General Server Security Guidelines

Section 1 - Rationale and Scope

(1) The purpose of this Policy is to establish standards for TDS staff and for any other operational group responsible for server administration for the base configuration of internal server equipment that is owned and/or operated by UNE. Effective implementation of this policy will minimize unauthorized access to UNE proprietary information and technology.

(2) This Policy applies to server equipment owned and/or operated by UNE, and to servers registered under any UNE-owned internal network domain.

(3) This Policy is specifically for equipment on the internal UNE network.

Section 2 - Policy

Ownership and Responsibilities

(4) All internal servers deployed at UNE must be owned by an operational group that is responsible for system administration. Server configuration guides must be established and maintained by suitably qualified IT personnel, articulate how the server fulfils business requirements and be approved by Technology and Digital Services (TDS).

(5) Operational groups should monitor configuration compliance and implement an exception policy tailored to their environment. Each operational group must establish a process for changing the configuration guides, which includes review and approval by TDS.

(6) Servers must be registered with TDS. At a minimum, the following information is required to positively identify the point of contact:

  a. Custodian contact(s) and location, and a backup contact(s)
  b. Hardware and Operating System/Version, MAC address, IP and DNS information.
  c. Main functions and applications, if applicable
  d. Information held with IT must be kept up-to-date.
  e. Configuration changes for production servers must follow the appropriate change management procedures.
  f. Servers must fit a specific business requirement and should comply with all other IT policies. In the case of new servers, if an existing service is already provided by IT and fits the requirements, this system should be used instead (e.g. web servers).

(7) Encryption technologies such as SSL certificates must be used to protect Web based login forms to protect the username and password from being intercepted by a third party on the LAN and WAN. They must use at least 256bit SSL single root certificate from a well known registered Certificate Authority. Please check with TDS for a list of currently accepted certificate issuers.

This policy document may be varied, withdrawn or replaced at any time. Printed copies, or part thereof, are uncontrolled and should not be relied upon as the current version. It is the responsibility of those printing this document to always refer to UNE Policy Library for the latest version. University of New England - CRICOS Provider Number 00003G – TEQSA Provider Code: PRV12054 Australian University – ABN: 75 792 454 315   *Page 1 of 4*

Guidelines

(8) Operating System configuration should be in accordance with approved IT guidelines. This includes hardening of the Operating System using guidelines published by Technology and Digital Services.

(9) Services and applications running on the server, which will not be used, must be disabled where practical.

(10) Access to services should be logged and/or protected through best practice IT access-control methods

(11) The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.

(12) Always use standard security principles of least required access to perform a function.

(13) Do not use root/Administrator when a non-privileged account will do.

(14) 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 SSL, SSH, VPN or IPSec).

(15) Servers should be physically located in an access-controlled environment:

(16) Premises must be physically strong and free from unacceptable risk from flooding, vibration, dust, etc.

(17) There must not be an inordinate amount of combustible material (e.g. paper) stored in the same room as the computer system.

(18) Air temperature and humidity must be controlled to within acceptable limits at all times.

(19) Servers are specifically prohibited from operating in uncontrolled cubicle/office areas.

(20) The Operating system must be server based i.e. Windows 2003 server, Windows 2008 server, Linux server.

(21) Windows XP pro/home or workstation versions of other Operating systems are not valid server platforms for production environments and as such they do not meet the IT guidelines for server platforms.

(22) Computing equipment should be electrically powered via UPS to provide the following:

   a. Minimum of 15 minutes' operation in the event of a power blackout.
   b. Adequate protection from surges and sags.
   c. Trigger an orderly system shutdown when deemed necessary.

Monitoring

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

   a. All security related logs will be kept online for a minimum of 1 week.
   b. Daily tape backups will be retained for at least 1 week.
   c. Weekly full tape backups of logs will be retained for at least 1 month.
   d. Monthly full backups will be retained for a minimum of 1 year.

(24) Security-related events will be reported to IT, 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:

   a. Port-scan attacks

b. Evidence of unauthorized access to privileged accounts

c. Anomalous occurrences that are not related to specific applications on the host.

Compliance

(25) Audits will be performed on a regular basis by authorized Staff within Technology and Digital Services.

(26) Audits will be managed by the internal audit group or Technology and Digital Services, in accordance with the University's [Audit Policy](#) and Procedures. Technology and Digital Services will filter findings not related to a specific operational group and then present the findings to the appropriate support staff for remediation or justification.

(27) Every effort will be made to prevent audits from causing operational failures or disruptions.

Enforcement

(28) Any employee found to have violated this policy might be subject to disciplinary action, up to and including termination of employment.

Section 3 - Definitions

(29) Server For purposes of this policy, a Server is defined as an internal UNE Server. Desktop machines and Lab equipment are not within the scope of this policy.

(30) Hardening The process of securing a system by reduce vulnerability of attack including the removal of unnecessary software, unnecessary usernames or logins and the disabling or removal of unnecessary services

Status and Details

Status	Current
Effective Date	27th July 2015
Review Date	28th February 2021
Approval Authority	Chief Information Officer
Approval Date	14th November 2011
Expiry Date	To Be Advised
Unit Head	Angie Hendrick Chief Information Officer 02 6773 2044
Author	Robert Irving
Enquiries Contact	Technology and Digital Services +61 2 6773 5000