Scripps Institution of Oceanography System Security Policy

Activity	**Date**	**Representative**
Drafted	3/1/2020	Tod Kuykendall
Approved	1/29/2021	SIO Research and Academic Committee

The *Scripps Institution of Oceanography System 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. It also applies to any remote computer, device or cloud service that processes or stores SIO information or research data.

I. Authority and Scope

In accordance with UC Office of the President (UCOP) policy *BFB-IS-3: Electronic Information Security* and the derived UC San Diego (UCSD) policies SIO has established this System Security Policy to address the unique needs and requirements of the 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. System Security Policy Contents

A. Use of UCSD Resources
B. Software Agent and Monitoring
C. Vulnerability Scanning
D. Logging and Log Forwarding
E. Computers and Devices Unable to Comply with Policy
F. Governance

IV. Policy

A. Use of UCSD Network Resources

    a. UCSD provides a full suite of network services and layers of monitoring and security controls are incorporated into many of them. For this reason use of campus services is required within SIO networks unless an exception has been granted for a specific use case.
    b. SIO may forbid internal duplicate services and block access to external network services to enforce usage of the UCSD service where a specific exception does not exist.
    c. Use of services that prevent routine network security monitoring by UCSD is allowed on by explicit exception after review.
    d. Use of some products, services are restricted or forbidden by UCSD and SIO to reduce security or liability risk to campus or in compliance with State or Federal directives.
    e. See *System Security Policy Appendix A* for a complete list of the covered services.

B. Software Agent and Monitoring

    a. SIO computers may have required software and/or configuration requirements based on a variety of factors including services offered, data sensitivity or availability requirements, physical or organizational location or leadership mandate.
    b. See *System Security Policy Appendix B* for examples and more specific information.

C. Vulnerability Scanning

    a. Both UCSD and SIO operate both scheduled and ad hoc network scan using a variety of tools to test for and detect potential security vulnerabilities for computers and devices on the network. These scans should not be blocked at the network or by endpoints to ensure accurate reporting. Any issues related to scanning should be elevated to USD Information Security and dealt with appropriately.

D. Logging and Log Forwarding

    a. UCSD and SIO support centralized log aggregation for computers, devices and servers where this is required.
    b. Required local logging requirements for servers, computers, and devices may be required for areas with increased sensitivity or additional compliance requirements,
        i. Instructions for configuration and any software will be supplied to computer administrators as needed.
        ii. See *System Security Policy Appendix B* for examples of required logging and log forwarding.

E. Computers and Devices Unable to Comply with Policy

   a. Computers and devices unable to comply with policy but continue to be essential to research or workflow should be identified to SIO IT so an exception can be created after proper compensating controls are put in place to protect the vulnerable device.

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. Services Controlled by UCSD and SIO
B. SIO Required Software and Configurations

Applicable Policies:

- University of California – Policy BFB-IS-3
    - III Policy
        - Section 9: Access Control
        - Section 12: Operations Management
            - 12.4 Logging and monitoring
            - 12.6 Technical vulnerability management and patch management
        - Section 13: Communications Security
    - UC Event Logging Standard
- UC San Diego 135-3 Network Security and Appendices
- UCSD 135-5 Electronic Communications Policy (ECP)
- UC Secure Software Configuration Standard
- UC Event Logging Standard
- University California - Systemwide IT Policy Glossary

System Security Policy Appendix A

Appendix A: Services Controlled by UCSD and SIO

UCSD Managed Network Services

Required UCSD Computer Service	Port	Security Impact
Domain Name Service - DNS	53 tcp/udp	UCSD DNS has “firewalling” to prevent name resolution of known bad sites (phishing email links etc.). DNS queries can be used maliciously by bad actors in a number of ways (exfiltrate data, etc.) so DNS logging is an important part of security review and we cannot review logs when UCSD DNS is not used.
Network Time Protocol - NTP	123 tcp/udp	Synchronization of log timing across the organization is an important element in security investigations so use of a single source of time is important. This is also a requirement of many security frameworks and audit regimes.
Dynamic Host Configuration - DHCP	67/68 udp	DHCP controls assignment of IP addresses and can be abused locally to confuse computer IPs.
UCSD VPN	Various	UCSD monitors many aspects of network traffic and the use of VPN systems that are not operated by UCSD defeats many of these security measures.
UCSD Proxy/NAT	Various	UCSD monitors many aspects of network traffic and the use of Proxy systems that are not operated by UCSD defeats many of these security measures. Running of proxies is restricted by campus policy.

SIO Prohibited Insecure Protocols

Insecure Services	**Security Impact**
SMB v1	SMB version 1 has been discontinued and has security flaws which will never be patched. Also exploit path for Eternal Blue on Windows.
SSH v1	ssh version 1 has been discontinued and has security flaws which will never be patched.
Outdated SSL/TLS Connections and cipher settings	Old HTTPS have a variety of security issues and should be used: ● All versions of SSL ● TLS v1.0
Telnet (any version)	Telnet is an unencrypted command protocol that should not be used.
SMNP v1	SNMP can send control commands without authentication
Unencrypted Authentication	Any form of authentication that is not encrypted is prohibited by both UCSD and SIO

SIO Prohibited Protocols Configurations

Insecure Protocol Configurations	**Security Impact**
SSH with root access via password	“Root” access via ssh is too powerful and dangerous a configuration to allow. Anyone guessing the ssh password can take full control of the computer.
SSH with known accounts: admin, adm, administrator, apache, www, user, guest, games, test, temp, student, webmaster, postgres, mysql	This list compiled from industry studies or ssh abuse and local logs.

UCSD Controlled or Forbidden Products and Vendors

Additional Controlled Services	**Security Impact**
Peer-to-Peer networking (BitTorrent, etc.)	Peer to peer (P2P) services have valid uses but are also used for the downloading of materials under