RDC Existing Server User Agreement (UA)

Effective Date February 2017

Purpose/Objective

This document outlines the general terms, support provided, and acceptable usage of the Research Data Center (RDC) at Idaho State University. The purpose of this document is to establish:

1. A clear representation of the capabilities of the RDC.
2. The acceptable use of the RDC.
3. A shared set of expectations regarding the operation and support.
4. A framework for bidirectional communication regarding operational issues and overall satisfaction with the services provided.

A separate UA is required for each existing server/cluster moved into the RDC environment.

Service Cost

The RDC currently provides rack/floor space free of charge to faculty and other members of the University research community, but reserves the right to review and change this agreement as needed. Changes to this agreement are subject to the approval of the Vice President for Research.

Service Description

The RDC currently has available rack space and floor space for new server racks. The RDC designated two environments in which all servers operate; one for projects that involve data that is regulated and/or sensitive in nature such as Protected Health Information (PHI) and requires a more secure/compliant environment. This system is referred to as the Protected Environment (PE). A second system is for all other projects and is referred to as the Standard Environment (SE).

RDC Provides

1. Additional software installation as per agreement with VM owner. However, this is typically done by the PI's systems administrator.
2. Secure physical infrastructure located at the Research Data Center.
3. Redundant power through backup/uninterruptible power supplies.
4. Static IP address (addresses) using IPv4 and/or IPv6.
5. Firewall protection.

Acceptable Use of VM

The RDC is available to support ISU research purposes. All RDC existing server requests must come from the PI of the research project. The PI and all users must have a valid ISU user's account. The PI will meet with RDC personnel to discuss the project in order to determine if the project is a good fit for an RDC. If it is found that the project is a good fit, the PI will coordinate with RDC personnel to setup access times in which the PI can move equipment into the RDC and setup/configure this equipment. Prior to this, the following criteria must be met:

1. The server must be running a current/supported OS that is fully-patched. Furthermore, the server must be configured to update software patches following an automated schedule that does not exceed one (1) week in the deployment of security patches. RDC personnel will work with the researcher to determine and implement the appropriate security model (RDC administered, shared administration, or self-administered).
2. The server must be running university approved anti-virus software.

It is the customer's responsibility to protect sensitive information in accordance with Idaho State University Information Security policies[1]. Under no circumstances will any protected data be placed in the standard environment (SE).

Customer/User Responsibilities

1. Provide current contact information.
2. Provide necessary network configuration information.
3. Provide a list of software used on the server.
4. Prompt reporting to the RDC of issues and/or changes to services.
5. Provide account maintenance for any application level user accounts.
6. Respond in a timely manner to all security concerns.
7. Data backup/archiving
8. The researcher is responsible for all system administration of their Server and is required to keep the OS updated.
9. For a PE server, all users will complete the University's HIPAA training, and keep this training current. Users also agree to any other future compliance requirements.

RDC Responsibilities

1. Provide key contacts to coordinate communication, incident management, and problem management processes.
2. Assist in protecting private or sensitive information in accordance with Idaho State University Information Security policies
3. Publish planned maintenance windows
4. Adhere to maintenance windows for infrastructure changes.
5. Maintain data center physical and virtual security.
6. Provide appropriate notification to customers for all scheduled maintenance, unscheduled down times, or times of service degradation.
7. Provide an estimated timeline for the provisioning of new server space.

RDC Hours of Operation and contact information
Phone: 208.282.6078 (during normal University Working Hours)
E-mail: RDC@isu.edu

Normal RDC business hours are Monday-Friday 8AM-5PM, except on University holidays and closed days. RDC personnel strive to acknowledge the receipt of messages submitted to the issue tracking system within three hours during these business hours.

Signature Line(s)

____

(Principal Investigator making request)

Acknowledgements: this document is based upon user agreements from the University of Utah.

[1] See http://www2.isu.edu/policy/ for access to all policy documents.
Policies regarding information technology are available at http://www2.isu.edu/policy/2000/index.shtml (cf. policies 2400-2520 as well as policy 2280).
HIPAA policies are available at http://www2.isu.edu/policy/10000/ (cf. policies 10010-10600).
Export control policies are available at http://www2.isu.edu/policy/7000/index.shtml (cf. policy 7040)