator & Catastrophe Support:
    - There are two generators that supply the data centers with emergency power. One of the generators supports only the SDNAP. A 2 MW unit is shared with a nearby facility but does supply substantial energy to the data centers. Both of these generators run on diesel fuel and are checked by UCSD Facilities Management regularly for proper operation and condition.

- UCSD operates a large natural gas powered cogeneration plant as well as other energy generative and storage systems. This Smart Microgrid can provide near normal campus operation in the event of commercial utility loss.

Security:

- Physical Access:
  - CCTV Security Camera System:
    - SDSC currently has security cameras focused on all entry and exit points of the data centers. The security camera infrastructure extends beyond the data centers to hallways, public spaces, and the physical exterior of the host building.
    - The recorded footage is stored digitally, securely, and retained for a minimum of 60 days. If event footage needs review, it is readily available in the NOC with the assistance of SDSC personnel.
  - Physical Access to the building and data centers can be segregated through the use of the biometric access system. The Identiscan system utilizes a unique PIN and hand vascular pattern for identity verification.
  - During normal business hours of 8am to 5pm PDT, SDSC's lobby doors are unlocked and open. Outside of these times, the doors are locked and require biometric access or an alternative method to enter. The data centers require identity verification 24x7x365.
  - If a person attempting to enter SDSC is not enrolled in the biometric system, there are call boxes located outside of the lobby and the loading dock. These phones call directly to the SDSC NOC, where on duty operator(s) are responsible for verifying and authorizing access.
  - Enrollment for SDSC / Data Center Access:
    - By default, all technical points of contact (TPOC) specified on each SLA will be enrolled in the Identiscan system and considered by SDSC authorized representatives of the customer/campus.
    - The enrollment process requires the individual to be physically present at the SDSC NOC. Photo identification will be required to enroll.
    - Authorization by the customer:
      - Prior to the individual(s) arriving at the SDSC data centers, the customer should authorize access through one of these channels:
        - An email sent to operator@sdsc.edu with the customer name, contact information, the name of the individual(s) to allow entry, and any special instructions to SDSC NOC staff (e.g. certain hours of access, etc.).
        - Call the SDSC NOC at 858.534.5090 to verbally authorize the individual(s). The passcode chosen during the SLA will need to be referenced by the customer. These are accessible in the SDSC NOC indefinitely for verification purposes.

        - During the enrollment process the following information is collected: full name, employee or identification number, and any specific access directions or limitations.
        - To complete the registration process, the enrollee uses either hand for vascular recognition and creates a unique PIN of 4-8 numbers.
    - If the biometric access system is offline use of a call box is required to gain entry to the data centers.
    - Access to the SDSC facility without biometric enrollment:
        - This is primarily intended for non-revisiting contractors or special staff needed in the event of an outage.
            - SDSC NOC staff will provide manual entry. The individual(s) requesting access will be required to show photo identification and to sign-in on the SDSC data center access log, located just outside the SDSC NOC.
- System and Network:
    - SDSC's network and security practices are managed by SDSC staff under a different security model than the rest of UCSD. Tools such as Foundstone, for detecting system vulnerabilities, network monitoring and intrusion detection/prevention are utilized. General practices do span across both SDSC and UCSD but are not identical.
    - System security is the responsibility of the customer unless otherwise specified in the appropriate SLA. (E.g. The system is managed by SDSC for an additional fee)
    - To ensure the availability, security and integrity of SDSC data centers, systems located in the data centers are subject to network security monitoring by SDSC security personnel.
    - SDSC will scan the network for vulnerable and/or compromised systems on a regular basis. SDSC maintains control of scheduling and depth of the scan.
    - There are two clear security incident scenarios:
        - Suspected Vulnerability: If the results from an SDSC scan show vulnerabilities exist on a host, the campus technical point of contact will be emailed with detailed information including:
            - Detection date
            - Vulnerability type
            - Report information generated by the scan.
            - If remediation of a vulnerability that could lead to a compromise is not detected by the next scheduled scan, the host(s) may be disconnected from the network.
        - Suspected Compromise: If a system compromise is suspected, SDSC reserves the right to disconnect the system from the network to prevent further communal infection. At this time, an email notification will be sent to the contacts specified in the SLA with the following information:
            - Time of disconnect
            - A report of affected system(s) including which vulnerabilities were detected.

        - The Footprints ticket number associated with the incident.
        - To protect other systems and the network, SDSC may request from the technical POC that a forensic image of the system be created for further analysis. All personal and private data will be kept confidential.
    - It is the campus technical point of contact's responsibility to coordinate all activities with their campus end users of the colo. SDSC personnel will create a Footprints ticket to track the process of remediation and communication with each campus. The campus technical point of contact will be responsible for ensuring issues are remediated and any tickets are communicated as closed to SDSC.
- Systems containing restricted data (HIPAA, FISMA, FERPA, etc.) will need identification prior to installation at SDSC. There are additional physical security requirements for these systems.
- For more information regarding specific policies, please contact SDSC's Chief Security Officer.

IV. SERVER & EQUIPMENT MANAGEMENT:

Shipping & Receiving:

- SDSC's loading dock can accommodate all vehicles including a standard commercial semi-truck. A call box mounted on the North wall calls directly to the SDSC NOC.
- SDSC does not offer pallet or packing services for equipment. If SDSC personnel are requested or required to perform this service, the customer will pay time and materials.
- Incoming:
    - When a customer ships equipment to SDSC, it is their responsibility to arrange shipment with the carrier.
    - Once tracking information has been received, it should be emailed to SDSC (operator@sdsc.edu) or the existing Footprints ticket should be updated with the following information:
        - Customer name
        - Campus or organization name
        - Name of carrier
        - Number of packages
        - Tracking numbers for all containers
    - Upon delivery SDSC will inventory and assess the condition of the shipping containers. In the event of damage or missing items, SDSC will decline the delivery or attempt to contact the customer for further instruction.
    - If the shipment is complete and integrity verified, SDSC will accept the containers and move them into temporary storage. Currently none of SDSC's storage spaces are environmentally controlled.
    - SDSC will not be held liable for any damaged or missing items during shipping.
- Outgoing:

- When equipment is scheduled to leave SDSC, it is the responsibility of the customer to make all carrier arrangements. It is also the responsibility of the customer to pack the equipment for shipment adhering to SDSC data center policies and safety rules.
- Once the pickup is scheduled, the customer will email SDSC (operator@sdsc.edu) or update the appropriate Footprints ticket with the following information:
  - Customer name
  - Campus or organization name
  - Name of carrier
  - Number of packages
  - Tracking numbers for all containers
- After the shipment leaves SDSC, a confirmation email will be sent to the customer and TPOC specified on the corresponding SLA.

Commissioning Equipment:

- In accordance with the current SDSC data center policy, packing materials are not permitted inside the data centers. Therefore all unpacking and assembly of equipment must take place in a designated storage or build area. The customer will be responsible for the disposal of all packing materials.
- Prior to the installation of equipment in SDSC data centers, the following information will need to be sent to SDSC (operator@sdsc.edu) or the appropriate Footprints ticket updated with:
  - Date(s) of installation
  - Equipment list if different from the one provided with the SLA.
  - Any additional networking needs.
  - Any additional materials needed for the installation (e.g. cabling, etc.).
  - Any work specifications to be contracted to SDSC to complete installation.
- Equipment being commissioned in SDSC data centers will be entered into an asset management system. SDSC may affix labels to the front and rear of any equipment.
- Iso-base seismic platforms will be ordered and installed prior to customer equipment installation.

Decommissioning Equipment:

- Prior to the decommissioning equipment, the customer must contact SDSC (operator@sdsc.edu) or update the appropriate Footprints ticket with the following information:
  - Date(s) of planned decommissioning (SDSC will need to be notified of any change)
  - Equipment being removed (by either rack unit, rack location, or system name)
  - Name(s) of authorized personnel performing the work on behalf of the customer
- When the equipment is removed from the data centers it will be removed from the SDSC inventory system.
- All SDSC provided cabling should be returned to the SDSC NOC at this time.
- All packing of equipment must take place outside of SDSC data centers in accordance with approved data center policies. SDSC will provide the service equipment including dollies,

ladders, carts, and hand tools to properly dismount or disconnect all equipment. Packing of equipment can take place in designated build or storage locations. Once the customer begins removing equipment from the data centers, SDSC will no longer be responsible for the equipment condition or integrity.

Cabling:

- Cable management arms are not required. However tidy cabling practices must be followed at all times.
- All cables will be labeled with the following information:
    - Network cable: Rack Coordinate / hostname / Footprints ticket number (e.g. G133 – yoda – FP#00001)
- All SDSC cabling will need to be returned during the decommissioning process. The customer will be responsible for any cost in replacing lost or damaged cables.
- SDSC NOC staff will inspect customer cabling at the time of installation. In the event that installation does not meet SDSC standards, cabling will need reinstallation or rerouting. SDSC NOC staff for an additional fee can perform this work.
- Periodic inspections will take place by SDSC NOC staff to ensure proper cabling practices. In the event of non-compliance, the technical point of contact will be contacted via email and the SDSC master Footprints ticket updated with remediation requirements.

Equipment Mounting in Racks:

- Customer shall provide all rails for mounting equipment.
- For equipment that doesn't have rail mounts shelves can be purchased for an additional onetime charge either directly or through SDSC. Each shelf supports ~250 lbs.

OS Installation & Maintenance:

- SDSC does not include operating system installation and maintenance in the standard colocation service. Additional OS maintenance services are available (refer to the **SLA** for additional service specifications).

V. OPERATIONS, MONITORING, & SUPPORT

Hours & Contact Information:

- SDSC Operations: 24x7, 365 days a year
    - Contact: operations@sdsc.edu or call 858.534.5090
- SDSC Business hours:
    - Monday-Friday: 8am-5pm PDT.
    - Saturday-Sunday: closed.
- Department Contact:
    Matt Campbell

Data Center Services Manager
mattc@sdsc.edu
ph: 858.361.8343

Support:

- SDSC NOC staff will provide remote support specified in the **SLA** (if applicable).
- Common request methods include:
    - Via telephone. SDSC NOC staff activity will need the pass code defined in the **SLA** before work begins. If the pass code is not correct, the request will be denied.
    - Via the master Footprints ticket. No passcode required.
- All Footprints tickets will be kept for auditing and review purposes.
- If no SDSC remote hands service has been established, all requests will be denied.

Notifications & Outages:

- Planned maintenance (performed by SDSC): 2-week average announcement prior to work being performed.
    - All attempts made to perform outside of normal business hours (see above).
- Unplanned outage or emergency: SDSC and its partners will make every effort to return equipment or facility to normal service as quickly as possible. An email notification will be sent to customers as appropriate.
- All notices are currently sent to colonotice@sdsc.edu.
    - Subscription to this mail list is mandatory for all technical points of contact (TPOC) specified in the SLA. It is the responsibility of the customer to keep this information up to date by notifying SDSC of any personnel changes through the master Footprints ticket.
- SDSC maintains an external site and mail list in case internal network communication is interrupted.
    - The site for status and maintenance updates is: http://status.sdsc.edu. Visit this site for instructions on how to subscribe to the external mail list.
    - Subscription to the external mail list is optional but recommended. If your primary email address resides at UCSD, it is recommended that you subscribe an external address such as Gmail.

Monitoring:

- Real time monitors:
    - *Network:* Systems monitor not only many of SDSC's internal systems and connections, but the main links to the UCSD campus and main uplinks to CENIC, ESNet, etc.
    - *Systems and Network Security:* The SDSC Security team utilizes security monitoring tools to protect against, track, and report system compromises and attempted attacks. These

tools also permit the Security Staff to notify a campus's technical point of contact in the event a system is potentially compromised.

- *Building Security:* The CCTV security camera systems are monitored 24x7x365 in the NOC.
- *Facilities:* Automated building monitors for the host building as well as the data centers alert NOC personnel and UCSD Facilities Management of any failure. NOC staff also performs multiple physical inspections daily to maintain facility integrity.
- *UPS:* SDSC UPS systems undergo multiple checks daily. SDSC NOC personnel are immediately notified visually and audibly if there is an integrity failure. At that time replacement parts or service is scheduled through maintenance contracts.
- *Temperature, Pressure, and Humidity:* Multiple probes and sensors exist in the data centers. If a parameter is exceeded, NOC staff is immediately notified.

Service Definitions:

- *System Administration:* SDSC System Administration is available on an hourly or subscription basis. It includes application and software maintenance during SDSC's normal maintenance cycle. This maintenance is performed once a month at a specific time unless a critical vulnerability is discovered. Refer to the *Notification* section for SDSC announcement procedures.
- *Security Services:* The SDSC Security team is available on an hourly basis to support all areas of system security, including OS hardening, Intrusion Detection System, firewall configuration, antivirus, auditing, intrusion protection, forensics, and penetration testing and system lockdown.
- *Backup Services:* SDSC has a number of backup options in place to suit different levels of need. CommVault is used for most Windows, Linux, and SQL backup needs. The system writes to a disk cache and is then stored on tape. Retention periods are configurable based on campus requirements.
- *Out-of-band remote access:* SDSC does not provide any out-of-band access at this time. Customer furnished if needed.
- *Assisted Installation and Remote Hands:* SDSC Operations staff assistance is available. SDSC staff is experienced in installing systems and networking equipment, including rack mounting and cabling. Customers should inquire regarding additional expertise and assistance.

VI. SAFETY & CONDUCT:

- Refer to **SDSC Data Center Rules**.

VII. BILLING:

Billing Cycle:

- SDSC's standard billing cycle for colocation is quarterly based on the university's fiscal year. Alternate arrangements available as well.

Sample Invoice:

- Below is a sample invoice. Each service will have its own 'recharge type.' For example if you purchase a rack and a 1gb network connection this would show on the ledger as two line items.

Recharge Statement for Colocation Services

Index Number: RCICOLN UCSD UNDER PAYMENT FOR COLO
Fund-Orgn-Prog: 62111A-436268-434030
Ledger Date: 201203

Ledger Date	Sale Date	Index	Buyer	Recharge Type	Description	Quantity	Unit Cost
201203	01/31/2012	RCICOLN	EDSALL, LEE	RACK SPACE	O10 - RenLab/UCSD - Ren	-0.30	535.33
201203	02/29/2012	RCICOLN	EDSALL, LEE	RACK SPACE	O10 - RenLab/UCSD - Ren	-0.30	535.33
201203	02/29/2012	RCICOLN	PAESANI, FRANCESCO	RACK SPACE	J122 - UCSD/Chem - Paesani	0.07	535.33
201203	03/30/2012	RCICOLN	ORTEGA, HUMBERTO	RACK SPACE	R113 - UCSD/Psych - Ortega	0.07	535.33