IT Server Room Access Procedures

Section 1 - Overview

(1) This procedure outlines the processes to be followed when granting or revoking access to the Technology and Digital Services Server Rooms. The procedure also covers the responsibilities and requirements for University Representatives when accessing the University's TDS Server Rooms.

Section 2 - Scope

(2) The NSW State Auditor requires that access to University TDS server rooms is strictly controlled, monitored and logged. The server rooms are classified as a restricted area containing sensitive and business critical data and services. The procedures outlined in this document are applicable to all University Representatives who have access to University TDS server rooms.

Section 3 - Procedure

Approval

(3) The Chief Information Officer, Associate Director Infrastructure Services or the IT Security Manager may grant or revoke access to the University TDS Server Rooms.

Submitting the Approved Form

(4) All requests for TDS Server Room access must be made using the ITD Server Room Access Request form.

(5) The approved, form should be submitted to TDS Business Services in person or via email to itoffice@une.edu.au

Responsibilities

(6) TDS Business Services will ensure that the TDS Server Room Access Request Form has been completed and approved in accordance with this procedure.

(7) TDS Business Services will arrange for access to be added to the University ID card for the time period specified on the approved form.

(8) If the person making the request does not have a University ID card, TDS Business Services will issue a temporary IT Visitor card with the access privileges for the time period specified on the approved form.

(9) TDS Business Services will confirm, in writing via email, to the UNE Representative that access has been added to their University ID card or TDS Business Services will, in writing via email, request the University Representative to collect the IT Visitor Card and sign for the collection on the space provided on the approved TDS Server Room Access Request Form.

(10) The UNE Representative must return the IT Visitor Card to IT Business Services upon expiration of the time period specified on the approved ITD Server Room Access Request Form or upon the written request of the Chief Information

Officer, Associate Director Infrastructure Services or the IT Security Manager. Irrespective of the circumstances upon which the IT Visitor Card is returned the University Representative must sign the TDS Server Room Access Request form, lodged with TDS Business Services, indicating the return.

(11) UNE Representatives must use their University ID card to access the TDS Server Rooms whenever card access is operational.

(12) An TDS Server Room key is available to approved TDS staff via the TDS Keywatcher system. The key will only be used if card access is not available. Sections 16, 17 and 18 of this Procedure apply to the use of this key.

(13) Keys to TDS server rooms will only be issued under special circumstances and requested via the TDS Server Room Access Request form and approved by the Chief Information Officer, Associate Director Infrastructure Services or IT Security Manager.

(14) TDS Business Services will request, in writing via email, the UNE Representative to collect the TDS server room key as specified on the approved form and sign for the collection of the key on the space provided on the approved ITD Server Room Access Request form.

(15) The UNE Representative must return the key to TDS Business Services upon expiration of the time period specified on the approved ITD Server Room Access Request form or upon the written request of the Chief Information Officer, Associate Director Infrastructure Services or the IT Security Manager. Irrespective of the circumstances upon which the key is returned the UNE Representative must sign the ITD Server Room Access Request form, lodged with TDS Business Services, indicating the return.

(16) Any UNE Representatives holding keys to any of the TDS Server Rooms must ensure the keys are kept in a secure, locked location when not in use. It is the UNE Representative's responsibility to ensure keys are always secure.

(17) UNE Representatives must inform University Safety & Security prior to the use of the key if a key is to be used to access the TDS Server Rooms. The IT Security Manager must also be informed via email to it-security@une.du.au outlining the reason for accessing the TDS server rooms via a key and include the date, time and duration of the access.

(18) UNE Representatives who become aware of or suspect there may have been unauthorised access to an TDS Server Room must inform the IT Security Manager via email to it-security@une.edu.au . Please include the location, date and time of the event.

(19) UNE Representatives who discover or become aware of a weakness in the security controls for any of the TDS Server Rooms (e.g. unlocked doors, inappropriate access assigned to an ID card, etc) must report the matter immediately or as soon as practicable, including all relevant information to the IT Security Manager via email to it-security@une.edu.au .

(20) TDS Business Services will provide a copy of these procedures to UNE Representatives with the ITD Server Access Request form.

Authority and Compliance

(21) The Procedure Administrator, the Chief Information Officer makes these procedures.

(22) UNE Representatives must observe these Procedures in relation to University matters.

(23) This Procedure operates as and from the Effective Date.

(24) Previous Procedures relating to TDS Server Room Access are replaced and have no further operation from the Effective Date of this new Procedure.

Section 4 - Definitions

(25) Approved - means authorised by the Chief Information Officer, the Associate Director (Infrastructure) or the IT Security Manager.

(26) TDS Server Rooms - means the server rooms maintained by the Technology and Digital Services and includes the TDS building server rooms, the T.C. Lamble building server room, the Austin College server room and the Booth Block basement PABX room.

(27) Effective Date is the date on which this Rule will take effect.

(28) Procedure Administrator is the Chief Information Officer.

(29) University Representative means a UNE employee (casual, fixed term and permanent) contractor, agent, appointee, UNE Council member, adjunct, visiting academic and any other person engaged by UNE to undertake some activity for or on behalf of the UNE. It includes corporations and other bodies falling into one or more of these categories

Status and Details

Status	Current
Effective Date	18th January 2016
Review Date	5th October 2022
Approval Authority	Chief Information Officer
Approval Date	18th January 2016
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

Glossary Terms and Definitions

"UNE Representative" - Means a University employee (casual, fixed term and permanent), contractor, agent, appointee, UNE Council member, adjunct, visiting academic and any other person engaged by the University to undertake some activity for or on behalf of the University. It includes corporations and other bodies falling into one or more of these categories.

"University Representative" - University Representative means a University employee (casual, fixed term and permanent) contractor, agent, appointee, UNE Council member, adjunct, visiting academic and any other person engaged by the University to undertake some activity for or on behalf of the University. It includes corporations and other bodies falling into one or more of these categories.