UC SANTA BARBARA

UCSB Information Technology
Enterprise Technology Services
4101 SAASB
Santa Barbara, CA 93106-3020
it.ucsb.edu

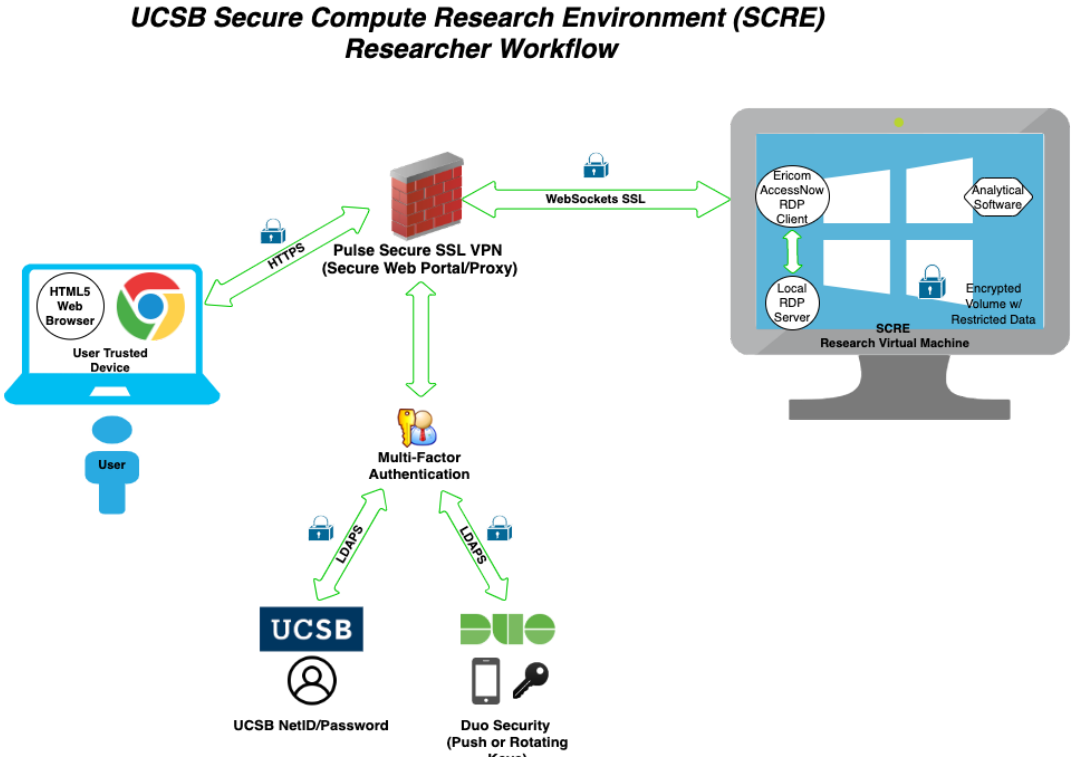
Secure Compute Research Environment

System Security Plan (SSP) - v.2.0 - November 2020

Overview

The Secure Compute Research Environment (SCRE) is a private, secured virtual enclave environment designed for University of California, Santa Barbara (UCSB) researchers to securely store, access and analyze restricted data in a remote desktop session, without storing data on local computers.

The user experience is similar to a Remote Desktop session, but additional significant security controls are in place around and within the environment, while still remaining simple and straightforward for the researcher to use.



Access to the SCRE is protected by strong, multi-factor authentication, and can be accessed from any HTML5 web browser from multiple platforms (Mac, Windows, Linux, tablets etc.) Industry-standard security protocols are used for end-to-end encryption and encryption at rest. All network traffic is encrypted between the user desktop all the way to the research Virtual Machine (VM) guest. Restricted data resides on the research VM guest on a separate virtual disk image, also protected by strong encryption. All services and network access controls within the SCRE operate on the "minimum services, "minimum permissions" and "default deny" principles, with specific exceptions made in firewalls and access control lists to allow only for hosts/services needed for secure operation of the service.

The SCRE was designed using the "defense-in-depth" security principle, in which security controls are put in place at multiple layers of the environment. A checklist based on the Top 20 Critical Security Controls was created for initial deployment, and a routine review of this service and environment against NIST 800-171 rev1. The controls within the SCRE are intended to meet and exceed the data security plan requirements for the majority of secure data providers/agencies.

The remainder of this Data Security Plan will outline the security controls in place in the SCRE, and address specifically which objectives are met, and how.

I. Physical Access

The SCRE is hosted on dedicated servers on private, dedicated, secure non-routed networks.

The VM server host hardware, VPN hardware and network hardware are located in locked racks in the North Hall Data Center (NHDC) in room 1201A of North Hall on the UCSB campus in Santa Barbara, California. The North Hall Data Center is staffed during standard university business hours (5 days a week, 8am-5pm) and alarmed/monitored 24 hours/day, 7 days/week.

UCSB Personnel accessing the NHDC must present a UCSB-issued Access Control/ID KeyCard and must have explicit authorization for access to the NHDC. Access Control/ID KeyCards are managed by the facilities management department. The NHDC has video surveillance systems that record all activity in NHDC. Any visitors to the NHDC are logged and escorted by authorized personnel and are given only minimum privileges to the physical areas required.

II. Host Security

Each SCRE administrative function is assigned a unique and dedicated VM guest image on a VM server. These VM guests in the SCRE (DNS, DHCP, RADIUS, Logging, Proxy, Licensing Server, Monitoring Server, File Transfer Gateway) were built from known good media and

"hardened" from the CIS Benchmarks for the OS. Only necessary services are installed, running and listening on each system.

A FireEye Endpoint Security agent is installed on all SCRE administrative VM host servers and guests to provide anti-malware protection and endpoint detection and response. A baseline configuration has been developed, documented and maintained for each administrative VM guest, including information about software versions and patch levels, configuration parameters, and network interconnection/topology.

SCRE Administrators are assigned regular accounts on the SCRE administrative VM host and guest servers, and have the ability to change to privileged mode in order to install and update software or change system configurations. Administrative accounts are not used on a routine basis to login.

Each researcher and enrolled research project is assigned a unique and dedicated VM guest image on a VM server, referred to in customer communication as a "SCRE Research Virtual Desktop." Each SCRE Research Virtual Desktop has an up-to-date Windows 10 Enterprise operating system installed with a package of standard research software. Each SCRE Research Virtual Desktop is built from known good media and "hardened"from the CIS Benchmarks for the OS - only necessary services are installed, running and listening on each VM guest.

A FireEye Endpoint Security agent is installed on all SCRE Research Virtual Desktops to provide anti-malware protection and endpoint detection and response. A baseline configuration has been developed, documented and maintained for the SCRE Research Virtual Desktop "golden image," including information about software versions and patch levels, configuration parameters, and network interconnection/topology.

Enrolled researchers are assigned a standard (non-administrative) account on a dedicated SCRE Research Virtual Desktop with a unique strong password (14 characters: mixture of numbers, lowercase, uppercase letters and special characters, no dictionary words). Passwords may not be reused within the SCRE. Researchers can not install software or modify the VM guest system in any way. No mobile code technologies (Java, Flash etc.) are in use on any of the SCRE Virtual Research Desktops. Application "permit-by-exception" is in place on SCRE Research Virtual Desktops so that only pre-authorized software may run on the system, using Windows AppLocker. This list is reviewed annually by SCRE Administrators, or on an as-needed basis when new software is installed/updated on VM guests.

III. Network Security

- All systems within the SCRE have network interfaces connected to only the necessary networks, and services are limited to running only the appropriate network interface(s).

- All systems within the SCRE have host-based firewalls installed, running in default deny mode, with specific inbound/outbound exceptions made for below-defined services/protocols required for operation of the SCRE.
- Firewall security policies are in place on Palo Alto Firewalls which apply to all network segments that communicate with the public Internet, in default deny mode, with specific inbound/outbound exceptions made for below-defined services/protocols required for operation of the SCRE. These policies also apply Palo Alto Networks' threat prevention (Intrusion Prevention Services/IPS) to all systems on these networks.

There are 5 segmented networks within the SCRE, differentiated by traffic type and scope:

- Private non-routable Networks (2)
    - Admin VM Guests – Internal Services (Authentication, DNS, DHCP, Proxy, HIDS, Logging, Proxy)
    - End-User VM Guests - SCRE Research Virtual Desktops (RDP, Software License Checkout, Proxy)
- Public Internet routed Networks (3)
    - VM Host Lights-Out Management - filtered by firewall policy:
        - Default inbound and outbound deny
        - Permit inbound from SCRE Administrator subnet only
            - Lights-out Management: IPMI
    - VM Host and VPN Management – filtered by firewall policy:
        - Default inbound and outbound deny
        - Permit inbound from SCRE Administrators subnet only
            - Management services: HTTPS, SSH
    - Admin Hosts – filtered by firewall policy:
        - Default inbound and outbound deny
        - Permit inbound from SCRE Administrators subnet only
            - Management services: HTTPS, SSH
        - Permit outbound to defined services/protocols to trusted hosts/networks:
            - Campus services: DNS, NTP, LDAPS (primary authentication), SMTP (HIDS and daily logwatch notifications)
            - External Service Providers: HTTP proxy to whitelisted trusted software update providers, LDAPS to Duo Security for MFA

"SCRE Research Virtual Desktop" VM guests, which sit on a private, non-routable network segment, do not have direct access to the public Internet. VM guest firewalls allow specific exceptions only for the following services to and from specific hosts on the 2 private SCRE network segments:

- Inbound
    - IP address assignment from DHCP server to VM Guest
    - Ericom AccessNow and RDP services running on VM Guest (provides clientless RDP view session in HTML5 web browser) from VPN Proxy

- Outbound
    - IP address assignment from DHCP server to VM Guest
    - Name resolution to local DNS server
    - License checkout with SCRE license server (research software)
    - HTTP Proxy server (provides limited access outbound to obtain authorized and whitelisted operating system, application and anti-malware updates to VM Guest)
    - Secure logging over TLS from VM Guest to SCRE syslog server
    - Host Intrusion Detection System (HIDS) logs to local HIDS server

IV. Network Access Controls

Researcher/End-User authentication/authorization

Researcher access to the SCRE is controlled by a dedicated VPN web portal which allows remote access from any device running an HTML5 browser on the public internet. Portal access is protected by multi-factor authentication. The research must complete all of these authentication methods to login to the web portal:

- Local RADIUS server – username must be defined as enrolled SCRE user (authorization)
- UCSBNetID and password (campus Identity service) authentication
- Duo Security multi-factor authentication (Duo Mobile App Push, Duo codes, hardware token or SMS codes)

Remote Desktop access (Ericom AccessNow/RDP) to the SCRE Research Virtual Desktops on the private network is restricted to authenticated connections originating from the VPN web portal/proxy only. The RADIUS server assigns unique access controls to each user's VPN session to permit Ericom AccessNow RDP communication only between an authenticated user and their assigned/dedicated SCRE Research Virtual Desktop(s). VPN access control lists permit communication only between authenticated users and their dedicated/assigned SCRE Research Virtual Desktop(s). Firewall policies restrict outbound communication from the VPN web portal/proxy to necessary services - domain name service (DNS) and network time protocol (NTP) - on the campus network, and to Duo Security over HTTPS (for multi-factor authentication) on the public Internet.

The following controls have been enabled to limit the potential for unauthorized access during remote access sessions:

- Custom Login Warning Text displayed upon Windows session login – "restricted data"
- Windows Screensaver on Guest VM – 3 minute timeout
- Ericom AccessNow/RDP Remote Desktop session timeout – 25 minutes
- VPN web portal session timeout - 30 minutes
- VPN web portal lockout - 3 unsuccessful in 60 seconds, 2 min lockout

Admin Management authentication/authorization

Management access to SCRE Admin systems is controlled by unique username/strong passwords:

- IPMI over HTTPS (Lights Out Management of VM host servers)
- SSH (Admin VM host servers, VM guests and VPN)
    - Also protected with Duo Security MFA
- HTTPS servers: VPN management, log analysis/management
    - Also protected with Duo Security MFA

V. Encryption in Transit

Researcher/End-User Traffic

- Login to VPN web portal and to File Transfer Gateway:
    - Authentication/Authorization traffic to/from local RADIUS server occurs on private network segment
    - Authentication traffic to/from campus LDAP server is encrypted using TLS using public key infrastructure (PKI) with a 256-bit RSA certificate issued by InCommon Server CA
    - Authentication traffic to/from Duo Security service over LDAPS and HTTPS is encrypted using TLS using PKI with a 256-bit RSA certificate issued by InCommon Server CA

- Remote Desktop activity:
    - HTTP traffic between the end-user's remote web browser and the SCRE VPN portal is encrypted using TLS using using PKI with a 256-bit RSA certificate issued by InCommon Server CA
    - From the SCRE VPN portal, proxied WebSockets/HTML5 access is encrypted using TLS, using PKI with a wildcard 256-bit RSA certificate issued by InCommon Server CA to the Ericom AccessNow server on the SCRE Research Virtual Desktop, which connects to RDP locally listening on the SCRE Research Virtual Desktop

Admin Management Traffic

- IPMI host management – HTTPS traffic is encrypted using TLS using PKI with a 256-bit RSA certificate issued by InCommon Server CA
- SSH host management – encrypted using 256-bit RSA keys
- HTTPS management – (VPN and log management) – TLS using PKI with a 256-bit RSA certificate issued by InCommon Server CA
- Log traffic to log server – signed and trusted 256-bit RSA keys from self-signed CA
- HIDS agent to server – encrypted using agent encryption/authentication keys and sent over private network segment

Encryption Key Management

All public/private keys used for encryption in SCRE are issued by InCommon CA (Sectigo). Private keys used on SCRE systems are archived in the UCSB Enterprise Technology Services (ETS) instance of Secret Server, where access controls restrict viewing of these keys to SCRE Administrators and is protected by multi-factor authentication (Duo Security).

VI. Encryption at Rest

Each SCRE Research Virtual Desktop is assigned a unique virtual hard drive (VHD) image containing a BitLocker password-protected fixed volume, encrypted with AES 256-bit cryptographic keys (no diffuser). *Restricted data and interim research data are stored on this encrypted volume.*

Each encrypted volume is assigned a unique, strong password (14 characters, mixture of numbers, lowercase, uppercase letters and special characters, no dictionary words), which must be provided when mounting the volume. Restricted data volume BitLocker passwords are not saved or escrowed in any fashion, and are the sole responsibility of the user/researcher. *At time of BitLocker encryption of the encrypted volume, no BitLocker recovery key is saved, printed or escrowed.* FIPS 140-2 validated cryptographic modules are installed, enabled and used on each SCRE Research Virtual Desktop via Group Policy Object (GPO). These controls provide FIPS 140-2, Level 1 compliance for any restricted data stored on the encrypted volume.

User system variables are set so that all application temporary/scratch files are also stored on this encrypted volume. No restricted data shall be stored on unencrypted or system volumes at any time.

The VHD/BitLocker encrypted volume will automatically detach/re-lock upon the user's Windows session logout.

VII. Data Security/Integrity

After login to the VPN web portal, researchers are presented with unique bookmark links that provide access to only the researcher's dedicated VM guest. Upon Remote Desktop login to the VM Guest, researchers are presented with the following warning dialog:
"WARNING - You are attempting to access a computer system with restricted access data, operated by the University of California, Santa Barbara (UCSB). If you do not have the appropriate permissions, you should not proceed. Unauthorized use of these data is subject to

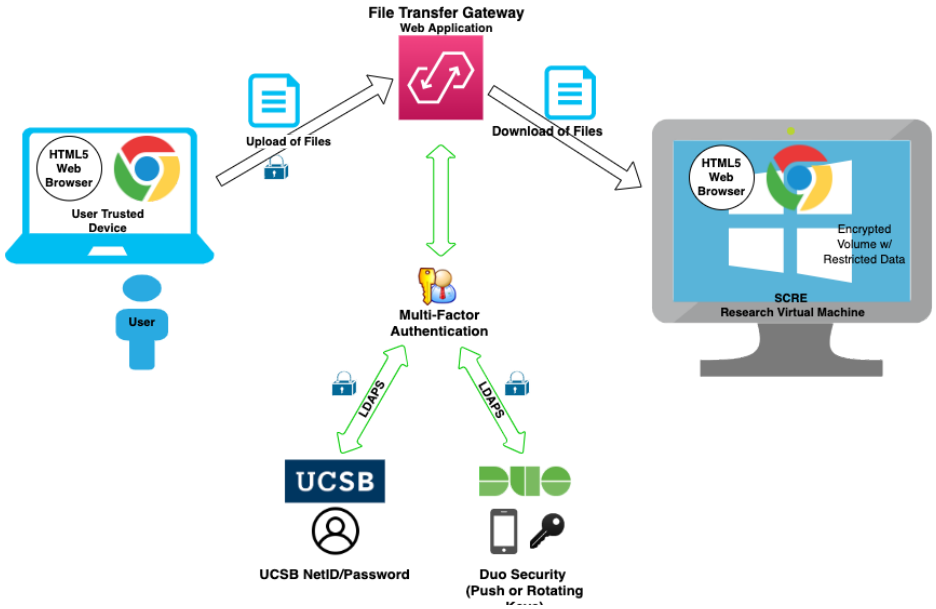
penalties imposed by UCSB and by the providers of the data. Unauthorized Access to Data (Individually Identifiable Information) on this Computer is a Violation of Federal Law and may Result in Prosecution. By continuing to use this system, you indicate your awareness of and consent to these terms and conditions of use. "

No removable media (USB flash drives, optical media) are accessible from the SCRE Research Virtual Desktop. Printing and copy/paste are also disabled on the SCRE Research Virtual Desktop. There is no access to outside Internet sites and no access to email providers from the VM Guest. An anti-malware program (FireEye Endpoint Security) is installed on each SCRE Research Virtual Desktop, and receives signature updates daily from a trusted source, through the HTTP proxy server.

The SCRE File Transfer Gateway is a custom internal web application (also protected by multi-factor authentication and end-to-end encryption) that provides a mechanism for researchers to securely transfer files into their SCRE Research Virtual Desktop for further analysis.

Files uploaded into the File Transfer Gateway are viewable only from a SCRE Research Virtual Desktop, and by the user that uploaded them. Files are scanned for malware upon upload and infected files are logged and discarded. Files that have not been downloaded from a user's directory on the File Transfer Gateway are automatically deleted when they reach 7 days age. All activity on the File Transfer Gateway is logged.

UCSB Secure Compute Research Environment (SCRE)
File Transfer Workflow



Where permitted by the restricted data provider, researchers may request the ability to export files from their SCRE Research Virtual Desktop using the secure File Transfer Gateway. In this situation, as well as at the end of any research project, a disclosure review by the PI on each file is required before any files are exported.

VIII. Credential Review/Access to Data

Only users who have signed the relevant contract documents from the restricted data provider are assigned accounts within the SCRE. The SCRE Administrators and the Chief Information Security Officer shall sign all appropriate license and non-disclosure documents.

SCRE Administrators perform initial secure intake of the restricted data set, labeling physical media with an assigned project ID number, date, and other identifying details. The SCRE Administrators then perform secure upload of data set from a trusted workstation to the SCRE File Transfer Gateway, from where the researcher can download it to their assigned SCRE Research Virtual Desktop.

After secure intake, all physical media associated with each restricted data set and project is stored in an individual tamper-evident envelope. This envelope is labelled with project name, date and a label to indicate restricted data, along with a chain of custody/access log. This envelope is placed inside a US GSA Class 6 multi-lock secure media storage cabinet, in the access-controlled (high security fenced) area of UCSB's North Hall Data Center (NHDC). Access requires a physical key to the access-controlled area and a combination to the assigned multi-lock drawer of the secure cabinet, in addition to the NHDC access controls already described in the Physical Access section of this document.

The restricted data provider or Principal Investigator of an enrolled research project may request termination of a user's access to the SCRE at any time. SCRE Administrators will terminate a user's access within 24 hours of notification by authorized personnel and will notify the Principal Investigator of such activity.

SCRE Administrators will maintain confidentiality of passwords for all accounts. Passwords will be changed by SCRE Administrators if they are suspected of having been, or are known to have been, disclosed. Devices enrolled in Duo Security for multi-factor authentication will have access revoked by SCRE Administrators if they are reported lost or stolen by the end-user. Inactive user accounts will be deactivated after 60 days of inactivity.

All active projects utilizing restricted data within the SCRE will be reviewed on an annual basis to ensure that the project is still active and that there are no personnel changes on the license that will require revocation of credentials.

Any stored temporary/scratch files in the encrypted volume in the Z:\USERTMP directory will be secure erased by a scheduled job running on the 1st of every month, using the Eraser program with US DoD 5220.22-ME standard.

At the scheduled end of a project, all VM Guest images on disk will be cryptographically erased by SCRE Administrators using the secure-delete Linux packages (srm) command, compliant with NIST SP 800-88 rev1 "Purge" methods. All physical media containing restricted data associated with the project will be returned or destroyed, per restricted data provider license agreement. Media will be destroyed in accordance with guidelines outlined in NIST SP 800-88 rev1 "Destroy" methods.

IX. Logging/Auditing

Audit logs of physical access to the NHDC (key card swipes) are kept by NHDC Administrators. Video recordings of physical activity in NHDC are retained by NHDC Administrators for 90 days.

All administrative and end-user/researcher systems within the SCRE have operating system and application level logging enabled, forwarded in real-time to the SCRE log server for central storage, monitoring and alerting. Log timestamps on all VM guests are synchronized from the VM host, which synchronizes time via Network Time Protocol (NTP) to the UCSB campus timeservers. SCRE system logs are only viewable by SCRE Administrators and are reviewed on a daily basis. Log delivery is being monitored and will alert SCRE Administrators in the case of a failure.

Host-based intrusion detection (HIDS) agents are installed on each administrative VM host and guest within the SCRE, to ensure integrity of the operating system, application software and configuration files. HIDS notifications are sent in real-time from the HIDS server to the SCRE log server as well as an email address reviewed on a daily basis by the SCRE Administrators.

Anti-malware scans are performed, by policy, after each new signature update is downloaded by the FireEye Endpoint Security agent.

Network and application vulnerability scans are performed on all SCRE networks and systems, and compared with baseline scan results to provide a report of listening services and application patch levels, on a monthly basis.

The UCSB Security Operations Center (SOC) monitors network traffic and threat logs for potential indicators of compromise of SCRE systems. The SOC responds to appropriate events to initiate the Incident Response plan as needed.

Network traffic and threat logs from the Palo Alto firewall protecting the SCRE are also forwarded in real-time to the SCRE log server for monitoring, alerting and reporting.

X. Updates/Maintenance

All systems (both administrative VM guests and end-user SCRE Research Virtual Desktops) are kept up-to-date with Operating System and Application updates/patches and anti-malware signature updates through the proxy. Admin and End-user research VM guests check for and install OS updates daily. Additionally, a monthly maintenance window is defined for any significant update activities that may require a service outage.

All maintenance and update activity in the SCRE is performed by or under direct supervision of the SCRE Administrators. Any maintenance activity that affects production-level services in the SCRE will go through UCSB ETS' Production Change Request (PCR/change control) system for relevant pre-approval before the changes are made. Any changes that significantly impact regulatory compliance or the security controls described in this document will go through PCR as well as approval by the CISO.

The UCSB Security Operations Center (SOC) subscribes to a variety of security advisory mailing lists. These advisories are monitored on a daily basis and communicated to SCRE Administrator for all relevant technologies, software and services that may be in use within the SCRE. Updates to critical and high vulnerabilities in Operating Systems and applications will receive highest priority for remediation.

XI. Backups/Disaster Recovery

Backups/snapshots of SCRE Admin VM guests and SCRE Research Virtual Desktops are performed on a weekly basis.

Where permitted by the restricted data provider, and requested by the researcher, backups of encrypted volumes (where restricted datasets are stored) are performed. Such backups are performed weekly, encrypted (the volumes are BitLocker encrypted) and stored in a physically secure location in NHDC. No off-site backup storage is permitted.

XII. Review/Assessment

An independent review and risk assessment of the Secure Compute Research Environment systems and network, and associated security controls, will be performed by University of California Audit and Advisory Services on an annual basis.

This document (SCRE System Security Plan) will be updated annually or on an as-needed basis.

XIII. Roles/Responsibilities/Personnel

Security Office - Policy

- Review and approval of System Security Plan document
- Sign-off, as required, on Restricted Data License applications
- UCSB Electronic Security and Policy

Samuel Horowitz
Chief Information Security Officer
University of California, Santa Barbara
803-893-5005
samh@ucsb.edu

IT Operations

- Systems and Network Architecture
- Systems and Network Administration
- Systems and Network Security
- Development and maintenance of System Security Plan document

Jennifer Mehl
Information Security Analyst
University of California, Santa Barbara
(805) 893-5080
jennifer.mehl@ucsb.edu

Data Center

- Maintains physical security/access control to SCRE servers & network hardware
- Maintains physical security of GSA Class 6 secure media storage cabinet

UC SANTA BARBARA

Chris Sneathen
Acting Director, ETS Infrastructure
University of California, Santa Barbara
(805) 893-5052
sneathen@ucsb.edu

University of California Police Department

SCRE Administrator / Data Custodian

- Manages intake of restricted dataset
- Manages physical security and acts as Custodian of restricted dataset
- Manages access and credentials to SCRE
- Creates and Provisions SCRE Research Virtual Desktops
- Communicates with Principal Investigator for credential and restricted dataset management
- Performs routine backups
- Performs regular log review and analysis

Jennifer Mehl
Information Security Analyst
University of California, Santa Barbara
(805) 893-5080
jennifer.mehl@ucsb.edu

Technical Support

- Provides limited technical support to end-users/researchers
- Provides limited technical support to departmental IT personnel
- Maintains SCRE end-user documentation on UCSB IT website

Jennifer Mehl
Information Security Analyst
University of California, Santa Barbara
(805) 893-5080
jennifer.mehl@ucsb.edu

Principal Investigator

- Reviews qualifications, criteria and approves all project personnel
- Maintains list and qualifications of project personnel/end-users
- Communicates with SCRE Administrator for credential and restricted dataset management

- Maintains list of restricted data files
- Enters into contract/agreement with restricted data provider/agency
- Responsible for reporting to restricted data provider/agency

Researcher/End-User

- Requests use of SCRE Service/Research Virtual Desktop
- User of SCRE Service/Research Virtual Desktop