The UCT Research Data Store (RDS)

Version 1.2 – Last Updated on 13/05/2025

This document serves as documentation for users and prospective users of UCT's Research Data Store (RDS). It includes information on setting up an RDS share on a computer, UCT's data infrastructure, as well as security and security management. Version Control Information is included below. Any further queries to be directed to eResearch (eresearch@uct.ac.za) or through a SNOW eResearch Request: https://uct.service-now.com/sp?id=sc_cat_item&sys_id=5b6e6a80db276b4009b807f2ca9619f2

ABOUT UCT'S RESEARCH DATA STORE (RDS)

UCT offers secure on-site data storage for researchers with the Research Data Store (RDS). It is a secure, scalable, reliable and resilient storage facility for research data which is accessed with a network drive (SMB) across the UCT network or remotely through a VPN.

The RDS server infrastructure is stored in the Upper Campus Data Centre (UCDC) - a secure, biometrically controlled on-premises data centre. The total capacity of the RDS is approximately 3.5 petabytes (PB).

YOUR RDS SHARE

Allocation of RDS shares

After initial consultations with an eResearch analyst, a share or partition will be provisioned. Once quotations have been generated, an invoice for an upfront payment will be sent, and once payment has been made, the share will be created. The path to the allocated share will look like this:

\\resesearchdata.uct.ac.za\YourShareName
OR
\\researchdata2.uct.ac.za\YourShareName

YourShareName should be replaced with the name of your share as provisioned.

Folder Structure, Access and Permissions

At the outset of configuring a share on the RDS, the Data Owner (usually a Principal Investigator) will work with an eResearch Technical Specialist to set up the folder structure and access permissions. Access to the RDS is preserved using UCT's identity and access credentials.

Only members specified by the Data Owner are granted access to the share. Permissions are defined as per the requirements (READ ONLY or READ & WRITE) set out by the Data Owner. The folder structure and access permissions can be as simple or as complex as necessary, depending on data sensitivity etc. If all users will have equal access (READ & WRITE) to all folders, then a simple list of users of users will suffice. If the folder structure is more complex, then the Data Owner will be requested to complete a Folder Structure and Permissions (https://uct.ac.za/sites/default/files/media/documents/uct_ac_za/68/rds-folder-structure-and-permissions.xlsx) document, which will be the template that guides the setup of the share.

Collaborators need to have UCT credentials to gain access to the RDS. If external collaborators need to be included, they will need to obtain UCT third party access. Third party access can be arranged through https://thirdparty.uct.ac.za/.

Accessing the RDS

Permanently mapping a drive to your RDS share is a straightforward process. You need to be logged in to the server (either on the network or via the VPN) in order to map the network drive to your RDS share.

** Auditing and Dashboard are not currently available at the moment. Auditing information is discretionary if the drive is mapped in Windows.*

Windows

In **Start**, select **File Explorer**
Select **Map network drive**
Specify the folder: **\\researchdata.uct.ac.za\YourShareName**
Click **Finish**
In dialogue box, enter your UCT credentials (01416666@wf.uct.ac.za)
Click **OK**

MacOS

In **Finder**, select **Go**, then **Connect to Server**
In the dialogue box, enter: **smb://researchdata.uct.ac.za/YourShareName**
(this can be saved to favourites)
Click **Connect**
In the dialogue box, enter your UCT credentials (01416666@wf.uct.ac.za)
Click **Connect**

Linux

Use the following to mount your RDS share:

Use an entry in /etc/fstab

//researchdata(2).uct.ac.za/YourShareName /mnt/YourShareName cifs user,uid=<UID>gid=<GID>,rw,credentials=/home/<staffID>/.smbcreds,(no)auto 0 0

contents of /home/<staffID>/.smbcreds

username=<staffID>
password=<myStrongPassword>

The share would be mounted automatically at boot time if using credentials=/home/<staffID>/.smbcreds,auto 0 0

For a manual process change auto to noauto as indicated and then use the command sudo mount /mnt/YourShareName

Alternatively, for users with a Linux workstation with a GUI:

Use GNOME File Explorer
Connect using: smb://researchdata.uct.ac.za/YourShareName
Login as: <staffID>@wf.uct.ac.za

Accessing the RDS from off-campus

All external access to UCT services and resources are blocked by the UCT perimeter firewall, and the RDS can be securely accessed over the internet via the UCT VPN solution. Secure access to data stored in the RDS via the VPN makes is possible to access from anywhere in the world. Each partition in the RDS is user-controlled, with permissions for access specified by the Data Owner.

Information about installing UCT's VPN, Cisco AnyConnect can be found here: https://icts.uct.ac.za/services-working-remotely/virtual-private-network

Data Transfer

Transferring data securely is paramount in safeguarding sensitive information and maintaining the integrity of research endeavours. Making use of a secure and reliable data transfer method ensures that research data remains confidential and protected from unauthorised access or interception.

One approach to secure data transfer is by employing encryption protocols, such as SSL/TLS, which encrypts data during transmission, making it unreadable to anyone without the decryption key. Additionally, implementing secure file transfer protocols like SFTP or SCP adds an extra layer of protection by ensuring data is transferred over a secure connection.

When transferring research data to your RDS share from another system, we recommend using a secure application like Globus - https://app.globus.org/. Login to the Globus web app with your UCT credentials.

If you are uncertain about transferring your data to the RDS or have complex data transfer requirements, consult with an eResearch analyst for guidance to ensure that data transfer methods align with best practices and compliance standards.

Storage Capacity

Storage allocation can easily be increased or decreased as required. Storage is allocated and costed on a per-TB basis.

DATA CENTRE INFRASTRUCTURE

The data centre has redundant power feeds from separate distribution boards, supported by redundant UPS power. There is also redundant generator power available. Secure access to the data centres is via biometric control and only to designated ICTS personnel.

Data is protected by an archiving solution which is written to tape and stored at an off-site vaulting company with premises in Cape Town Northern suburbs.

The data are currently stored on Dell storage arrays hosted in the highly secure UCDC. Migration to new storage hardware, NetApp, is in progress and will be completed mid-2024.

PHYSICAL SECURITY MANAGEMENT

The UCDC is extremely secure from physical risks:

- **Locked Server room:** Secured Data Centre with restricted and/or escorted access only. Unrestricted access allowed only to a closed controlled group of UCT staff using proximity reader and biometric access control locks.
- **Secured Power Supply:** Server racks powered by e-PDU's supplied by dual UPS with dual, independent emergency diesel power generators as backup for utility electrical supply.
- **Controlled Environment:** Servers are housed in a closed, filtered, temperature and humidity-controlled environment.
- **Theft and Malicious Damage:** Data Centres entrances are monitored by CCTV and have burglar alarms monitored by the UCT 24/7 Security centre. Internal CCTV monitored by ICTS only.
- **Hazard Control - Fire Alarms:** Data Centres are fitted with heat and smoke or aspirating smoke detector systems linked to the UCT 24/7 monitored security centre and the data centre BMS (building management system) system.
- **Hazard Control - Fire Response:** Data Centres are fitted with automated flood gas fire suppression system (Inergen gas fire system and/or HFC227/MP200) with automated and/or controlled power and HVAC shunt.
- **Hazard Control - Water:** Flood/water ingress sensors are linked to the (BMS) automated environmental monitoring system.

NETWORK SECURITY

UCT's network perimeter and data centres are protected and secured Cisco Firepower 9300, a robust and highly scalable security appliance designed for advanced threat protection and firewall capabilities. It provides:

- High-performance threat prevention and application control capabilities.
- Scalability to meet the demands of large and distributed networks.
- Advanced threat detection and response features, including intrusion prevention, malware protection, and URL filtering.
- Integration with Cisco's Security Intelligence Operations (SIO) for real-time threat intelligence updates.
- Simplified management through Cisco Firepower Management Center (FMC), providing centralized policy management and advanced analytics.

Additionally, for network monitoring, UCT utilises Cisco Prime Infrastructure, which offers:

- Comprehensive network lifecycle management, including device provisioning, monitoring, troubleshooting, and optimization.
- End-to-end visibility across the entire network infrastructure, including wired and wireless devices.
- Automated configuration management and compliance checks to ensure network consistency and security.
- Performance monitoring and reporting to identify and address potential issues before they impact operations.
- Integration with other Cisco network management solutions for enhanced functionality and workflow automation.

UCT's Anti-Virus Policy (https://icts.uct.ac.za/services-security-securing-your-device-anti-virus/uct-anti-virus-policy) states that "all devices connected to the UCT network or networked resources shall have anti-virus software installed and configured so that the virus definition files are current, routinely and automatically updated".

All UCT-owned servers and computers are centrally managed by the enterprise Trellix (formerly McAfee) ePolicy Orchestrator (ePO) antivirus system. Trellix ePO antivirus system deploys daily scheduled antivirus updates to all computers on the network.

All windows computers and servers receive scheduled monthly updates via the Microsoft Windows Server Update Services (WSUS) system for security updates and patches. MacOS and Linux-based computers can receive updates either from Apple macOS or Linux update services (and for local update server configurations, clients must be set up to obtain updates locally) otherwise, they will receive updates from the default external servers.

***Note** this may not include *all* devices connected to the UCT network as BYOD (personal devices used to connect to UCT's network by staff and students) may have their own anti-virus installed, and it is impossible to monitor and regulate personal devices.

Access to UCT resources such as websites, file systems, RDS shares, servers and desktops are via secure UCT Active Directory credentials as stipulated in the UCT Information Security Policy (https://icts.uct.ac.za/media/10766).

COMPUTER SECURITY INCIDENT RESPONSE TEAM (CSIRT)

UCT has a defined process for management of incidents and events, including those that may pose a threat to the security or integrity of data. There are processes in place for the management of vulnerabilities and threats including mitigation, minimisation, defences, and controls. This includes regular testing including vulnerability and penetration testing.

The CSIRT is responsible for protecting the UCT network, its digital assets and your information. Coordination of information and cyber security incident and event management is handled by them. More information can be found on https://csirt.uct.ac.za/

The CSIRT:

- responds to, controls and manages computer security incidents, and facilitates a speedy and safe resolution;
- ensures the timely investigation and assessment of security incidents;
- ensures a return to normal operating conditions on the UCT network should it in any way be affected by a security incident;
- speedily notifies the UCT senior leadership in case of serious security incidents;
- manages potential risks on campus and prevent the recurrence of incidents;
- provides education and advice on reporting and avoiding risks, and
- announces potential vulnerabilities and threats to hardware and software on campus.

OPERATIONAL MAINTENANCE

Monitoring

The entire UCT computing infrastructure is monitored with continuous operational availability every hour of every day throughout the year by various monitoring and management systems, including:

- Dell OpenManage System;
- Microsoft System Centre Operations Manager (SCOM);
- CiscoPrime; and
- UCT's SIEM (security information and event management) tool.

Server hardware, virtual servers and the storage platform are monitored via Dell OpenManage System and SCOM. The network infrastructure is monitored via CiscoPrime.

System Maintenance and Patching

UCT Information Communication Technology Department (ICTS) has scheduled monthly maintenance slots during which times system and infrastructure maintenance are performed. Windows Servers are updated via a controlled process via the Windows Server Update Services (WSUS) system. The process involves thorough testing of updates prior to deployment to productions servers during the maintenance slot. The SCCM (System Configuration Manager) is used to deploy Widows patches to servers.

Incident Management

Each incident should be logged on ServiceNow, mentioning the problem, the date, description, error messages and screenshots. An eResearch Request can be logged with ServiceNow https://uct.service-now.com/sp?id=sc_cat_item&sys_id=5b6e6a80db276b4009b807f2ca9619f2 or by emailing eresearch@uct.ac.za.

DISASTER RISK MITIGATION

Active Data Centres

- UCT runs an active-active data centre environment spread across the Upper Campus Data Centre and the Bremner Data Centre from where compute and data services are provided to campus. In this environment, both data centres are actively serving requests and processing data simultaneously. This configuration is designed to provide redundancy and high availability.
- Backup infrastructure is located in the Bremner Data Centre.
- Bremner Data Centre is the standby Data Centre, and the services can be provided from this location.
- Switching services from the Upper Campus Data Centre to the Bremner Data Centres is seamless – as the application and its associated database are installed on Virtual Machines which are configured for high-availability.

Backup and Recovery Strategy

- All VMware virtual servers are backed up using the Veeam Backup and Replication v10 software on a nightly basis.
- The Veeam Backup and Replication servers are hosted in the Bremner Data Centre.
- The Veeam Backup and Replication repositories are hosted in the Bremner Data Centre (augmenting with Storage Grid, an on-prem object storage solution with ability to store immutable backups).
- Thirty (30) restore points are kept per server, which allows for a restore window of 30 days.
- Research data is protected by the archival solution and tapes sent to the off-site vaulting company

VERSION CONTROL

Version	Purpose/change	Author/s	Date
0.1	Creation of doc, collating info from older docs	Sarah Schäfer	7/2/2024
0.2	Updating security notes based on Randolph	Sarah Schäfer	26/2/2024
0.3	Confirming backup and systems info, data transfer	Sarah Schäfer	11/3/2024
0.4	Third party info	Sarah Schäfer	14/3/2024
0.5	Checks	Sarah Schäfer, Mattia Vaccari, Heine de Jager, Tim Carr	5/4/2024
1.0	Saved as PDF, uploaded to https://uct.ac.za/eresearch/research_data_storage	Sarah Schäfer	11/04/2024
1.1	Updated link, saved as PDF, uploaded to https://uct.ac.za/eresearch/research_data_storage	Sarah Schäfer	30/08/2024
1.2	Updated LINUX access information	Sarah Schäfer	13/05/2025