IT Security Office

Information Technology Division
San Diego State University
5500 Campanile Dr.
San Diego CA, 92182-8114
https://security.sdsu.edu

SAN DIEGO STATE UNIVERSITY

Memorandum

Date: October 7, 2021

To: IT Governance Committee

From: Ricardo Fitipaldi
Chief Information Security Officer

Subject: Server Policy - Review and Vote for Approval

SDSU drafted the attached Server Policy in response to the CSU Audit, which required SDSU servers to have security controls, including log management and endpoint protection. The Server Policy was also necessitated as a result of the security breach which occurred at CSU San Marcos. The Chancellor's Office, with the endorsement of the CSU Chancellor and Presidents, launched a cybersecurity hygiene project, which identified the need to accurately document information about the servers owned, operated, and housed by SDSU.

The Server Policy was shared for review and input with the University Senate Instructional and Information Technology (IIT) Committee, the IT Security Working Group, and the IT Governance Committee. In addition, the Server Policy was shared with SDSU Research Foundation (specifically, researchers and principal investigators) and the University Research Council.

After several reviews and comments, the substantive changes to the Server Policy include the following:

- Provide a clearer definition of what a server is,
- Remove the pre-authorization clause and change the server registration, including a 60-day window to register the server.
- Clarify the required minimum registration information.
- Clarify that physical security applies to physical and virtual systems.
- Change the server backup section to “Recommend” instead of ”Required”.

IT Security Office

Information Technology Division
San Diego State University
5500 Campanile Dr.
San Diego CA, 92182-8114
https://security.sdsu.edu

SAN DIEGO STATE UNIVERSITY

Please review the Server Policy and vote for approval. The decision to approve the Server Policy will be communicated campus-wide, which includes informing the University Senate IIT Committee.

Upon approval, the IT Security Office (ITSO) will lead the development of preparing operating procedures to address the processes of registering the servers, requesting exemptions, and communicating an adoption timeline.

cc: Jerry Sheehan, SDSU VP and Chief Information Officer

IT Security Office

Information Technology Division
San Diego State University
5500 Campanile Dr.
San Diego CA, 92182-8114
https://security.sdsu.edu

SAN DIEGO STATE UNIVERSITY

Server Policy Final DRAFT

SDSU Server Security Policy

Extends: CSU Policy ICSUAM 8050 - Configuration Management

1.0 Purpose

This policy establishes the server configuration management framework for San Diego State University (SDSU) servers to ensure security, reliability, and the coordination of technical operations. The practices below define roles, responsibilities, procedures, and controls to encourage consistent, secure, and documented IT services delivery.

2.0 Scope

2.01 All employees, faculty, staff, contractors, consultants, temporary and other workers at SDSU must adhere to this policy. (This includes but is not limited to employees of Auxiliaries such as the SDSU Research Foundation, centers, and research programs)

2.02 This policy also applies to all SDSU servers including those deployed and managed by SDSU Research Foundation, research labs/program, Centers, and other SDSU auxiliaries such as Aztecshops, KPBS and Associated Students.

2.03 This policy applies to server equipment that is owned, operated, and/or leased by SDSU. Systems registered under an SDSU-owned internal network domain, including those servers operated in cloud environments, are also in scope of this policy.

2.04 The policy extends to any computing servers that attach to either the wired or wireless network.

3.0 Definition of Terms

3.01 Server – a physical or virtual device that provides a specific type of service on behalf of another computer or computer user (i.e., a client). Examples include a file server that stores and manages access to files, a web server that facilitates access to websites, an application server that provides access to shared software, an High Performance Computing Cluster (HPC), or a name server that maps user and computer names to machine and network addresses.

3.02 Server Administrator – individual(s) designated by the server owner that are principally responsible for performing server management functions, including the installation, configuration, security, ongoing maintenance, and registration of the server.

Information Technology Division
San Diego State University
5500 Campanile Dr.
San Diego CA, 92182-8114
https://security.sdsu.edu

3.03 Server Owner – the department, Principle Investigator, or division lead charged with overall responsibility for the server asset.

4.0 Policy

4.1 General Requirements

4.1.1 Server Registration

The server owner or server administrator is required to register the server in a timely manner, but no later than 60 days. This server registration will ensure that the server has identified technical contact points, enrolled in the necessary security scans, and made all users aware of any essential server software required for campus security compliance.

4.1.2 Consequence if Server is Not Registered

The IT Security office may limit or remove the SDSU network from non-registered or non-compliant servers. A server may return to regular access when it meets the requirements of this policy.

Minimum Server Registration Requirements

Device Registration

The following items must be met:

- Servers must be registered within the SDSU Configuration Management Database (CMDB) or other authorized Technology asset management system. At a minimum, the server registration must contain point of contact information and server specifications listed below:
    - Server Owner contact(s): Name, email, and phone (also used for emergencies)
    - Server Administrator(s): Name, email, and phone (also used for emergencies)
    - Hardware and Operating System/Version
    - MAC and IP addresses
    - Main functions and applications
    - Type of data transmitted, stored, or processed in accordance with classification from CSU of data.

- Information in the SDSU Configuration Management Database (CMDB) or authorized

Information Technology Division
San Diego State University
5500 Campanile Dr.
San Diego CA, 92182-8114
https://security.sdsu.edu

Technology asset management system must be updated annually.

5.0 Auditing

For security, compliance, and maintenance purposes, IT Division personnel may monitor and audit equipment, systems, servers, processes, and network traffic.

Server administrators identified may be required to share logs associated with access with the IT Division. Requests for logs should be responded to in a timely manner, usually within 24 hours.

6.0 Server Configuration Requirements

Server administrators shall also make every effort to adhere to the latest applicable Security Configuration Benchmarks published by the Center for Internet Security (CIS). CIS Benchmarks are provided for various operating systems, application software, and multiple versions thereof. CIS Benchmarks are defined via consensus among security professionals worldwide and used by thousands of enterprises as their de facto local configuration standards. Contact SDSU's Information Security team (security@sdsu.edu) for assistance in utilizing these benchmarks.

At minimum, the server must comply with the following requirements.

6.1 Vulnerability Scanning and Remediation

The Information Security Office will perform vulnerability scans against all computer servers operated on the SDSU network on a monthly basis. All critical and high vulnerabilities[1] must be remediated or have appropriate controls applied in accordance with the SDSU vulnerability management standard within thirty days of report. All other vulnerabilities must also be addressed in a timely manner.

6.2 Computer Virus Protection

6.2.01 Malware protection software must be installed and enabled, as technology permits. If technology does not permit, a security exception must be submitted.
6.2.02 Malware protection software must be configured to update signatures at least daily.

6.3 Monitoring and Alerting

6.3.01 All servers and applications must maintain a means to log access and usage. Server administrators must implement appropriate logging and monitoring controls. At a minimum

[1] As defined by Common Vulnerability Scoring System (CVSS) or equivalent metric.

Information Technology Division
San Diego State University
5500 Campanile Dr.
San Diego CA, 92182-8114
https://security.sdsu.edu

and as technology permits, all changes, edits, logins, administrative activities, and accesses of Confidential Protected data (PL-1) must be logged and tied to an account and a timestamp. All administrative access and activity must be logged.
6.3.02 All logs must be retained in accordance with the CSU retention and disposition schedules and SDSU log retention policy.
6.3.03 Server administrators must review all logs regularly for, but not limited to, indicators of suspicious activity, such as configuration changes, successful and failed access attempts, the presence of threats identified by vendor databases or signatures.

6.4 Documentation and Inventory

Server administrators must register with the SDSU Change Management Database (CMDB) as listed above. Annual review by the server administrator is required to ensure all information is up to date.

6.5 Access Security

6.5.01 All application and server accounts must be reviewed for inactivity no more than semi-annually and any dormant accounts disabled.
6.5.02 As feasible, all privilege accounts must have multi-factor authentication enabled.
6.5.03 All application and server accounts with elevated access and privileges must be reviewed quarterly.
6.5.04 Only secure remote-access protocols such as SSH, SFTP, SCP, RDP w/ strong encryption, and VPN must be used to access the server remotely.
6.5.05 Service Banners - wherever feasible, a log-on banner stating that the system is for authorized use only should be displayed for anyone attempting to connect to the system.

6.6 Physical Security

6.6.01 Servers must be physically secured in the University Data Center or in physical or virtual cloud facilities approved by the Information Security Office.
6.6.02 Servers used for research and most direct connected lab equipment are permitted. However, proper physical security measures and documentation must be described during the server registration.

6.7 Recommended Backup Strategy

6.7.01 Server administrators should establish and follow a procedure to carry out regular server and application backups.
6.7.02 Backups should be verified monthly through automated verification, customer restores, or trial restores.
6.7.03 Server administrators must maintain documented restoration procedures for the

Information Technology Division
San Diego State University
5500 Campanile Dr.
San Diego CA, 92182-8114
https://security.sdsu.edu

server and the data stored on those servers.

7.0 Non-compliance and Exceptions

7.1. Compliance Measurement

7.1.01 The IT Security Office (ITSO) team will verify compliance to this policy through various methods, including but not limited to automatic network monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

7.1.02 In emergency circumstances, ITSO will attempt to notify the server owner or administrator whenever it determines that a server has become an imminent threat to university information resources, such as when a server's integrity is compromised or when it places other network devices at risk.

If the server administrator or the server owner does not respond in a timely manner, ITSO may request to isolate the offending server from the network until the risk is mitigated.

7.2 Exceptions

Any exception to the policy must be submitted by the server owner or designee. Exceptions to this policy and associated standards shall be allowed only if previously approved by the Vice President and Chief Information Officer.

7.3 Non-Compliance

7.3.01 Non-compliance with these standards without an approved exception will result in revocation of server or network access, notification of supervisors, and reporting to the Internal Audit Office.

7.3.02 ITSO will attempt to notify the server owner or administrator of all non-compliance issues.

7.3.03 The information system may be allowed back on the campus network by the IT Security Office after complying with the configuration and security standards or by submitting an approved exception to the IT Security Office.

Information Technology Division
San Diego State University
5500 Campanile Dr.
San Diego CA, 92182-8114
https://security.sdsu.edu

SAN DIEGO STATE UNIVERSITY

REVISION CONTROL

Revision History

Version	Revision Date	Summary of Revisions
0.1	January 2021	Initial Draft
0.2	June 2021	Revised Draft
0.3	October 2021	Final Draft

Review / Approval History

Review Date	Reviewed By	Action (Reviewed, Recommended or Approved)