ROI Server Room Policy

Purpose:

The purpose of the Server Room Policy is to describe the minimum requirements for designing, installing, securing, monitoring, maintaining, protecting, and decommissioning a server room at the Red Opal Innovations.

Applies to:

Red Opal Innovations employees and other covered individuals (e.g. vendors, service providers, independent contractors, etc.) in their access and usage of ROI resources during the course of conducting business operations (administrative, financial, research, or service).

Policy Statement:

Performing any type of computer technology work in the server room as permitted by ROI management, shall implement and maintain their respective technology services via the approved ROI Server Room Standards only.

Exclusions or special circumstances:

Exceptions to this policy and associated standards shall be allowed only if previously approved by the ROI Information Technology Security Office and such approval documented and verified by the Chief Information Officer.

Consequences:

Employees who violate this policy may be subject to disciplinary action for misconduct and/or performance based on the administrative process appropriate to their employment.

Any other individuals (e.g. vendors, service providers, independent contractors, etc.) may also be subject to the discontinuance of specified information technology services based on policy violation.

Contact:

Server Room Policy

Chief Information Officer

Building 25

Beverly Street,

Sydney 2000 NSW.

Approval information

Approved by:

Chief Information Officer

Approved on:

Tuesday 29th October 2019

Effective on:

Tuesday 29th October 2019

Review cycle:

Annual (or as needed)

Background

The standards associated with this policy are designed to represent the baseline to be used by the Server Rooms located on the Red Opal Innovations main office premises. While specific-standards organisations are referenced for examples of best practices, it should be noted that site conditions, special requirements, and cost of modification will be taken into consideration when implementing the final configuration of a site. The standards will be regularly reviewed and updated based on new industry standards, new technology, and lessons learned.

Related statutes, regulations, and/or policies and procedures

- Server room access procedure
- Work Health and Safety (WHS) rules
- Server room environment requirements
- ROI_Risk_Identification&Control_form

Server room environmental requirements

Maintenance

- Cabling must be maintained in an orderly fashion to reduce the possibility of an accidental outage.
- All network devices must be labelled and mounted on server racks in a secure and orderly manner.
- The equipment and server room should be maintained and kept free of dust.

Temperature control

- The server room must have sufficient temperature control to maintain temperatures within the operational limits defined for the hardware located in the room.
- The server room should have dedicated, redundant air conditioning sufficient to maintain temperatures between 65 and 70 degrees Fahrenheit.
- Fully enclosed racks with built-in cooling may also be used.
- Environmental monitoring should be configured to alert administrators in the event of a cooling failure (i.e., a NetBotz monitoring system that sends text messages; a thermostat with only a local alarm is not sufficient).
- For large rooms, cooling systems and equipment should be installed in a hot aisle / cold aisle configuration to maximize efficiency.
- Procedures should be posted in the room explaining how to respond in the event of a cooling failure.

Power

- The server room should have sufficient dedicated circuits for all equipment, plus one or more additional circuits, as needed for flexibility in the event a circuit fails.
- All systems must be properly grounded.
- Critical systems should be connected to uninterruptable power supplies (UPS) and/or generator power, depending on the business requirements for server uptime.
- Uninterruptable power supplies (UPS) and/or generator power should be tested at least annually and maintained according to manufacturer specifications.

- Based on UPS monitoring thresholds, automatic shutdown features should be configured when feasible to gracefully shutdown and protect systems prior to power loss.
- Large rooms should have a clearly-labeled emergency power-off switch.
- Procedures should be posted in the room explaining how to respond in the event of a power failure.
- Server rooms should have emergency lighting to provide for life safety in the event of a power outage.

Fire / Flood

- The server room must have some form of fire detection and suppression, adequately maintained and routinely tested.
- Server rooms must be reasonably free of fire hazards such as boxes, papers, etc.
- Each server room may have an easily visible and accessible clean-agent fire extinguisher. A standard “ABC” fire extinguisher is not recommended for use around electronic equipment.
- If the server room is located near potential leak hazards (AC condensers, overhead water lines, sprinklers, kitchens, break rooms, restrooms, etc.) sufficient steps should be taken to protect systems, such as racks with solid tops, systems elevated off the floor, etc. Moisture sensors should be used in areas where leaks are most likely or would be most problematic.

Server Cabinets Cleaning Procedure

- Clean/ wipe inside and outside of all cabinet doors, include cabinet tops.
- Clean inside of server cabinet floor (if accessible).
- Clean/ wipe the bottom of all tiles that cannot be removed (server cabinet area).
- Clean/ wipe inside & outside of all cabinet doors, include cabinet tops
- Clean inside of server cabinet floor (if accessible)

Hazard identification and risk control guidelines

Technicians who are authorised to work in ROI server room environment should check the environment for potential hazards.

Anyl identified hazards in a server room environment should be documented using the ***ROI_Risk_Identification&Control_form.docx*** along with any recommended risk control measures.

The risk control measures should then be approved by the server room manager/supervisor before implementation of the control measure.

Guidelines for record keeping and storing of essential documents

A **Network Records Register** will be maintained to record and store all essential design and installation information

The **Network Records Register** – This register will record the following details on all essential documentation that are created during the design and maintenance of the ROI network infrastructure.

- Name of document
- Location where the document is store
- Summary of what the document contains
- Size of the document (in MB)
- Number of pages
- Date of creation
- Name of person who created the document
- Last updated date
- Name of person who updated the document
- Reasons for latest update

Legal obligations

Employer and business obligations:

https://www.safework.nsw.gov.au/legal-obligations/employer-business-obligations

Visitor obligations:

https://www.safework.nsw.gov.au/legal-obligations/visitor-obligations

Contractors and labour-hire:

https://www.safework.nsw.gov.au/legal-obligations/contractors-and-labour-hire

Legislation

https://www.safework.nsw.gov.au/your-industry/information-media-and-telecommunications

Codes of practice

https://www.safework.nsw.gov.au/resource-library/list-of-all-codes-of-practice

Standards Organizations:

- ANSI: American National Standards Institute
- TIA: Telecommunications Industry Association
- BS/IEC/EN: British National Standard/International Electrical Commission/European Standards.
- EIA: Electrical Industry Alliance
- IEEE: Institute of Electrical and Electronics Engineers
- ISO: International Organization for Standardization