Scripps Institution of Oceanography Network Security Policy

Activity	Date	Representative
Drafted	2/1/2020	Tod Kuykendall
Approved	1/19/2021	SIO Research and Academic Committee
Appendix C Added	11/8/2023	Bruce Applegate

The *Scripps Institution of Oceanography Network Security Policy* applies to all computers and network attached devices within Scripps Institution of Oceanography (SIO) campus, Nimitz Marine Facility (MarFac), or any remote network segment that is managed by SIO that is not already managed by another UC San Diego (UCSD) entity such as Information Technology Services (ITS) or Facilities.

I. Authority and Scope

In accordance with UC Office of the President (UCOP) policy *BFB-IS-3: Electronic Information Security* and the derived UCSD policies, SIO has established this Network Policy to address the unique needs and requirements of its varied and multi-faceted research and educational efforts.

II. Goals

- Protect UCSD and SIO users, computer resources and research
- Preserve academic freedom and foster research collaboration
- Follow a risk-based approach to policy implementation and enforcement
- Policy, requirements and specifications will be clear and reasonable
    - Technical Specifics will be held in Policy Appendix rather than policy

III. Network Policy Contents

A. Public Facing Computers Services and Functions
B. Remote Access to SIO Network Resources
C. Access to Network
    a. Acceptable Use Policy
    b. Registration and Contact
D. Inbound Network Monitoring and Blocking
E. Outbound Network Monitoring and Blocking
F. Governance

IV. Policy Text

A. Public Facing Computers Services and Functions

a. Both UCSD and SIO have determined that certain computer functions and services pose too great a security risk to be exposed for access by the public internet. UCSD Campus blocks a wide range of services/ports on a permanent basis and additional ports on a temporary basis.
b. SIO maintains a list of services that are blocked by default and are allowed open only by granted exception for labs and individuals who have requested that this functionality remain in place.
    i. Exceptions will only be granted after a security review for any potential vulnerabilities or risks from that service. Additional security settings, monitoring software, logging, or patching may be required before exceptions are granted.
    ii. Granted exceptions can be revoked if compliance with these security requirements lapses, required security patching is not maintained or new vulnerabilities are discovered for a service.
    iii. See Appendix A for a complete list of the restricted services.
c. SIO computers and devices that offer public services have additional security requirements to allow necessary visibility into this network traffic. Reference *Scripps Institution of Oceanography System Security Policy*, III, C. Software Agent and Monitoring for more information.

B. Remote Access through SIO Network Resources
    a. Any network traffic configurations that might allow UCSD/SIO network traffic to traverse to external resources without following the expected route and crossing the campus border exit must be disclosed and approved by the affected entities.
        i. This applies to San Diego Supercomputer Center and any other UCSD affiliated networks that might route SIO network traffic in an unexpected way.
    b. Any network connections that might allow external network traffic to traverse into or through the UCSD network as if it were local traffic must be disclosed and approved by the affected entities.
        i. An example of this would be a computer which is “dual homed” with one network connection to the UCSD/SIO network and another network connection to an external network. Traffic from this external network could flow into the UCSD as if it was coming from the internal computer address and the reverse flow is also possible.

C. Access to Network
    a. Acceptable Use - Access to all UCSD Network resources are governed by requirements outlined in IS-3 Electronic Information Security policy and the UCSD Electronic Communications Policy.

i. Many SIO user activities are further bound by additional data use agreements and Federal or State regulations governing data handling and sharing. Users in these areas may have to agree to different Acceptable Use conditions to allow UCSD and SIO to meet their obligations under these regulations and agreements.
ii. See Appendix B: Matrix of Network Profile by Data Sensitivity.

b. Registration and Contact - All resources on the SIO network will have an appropriate network registration with a current administrative contact.
i. See the *Scripps Institution of Oceanography Inventory Security Policy* for additional details.

D. Inbound Network Monitoring and Blocking
a. Following UCOP policy directives UCSD and SIO will use automated systems to monitor network traffic and to protect campus operations, resources and research.
i. All SIO network traffic will be routed such that the UCOP directives can be followed unless there is a clearly defined technical reason it cannot be and an exception is granted.
ii. Automated systems such as Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS) monitor network traffic to identify malicious network traffic via predefined patterns of known bad behavior. Identified traffic may be blocked depending on the system in place, the severity of the behavior and the sensitivity of the network destination.
iii. UCSD and SIO may block inbound traffic from network connections from "known bad" sources. The definitions of these sources may come from governmental or law enforcement sources, commercial firms, partner institutions or previously observed malicious behavior.
1. This blocking will always fall within the stated Goals of this policy and reviews of any traffic believed to be blocked incorrectly will be promptly reviewed.

E. Outbound Network Monitoring
a. Both UCSD and SIO may use automated monitoring of traffic originating on the campus network. This monitoring is designed to detect traffic patterns or access to resources that signal that a device may be compromised and/or accessing resources that may damage the computer or violate the security of UCSD networks. This access may be blocked immediately or network access may later be revoked until UCSD Security is confident the traffic has been fully investigated and mitigated as needed.
b. In network areas of high sensitivity additional outbound blocking may be in place to block access to unnecessary resources or services deemed to be potentially harmful to proper handling of sensitive data.

        i. Examples might be access to remote storage (eg Dropbox) that is not approved for sensitive data. These restrictions will be considered and implemented on a case by case basis.
    c. In the most sensitive areas all outbound access may be restricted with the exception of access to pre-approved "whitelisted" resources.
        i. See Appendix B: Matrix of Network Profile by Data Sensitivity.
    d. Networking services or equipment that interfere with the effective monitoring of network traffic may be prohibited or blocked depending on the sensitivity of the network traffic in that area.
        i. Examples of these services include non-UCSD operated VPNs or Proxy services or anonymizing software such as Tor. Equipment examples include NAT aggregators or VPN appliances.

F. Governance
    a. Per UCSD 135-3, V Access Restrictions "UCSD Electronic Communication Services may be wholly or partially interrupted, suspended, terminated, or limited" for violation of UCSD Policies among other reasons.
    b. Following a "risk based approach" as dictated by IS-3 implementation and enforcement may be directed by SIO leadership with emphasis on areas known to possess more sensitive data, higher availability needs or other concerns.

Appendices:

A. Public Facing Services Controlled by UCSD and SIO
B. Matrix of Network Profile by Data Sensitivity
C. Policy for UCSD Operated Ships

Applicable Policies:

- University of California – Policy BFB-IS-3
    - III. Policy
        - Section 8: Asset Management
        - Section 9: Access Control
        - Section 12: Operations Management
        - Section 13: Communications Security
    - V. Procedures
- UC San Diego 135-3 Network Security and Appendices
- UCSD 135-5 Electronic Communications Policy (ECP)
- University California - Systemwide IT Policy Glossary

Scripps Institution of Oceanography Network Security Policy

Appendix A: Public Facing Services Controlled by UCSD and SIO

Restricted Service Groups	Services and Typical Ports	Security Rational
Sharing	SMB - 137-138, tcp/udp 445 tcp AFP - 458 tcp NFS - 111, 2049 tcp/udp ftp - 21 tcp	Sharing services should only be opened intentionally to prevent accidental data spillage due to misconfiguration or protocol vulnerability
Web	HTTP/S - 80, 443, 4443, 8080, 8443 tcp	Web vulnerabilities are the most common forms of internet compromise used by attackers
Command	ssh - 22 tcp VNC - 5900 tcp ARD - (ssh+VNC) 5988 tcp RDP - 3389 tcp telnet - 23 tcp	Command ports allow unauthorized users to act as computer owners and the risk of general exposure is very high
Database Ports	MySQL - 3306 tcp MS-SQL - 1433, 1434 tcp Mongo DB - 27017, 27018 tcp Postgres - 5433 tcp	Databases should only be open to trusted IP addresses due to the potential for large data exposure spill
Discovery protocols (direct or multicast)	PnP - 1900 udp OS X - 427, 3283 udp	Discovery protocols can be used as reconnaissance techniques and these protocols rarely scale properly for use on a network as large as the on at UCSD
Commonly scanned ports for malicious activity	81 tcp, 2000 tcp	These ports are often scanned by external attackers and have no predefined services running on them that blocking disrupts

UC San Diego blocks a number of services at the campus border and SIO has extended this list to contain additional services and ports. Requirement of these services to be allowed open to the public only by exception was announced by Margaret Leinen Vice Chancellor for Marine Sciences and enacted by Scripps IT over the following year. This service prohibition is based on the exposure caused by a service and extends to equivalent services and those run on non-standard ports.

Exception Process:
Exceptions for Web and Command Services can requested here:
https://scripps.ucsd.edu/it/security

Exceptions to run these services open to the internet may come with a list of security recommendations and/or requirements. Computers that fail to meet the requirements will not be granted an exception and those granted an exception may have the exception revoked if the computer falls out of compliance and is not corrected.
Currently these requirements include:

- Comply with UCSD current operating system and patch criteria
- Inventory and/or Security endpoint agents (depending on function)
- Logging specifications and/or log forwarding (depending on function)

Exceptions can only be made for services that SIO controls not for those services blocked at the UCSD border.

Scripps Institution of Oceanography Network Security Policy

Appendix B: Matrix of Network Profile by Data Sensitivity

	PS	P4’	P4	P3	P2	P1
Inbound Internet	X	X	W	W/F	F	F
Outbound Internet	X	W	W	W/F	F	A
Inbound UCSD	W	W	W	F	A	A
Outbound UCSD	W	W	W/F	F	A	A
Inbound local/infrastructure	W/F	W/F	F	F	A	A
Outbound local/infrastructure	F	F	F	A	A	A

P4’: Data covered by Federal or State regulations (CUI/FOUO/ITAR)
P4: Most sensitive University data, PII, PCI
P3: UCSD Business information, proprietary
P2: Non-Proprietary business data,transactional data
P1: Public
PS: Security Exception computers and devices (XP, unsecurable devices)

X: Not Allowed
W: Whitelisted - Pre-approved allowed only
F: Filtered - some blocking and/or automatic protections (IPS, etc)
A: Allowed

Scripps Institution of Oceanography Network Security Policy

Appendix C: Policy for UCSD Operated Ships

All pertinent UCOP, UCSD and SIO security policies apply to the computers and networks of UCSD operated ships. Ship operations present unique network and bandwidth challenges so the network monitoring to ensure safe ship operations may exceed the ordinary monitoring and restrictions of the general campus network.
This appendix covers specifications of policy implementation as they relate to the ships.

Limitations of Activity:
The performance of normal business, research, education, and other vital functions is dependent upon the appropriate use of the ships resources, network and bandwidth. To maintain this performance, the activities below are strictly prohibited.

Any intentional or unintentional action that:

1. Impairs the overall function of the network
2. Impairs the ability to monitor or measure network traffic or network usage
3. Produces an excessive load on the network
4. Results in distribution of computer viruses or malware
5. Results in scanning any systems or networks other than the devices that belong to you

Note: In times of limited bandwidth network operators reserve the right to limit user functionality to preserve bandwidth and prioritize traffic for the most essential services.

Outbound Network Monitoring and Relevant SIO Security Policy:

IV, E, a: Monitoring may occur by UCSD and by external parties contracted by UCSD.

IV, E, d: Software and services that obscure details of network traffic are often used by malware and are not permitted and may be automatically blocked.

Software: Peer-to-peer (P2P) applications (ex. BitTorrent, Thunder.Xunlei)Services: Cloud VPNs (ex. Cloudflare, NordVPN) and anonymizers such as Tor

Note: Site to site VPNs are allowed (ex. VPN back to home institutions)

Federal Restrictions
All restrictions by the US Federal Government on use of any hardware (ex. Huawei networking) or software (ex. Kaspersky Anti-Virus, TikTok) will be enforced.

Matrix of Prohibited Network Activities and Standard Response

Network / Activity	P2P, Tor, Cloud VPN	Excessive or Abusive Network Traffic	Ransomware, Destructive Software	C&C Malware, InfoStealer, Confirmed Malware	Unwanted Software / Suspected Malware
Crew	Prohibited	Block/ Quarantine	Block/ Quarantine	Block	Notify, Patch
Crew BYOD	Prohibited	Block/ Quarantine	Block/ Quarantine	Notify, Patch	Notify, Potentially Patch
Scientific BYOD	Prohibited	Block/ Quarantine	Block/ Quarantine	Potentially Notify	Potentially Notify
Scientific	Prohibited	Block/ Quarantine	Block/ Quarantine	Potentially Notify	Potentially Notify

- Prohibited: Blocked on the firewall network in an automated fashion.
    - Blocks can be appealed via the exception process on a per device basis.
- Notify, Patch: Users will be identified and contacted about remediation to bring the device into compliance.
- Block/Quarantine: Devices can be blocked or removed from the ships networks manually or via an automated process.
- Potentially Notify: Notification can occur depending on time of a detection and presence on ship. Neither UCSD nor SIO commit to notifying visitors of any detected potentially unwanted software.