



Server Room Access Procedure

ROI Server Room Access Procedure

Overview:

This procedure outlines the processes to be followed when granting or revoking access to the ROI Server Rooms. The procedure also covers the responsibilities and requirements for IT representatives and service providers when accessing the ROI's Server Rooms

Scope:

The management of ROI requires that access to ROI 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 IT Representatives who have access to ROI's server rooms.

Procedure:

Approval

The Chief Information Officer, Associate Director Infrastructure Services or the IT Security Manager may grant or revoke access to the ROI's IT Server Rooms.

Submitting the Approved Form

All requests for ROI Server Room access must be made using the Server Room Access Request form.

The approved, form should be submitted to IT Business Services in person or via email to itoffice@roi.com

Responsibilities

1. IT Business Services will ensure that the **Server Room Access Request Form** has been completed and approved in accordance with this procedure.
2. IT Business Services will arrange for access to be added to the Employee ID card for the time period specified on the approved form.



Server Room Access Procedure

3. If the person making the request does not have an Employee ID card, IT Business Services will issue a temporary IT Visitor card with the access privileges for the time period specified on the approved form.
4. IT Business Services will confirm, in writing via email, to the ROI Representative that access has been added to their Employee ID card or IT Business Services will, in writing via email, request the ROI Representative to collect the IT Visitor Card and sign for the collection on the space provided on the approved IT Server Room Access Request Form.
5. The ROI Representative must return the IT Visitor Card to IT Business Services upon expiration of the time period specified on the approved IT 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 ROI Representative must sign the IT Server Room Access Request form, lodged with IT Business Services, indicating the return.
6. ROI Representatives must use their Employee ID card to access the IT Server Rooms whenever card access is operational.
7. An IT Server Room key is available to approved IT staff via the IT Keywatcher system. The key will only be used if card access is not available.
8. Keys to IT server rooms will only be issued under special circumstances and requested via the IT Server Room Access Request form and approved by the Chief Information Officer, Associate Director Infrastructure Services or IT Security Manager.
9. IT Business Services will request, in writing via email, the ROI Representative to collect the IT 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.
10. The ROI Representative must return the key to IT Business Services upon expiration of the time period specified on the approved IT 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 ROI Representative must sign the ITD Server Room Access Request form, lodged with IT Business Services, indicating the return.



Server Room Access Procedure

11. ROI Representatives holding keys to any of the IT Server Rooms must ensure the keys are kept in a secure, locked location when not in use. It is the ROI Representative's responsibility to ensure keys are always secure.
12. ROI Representatives must inform Safety and Security prior to the use of the key if a key is to be used to access the IT Server Rooms. The IT Security Manager must also be informed via email to it-security@roi.com outlining the reason for accessing the IT server rooms via a key and include the date, time and duration of the access.
13. Any ROI Representatives who become aware of or suspect there may have been unauthorised access to an IT Server Room must inform the IT Security Manager via email to it-security@roi.com . Please include the location, date and time of the event.
14. Any ROI Representatives who discover or become aware of a weakness in the security controls for any of the IT 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@roi.com.
15. IT Business Services will provide a copy of these procedures to the IT Representatives with the ITD Server Access Request form.

Authority and Compliance

1. The Procedure Administrator, the Chief Information Officer makes these procedures.
2. IT Representatives must observe these Procedures in relation to Business matters.
3. This Procedure operates as and from the Effective Date.
4. Previous Procedures relating to IT Server Room Access are replaced and have no further operation from the Effective Date of this new Procedure.

Definitions

- Approved - means authorised by the Director IT, the Associate Director (Infrastructure) or the IT Security Manager.
- IT Server Rooms - means the server rooms maintained by the Information Technology Department and includes the IT building server rooms and the Booth Block basement PABX room.



Server Room Access Procedure

- Effective Date is the date on which this Rule will take effect.
- Procedure Administrator is the Director, Information Technology.
- ROI Representative means an ROI employee (casual, fixed term and permanent) contractor, agent, appointee, and any other person engaged by ROI to undertake some activity for or on behalf of ROI. It includes corporations and other bodies falling into one or more of these categories.

Related statutes, regulations, and/or policies

- Server room policy
- Work Health and Safety (WHS) rules