Server Access/Maintenance Policy

a. Ownership and Responsibilities

i. An operational group in the respective Department/Centre/Section that is responsible for system administration must own all internal servers deployed at Sreenidhi.

ii. Approved server configuration guides must be established and maintained by each operational group, based on business needs and approved by Director/Deans/Heads.

iii. Operational groups should monitor configuration compliance and implement an exception policy tailored to their environment.

iv. Each operational group must establish a process for changing the configuration guides, which includes review and approval by Director/Deans/Heads.

v. At a minimum, the following information is required to positively identify the point of contact:

- Server contact(s) and location, and a backup contact
- Hardware and Operating System Version
- Main functions and applications, if applicable

vi. Information in the management system must be kept up-to-date.

vii. Configuration changes for production servers must follow the appropriate change management procedures.

viii. All logs will be maintained for a period of three months.

ix. On special requests static external IP addresses may be allocated to specific servers for access from outside on specific ports. This may be required for designated web servers and other research facilities.

x. Unrestricted access to internet access bypassing the proxy servers may be given from specific servers on request for special research and operational needs. It will be the responsibility of the facility in-charges to ensure that

   i. access to such a facility is restricted and users do not use such a facility to access the internet bypassing the proxy servers

   ii. IT usage policy and privacy policy are strictly adhered to.

   iii. Access logs are maintained for accesses on all ports as required.

b. General Configuration Guidelines

i. Operating System (OS) configuration should be in accordance with approved Department/Centre/Section guidelines.

ii. Services and applications that will not be used must be disabled where possible.

iii. Access to services should be logged and/or protected through access-control.

iv. The most recent security patches must be installed on the system as soon as practical.

v. Trust relationships between systems are a security risk, and their use should be avoided.

vi. Do not use a trust relationship when some other method of communication will do.

vii. Always use standard security principles of least required access to perform a function.

viii. Do not use root when a non-privileged account will do.

ix. If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH).

x. Servers should be physically located in an access-controlled environment.

xi. Servers are specifically prohibited from operating from uncontrolled cubicle areas

c. Monitoring

i. All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:

- All security related logs would be kept online for a minimum of 1 year.
- Daily incremental backups will be retained for at least 1 week.
- Weekly full backups of logs will be retained for at least 1 month.
- Monthly full backups will be retained for a minimum of 3 years.

ii. Security-related events will be reported to InfoSec, who will review logs and report incidents to IT management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:

- Port-scan attacks
- Evidence of unauthorized access to privileged accounts
- Anomalous occurrences that are not related to specific applications on the host.

d. Routine Precautions

a. Only authorized administrators are authorized to login to the mail, web, proxy and other servers.

b. The designated system administrator/operational group receives an email alert whenever such an advice is released by the official maintainers of the software.

c. The software is updated periodically and whenever required.

d. All ports except those necessary for functioning of the servers are blocked (firewalled) both from outside and inside.

e. Standard intrusion detection software is run on the Sreenidhi network to monitor any change of MAC addresses corresponding to IP addresses of trusted machines. The Systems Manager automatically receives an email alert in such cases.

e. DHCP Server

i. The DHCP service of Sreenidhi to enable automatic IP configuration of clients.

ii. Installation of unauthorized DHCP servers, without explicit consent from the Computer Centre, will not be permitted in any VLAN as such DHCP servers can interfere with normal usage.

f. Compliance

i. Audits will be performed on a regular basis by authorized organizations within Sreenidhi.

ii. The Computer Centre group, in accordance with the Audit Policy, will manage audits.

iii. Computer Centre Group will filter findings not related to a specific operational group and then present the findings to the appropriate support staff for remediation or justification.

iv. Every effort will be made to prevent audits from causing operational failures or disruptions.

Enforcement

Any employee/user found to have violated this policy may be subject to disciplinary action and as per IT laws of Govt. of India.