Waipapa Taumata Rau
University of Auckland

ResBaz
RESEARCH BAZAAR

Five Safes in Action

A tour of a Secure Research Environment

July 2026

Yvette Wharton, Dr Toby Johnson, Dr Sarah Hopkins
Centre for eResearch

Five Safes in Action: A Tour of SRE

By the end of this session, participants will:

- Understand the Five Safes framework
- Recognise how the Five Safes are implemented in a Secure Research Environment (SRE)
- Understand typical researcher responsibilities and actions
- Identify when a SRE may be appropriate for their projects

 researchdata@auckland.ac.nz

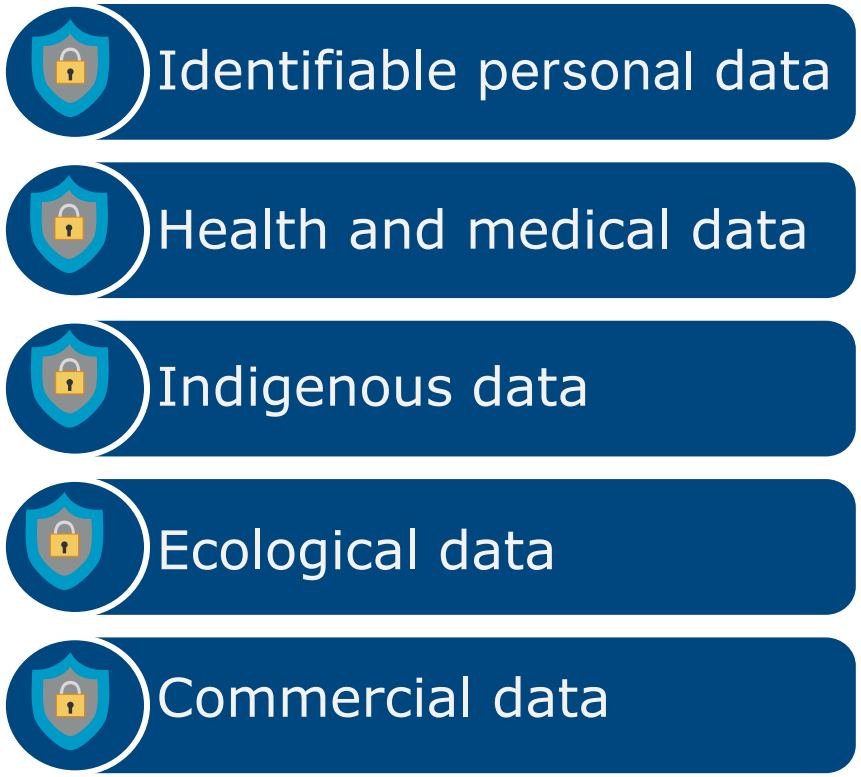
Overview of this session

Duration	Section	Topics covered
5 mins	Introduction	Welcome and outline
5 mins	Why Secure Research Environments Matter	Growing use of sensitive research data Data security classification Common considerations for sensitive data
10 mins	Five Safes Framework	The Five Safes at a glance Data security principles and controls Intro to the Secure Research Environment
30 mins	A Research Project Journey Through a SRE	Planning the project Getting access Preparing and managing data Working in the environment Publishing results
10 mins	Wrap up and Q&A	

What research data needs protection?

Growing use of sensitive, personal and linked data in research

Sensitive data can include:



IMPORTANT

Sensitive data is commonly subject to legal and ethical obligations describing how it can be accessed, used & handled.

Use the research examples in the Data Classification standard to help you to determine whether you are working with sensitive data.

Data security classification

PUBLIC	INTERNAL	SENSITIVE	RESTRICTED

- Considers damage or harm to people and the reputation of the University
- Helps you to:
  - Meet requirements
    (e.g., a DMP is required if working with sensitive or restricted data)
  - Identify systems/controls
    (e.g., what software or storage services are available if I am working with sensitive data?)

Examples:

- require **human ethics approval**, incl. personal information and de-identified health data
- require animal **ethics approval**
- are **commercially sensitive**
- may be protected as **intellectual property**
- are subject to **export controls**
- are part of **national defence**

https://www.auckland.ac.nz/en/about-us/about-the-university/the-university/data-governance/data-classification-standard.html

Common considerations for sensitive data

Privacy

- Ensuring participants cannot be identified or harmed through inappropriate access, sharing or publication
- **Linked** data, clinical data

Ethics

- Data use and confidentiality is appropriate, proportionate and aligned with participant expectations
- Research involving **Māori data** should consider Māori data sovereignty

Data providers

- Often impose specific requirements (e.g. security controls, data use/sharing agreements) to protect sensitive data
- Accessing **government or health** data

Collaborations

- Approved researchers in different locations and or countries need to work together without creating copies of sensitive data on multiple laptops, servers, or cloud storage platforms

Five Safes framework

Decision-making framework to help researchers decide how to share data safely

- **Safe people:** Who can access the data? Do they have the right training and knowledge?
- **Safe project:** Is the use of the data appropriate?
- **Safe settings:** Where will the data be accessed?
- **Safe data:** How is risk reduced within the data itself?
- **Safe output:** What can be published or released?

https://www.stats.govt.nz/integrated-data/how-we-keep-integrated-data-safe/

Principles of data security

The CIA Triad = three core principles of data security

Principle	What is it?	Example
Confidentiality	Only authorised people can access data	Restricting access to identifiable data
Integrity	Data is accurate and complete, not altered improperly	Preventing accidental overwriting of datasets
Availability	Data is accessible when needed	Backups ensure data isn't lost

Good security balances protection and usability

Security controls

Encryption	Access Controls	Authentication	Audit & Monitoring
• Protects data if stolen or intercepted • **At rest** (stored files, drives) • **In transit** (email, uploads, downloads)	• Limit data access to **those who need it** • Role-based access	• Verifies user identity • Strong passwords + multi-factor authentication (MFA) • Role-based access	• Track who accessed or changed data • Helps detect and investigate issues
Using FileSender to share data/files	Restrict access to identifiable data	Institutional SSO + MFA	System logs of file access

Secure research environment (SRE)

Project-specific virtual platform for the secure storage and analysis of sensitive data.

Security

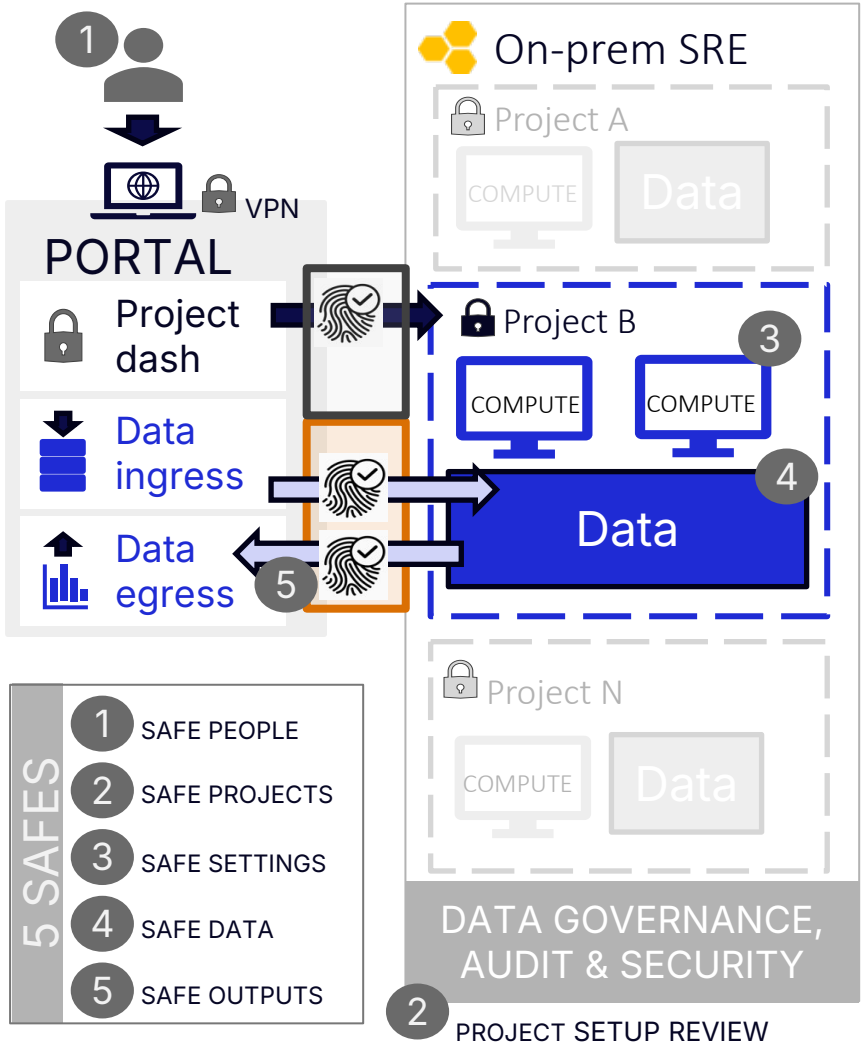
- Controlled access for authorised people
- Project data is encrypted
- Auditable data import, export and access

Collaboration

- Shared workspace for a project with data and analytical tools in one place

Compliance

- University approved for sensitive data
- Aligned with University security and governance standards



Research resources [Secure Research Environment (SRE)]

A Research Project Journey
Through a Secure Research Environment

A research project journey through a SRE

Researchers are collaborating on a funded research project:

- Principal Investigator, University of Auckland
- Clinical Lead, Health Organisation
- Biostatistician, University in Australia

The study aims to identify **social, demographic and behavioural factors** associated with **better disease management** and **reduced hospitalisations** among people living with **Type 2 diabetes**.

*__Disclaimer__: This is a fictional project developed solely to demonstrate the use of a secure research environment across the project lifecycle. The processes described are for illustrative purposes and are **not** intended as a project template or exemplar.

What data do they need?

The project requires access to multiple sensitive datasets:

🗂️ Clinical health data

- Hospital admissions, ED presentations, outpatient appointments, diagnoses, medications, laboratory test results (e.g. HbA1c)

📊 Self-reported survey data

- Health behaviours, mental wellbeing measures, health literacy, experience of healthcare services

👥 Demographic (identifiable) data

- Age, sex/gender, ethnicity, geographic region, socio-economic factors

Case Study: Data requirements

The data provider requires that:

- Clinical health data are held and accessed within a controlled environment
- Linked datasets cannot be downloaded to personal computers
- International collaborators access data through approved secure infrastructure that remains in NZ
- All outputs undergo disclosure review before release

Planning the Project

Access to sensitive data is based on a justified and approved use case

Safe Projects

- Research purpose demonstrated public benefit
- Data management decisions documented in a data management plan (DMP)
- Costs for SRE included in funding budget
- Ethics approval and data access applications include description of SRE to hold and access sensitive data

Getting Access

Trustworthy research relies on accountable researchers

Safe People

- Project team vetting
- Training requirements
- Managing external collaborations
- User agreements and responsibilities
- User access roles and groups

Project team

	Name	Role(s)
	**Principal investigator**	Leads project, approves project team Obtains ethics & governance approvals
	**Clinical lead**	Liaises with health data provider Reviews outputs before release Verifies that data use complies with approval conditions
	**Biostatistician** (overseas)	Conducts primary statistical analyses Creates analytical datasets, reports, visualisations
	**Data manager**	Responsible for data and linkage quality Manages project folders and file organisation
	**PhD student** (Wellbeing/literacy)	Examines survey responses & health literacy outcomes Access only to variables needed for thesis work
	**Research assistant**	Recruit participants, manage consent Administer surveys and follow-ups

Data use agreements and collaborations

Access to sensitive data is usually governed by agreements

	Data Use Agreement (DUA)	Data Sharing Agreement (DSA)
Purpose	Controls how you *use* data	Controls how data is *shared between organisations*
In this project	Accessing clinical data (e.g. Health NZ data)	Active collaboration or transfer between organisations

Five Safes helps us decide what conditions are needed

	Include in agreements...
Safe people	Who is allowed access
Safe projects	What the data can be used for
Safe settings	Where data can be accessed
Safe outputs	Publication restrictions

Research resources Research data / Research data policies ... / Data-sharing agreements

Researcher onboarding

Project team members all have credentials, experience and training required to safely handle project data

All members of the project team need to complete:

- Privacy, confidentiality and sensitive data handling training
- Data access agreements
- Security and project-specific onboarding/training

Preparing sensitive data

The safest data is the minimum data necessary to answer the research question

Safe Data

- Access only necessary datasets/variables
- Data minimization, de-identification
- Protecting highly sensitive information

Working in the Environment

The environment protects data while enabling research collaboration

Safe Settings

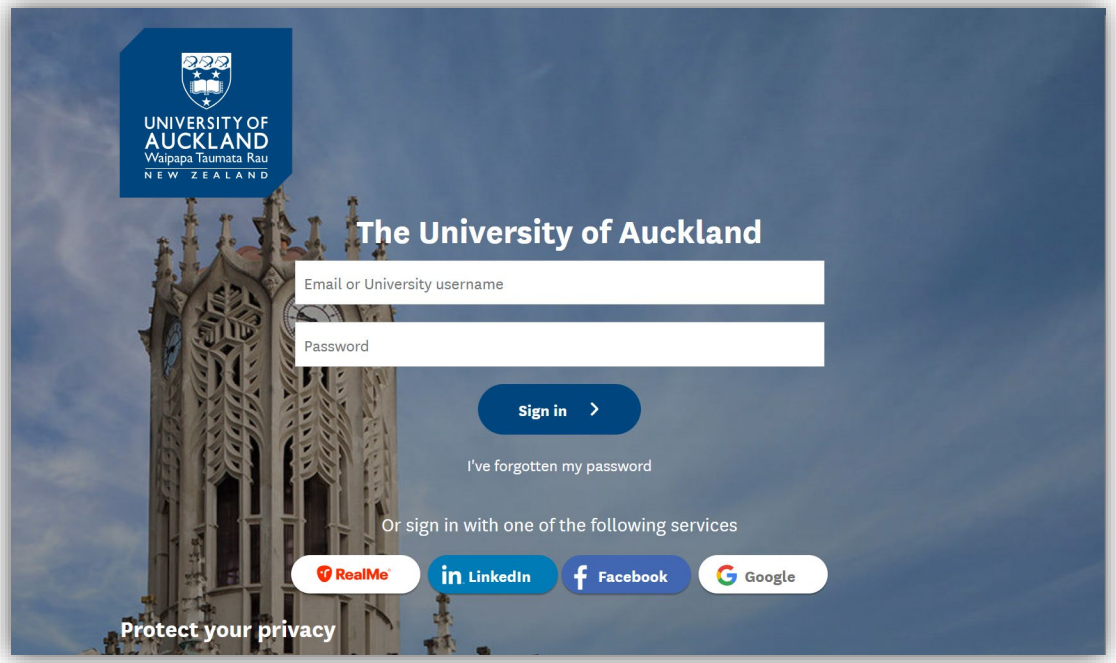
- Controlled access and role-based actions
- Multi-factor authentication
- Secure virtual desktops
- Restrictions on download, copy
- Activity logging and monitoring

SRE

Controlled access and authentication

http://www.sre.auckland.ac.nz/

1. Sign in with username and password



2. Enter two-factor authentication code

Enhanced session security

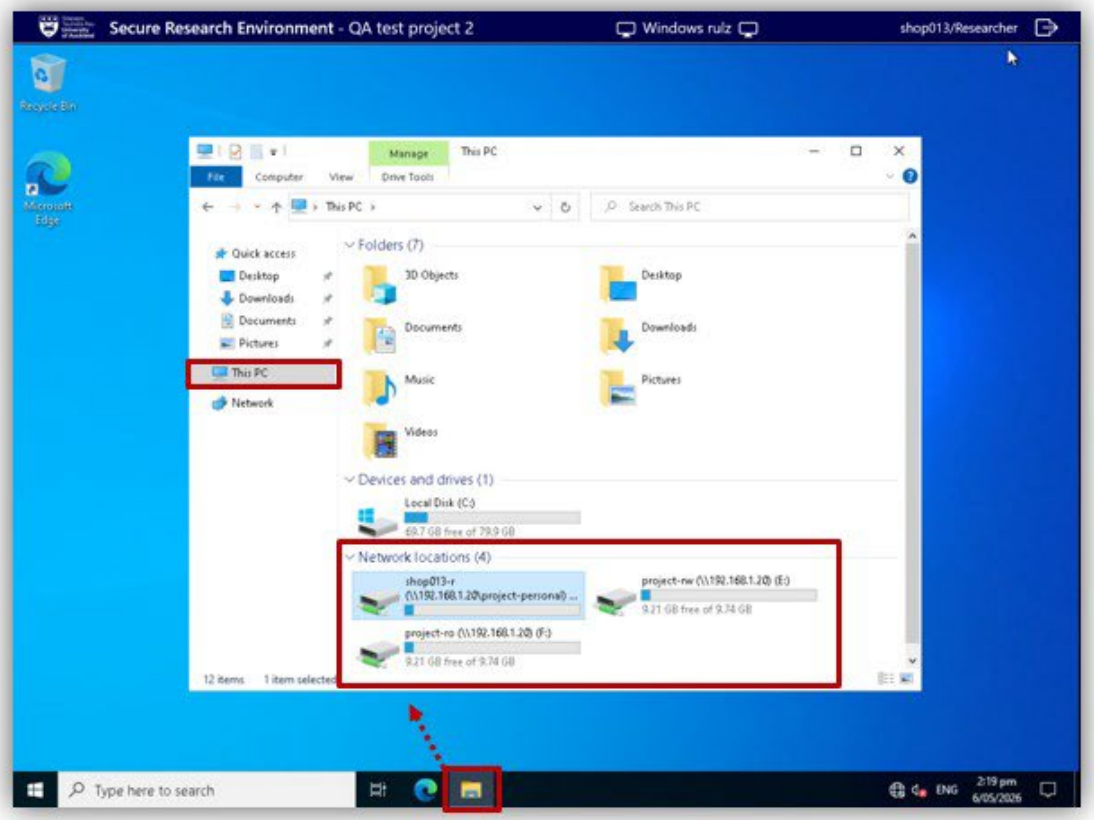
- Logged out of the SRE environment after 15min of inactivity
- Virtual desktop (VM) connection will be closed after 10min of inactivity
- If logged out, user will be prompted to log in and re-enter two-factor authentication (2fa) to continue

SRE

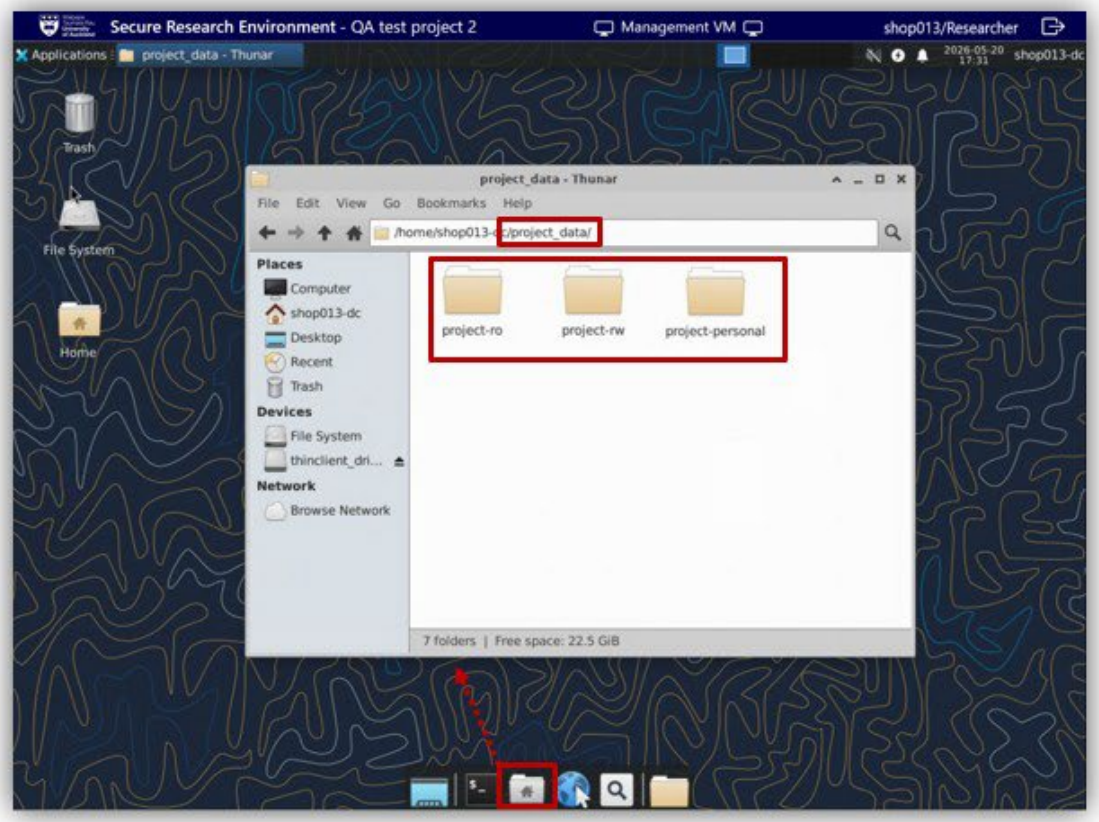
Secure virtual desktops

A virtual desktop (or virtual machine, VM) is a version of a computer that can be accessed from multiple devices and locations through a web browser.

2 Windows VM



Linux VM



Role-based access to SRE

Role-based controlled access and rights based on project needs

Role	Ingress	Egress	VM Access	Manage Users
Data Custodian	Direct	Direct	✅	✅
Researcher	Request	Request	✅	❌
Ingress Approver	Approve	❌	✅	❌
Egress Approver	❌	Approve	✅	❌

- Each role can be held by one or more project team members.
- A project team member can hold more than one role.

Project tasks

The Principal Investigator works with the SRE team to assign roles to project members and set up the project environment.

Professor Dataworth decides who needs access to the SRE and which access roles should be assigned to these project members.

Project team assigned SRE access roles

	Name	SRE role and access
	**Principal investigator** Prof Duckworth	--
	**Clinical lead** Dr Hoppy	**Data Custodian** **Egress Approver** Full access to linked data
	**Biostatistician** (overseas) Dr Stan Dardeviation	**Researcher** Full access to linked data
	**Data manager** Dexter Dataset	**Data Custodian** **Ingress Approver**
	**PhD student** (Wellbeing/literacy) Sarah	**Researcher** Access to data subset
	**Research assistant**	--

Project tasks

Sarah, the PhD student, wants to import the survey datasets into the Secure Research Environment

Sarah Surveyor creates an **Ingress Request** to import the data.

The **Data Manager** uses the **Ingress Approver** role to check and approve the files that Sarah wants to import into the project environment.

Project tasks

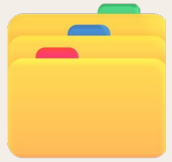
Dr Hoppy, the Clinical Lead, is asked to import the clinical datasets into the Secure Research Environment.

Dr Hoppy uses an **Ingress Request** to import the data.

They use the **Data Custodian** role, which means they can ingress data and files directly into the SRE without requiring approval from the ingress approver.

Project tasks

The Data Manager wants to ensure that project data and files are secure stored with appropriate access controls before cleaning data and managing linkage processes to create analysis-ready datasets.



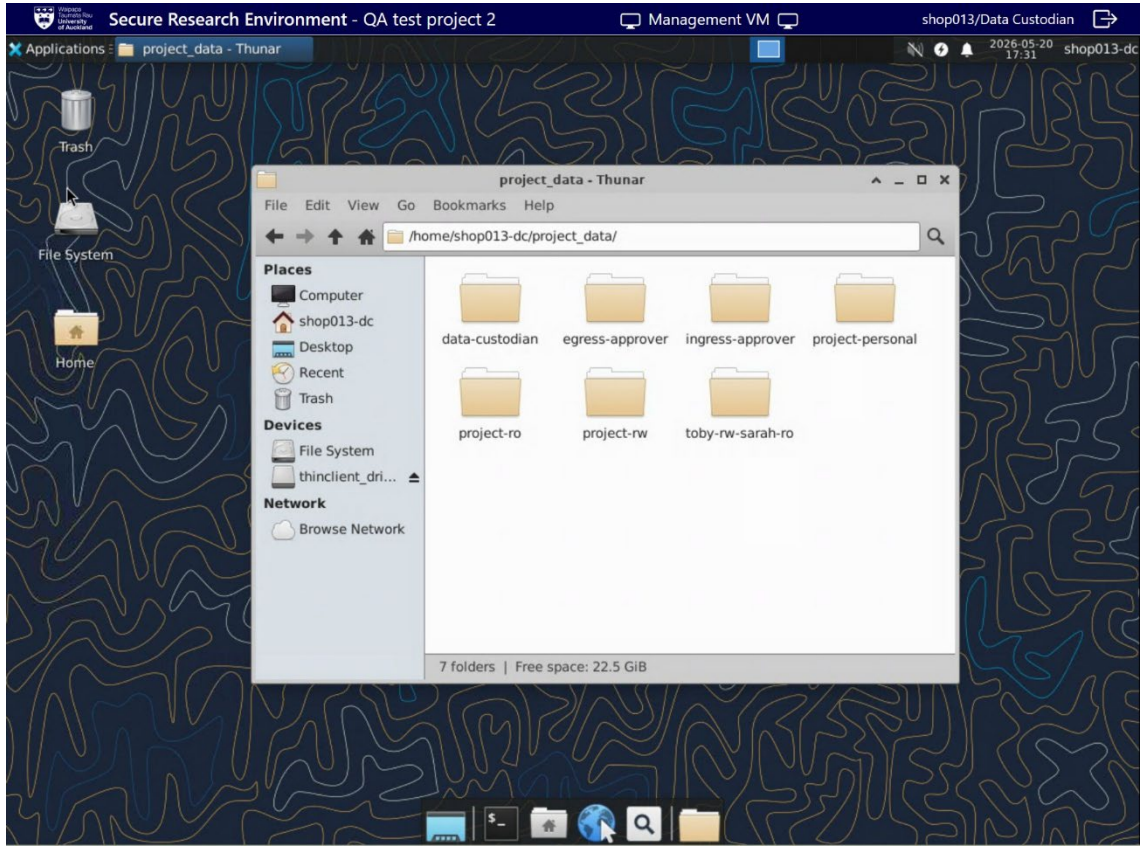
Dexter Dataset uses the **Data Custodian** role to:

- Move raw datasets to restricted location
- Create a copy to check data quality, clean data, and link datasets
- Save the analysis-ready de-identified dataset in the project read-only folder

Data custodian

File and data management

Data Manager manages data and files across the project storage locations to ensure data and associated files are shared only with appropriate project team members



1. Raw project data and files moved to a secure data custodian folder (contains direct identifiers)
2. After cleaning and data linkage, the analysis-ready dataset moved to the project-ro folder.
3. A data subset created for the PhD student is transferred to the students personal project folder.

SRE

Data storage

Data is stored separately for each research project and can only be accessed by the team assigned to that environment

Folder name	Access	Who can Access	Purpose
project-rw	Read / Write	All project users	Shared working directory for collaboration
project-ro	Read-only	All project users (Data Custodian has full access)	Stores raw or source data
project-personal ([username]-r)	Read / Write (own folder)	Individual researcher (Data Custodian has full access)	Private working space for individual research users
data-custodian ([username]-dc)	Read / Write	Data Custodians	Used for direct data ingress/egress and data management
ingress-approver	Read / Write	Ingress Approvers (Data Custodian can view)	Temporary storage for files awaiting ingress approval
egress-approver	Read / Review	Egress Approvers (Data Custodian can view)	Temporary storage for files awaiting egress approval

Project tasks

The Biostatistician can conduct statistical analyses without removing data from the environment.

Dr Stan Dardeviation, the Biostatistician based at an Australian university, can access the de-identified study dataset, as well as the software and tools they require to carry out all analyses and create outputs (e.g., tables, figures).

This ensures all data remains in New Zealand.

Researcher

System settings for SRE

Biostatistician accesses, cleans and creates linked research dataset

1. During access and analysis, SRE users cannot:
   - Access the internet (unless approved
   - Copy/paste or drag and drop into or out of the project environment
   - Mount a USB or local drive
2. Aligned with University security standards
3. Project data is encrypted
4. Audit logging
5. Continuous monitoring
6. Virus checking
7. Managed software

Publishing results

Secure research continues beyond the analysis stage

Safe Outputs

- Output checking and disclosure review
- Controlled data egress
- Releasing tables, figures and models
- Common output risks

Project tasks

The Biostatistician has prepared tables and figures for draft manuscripts.

Dr Stan Dardeviation prepares **tables and figures** that they wish to **export** from the SRE environment.

All outputs are reviewed by the **egress approver** to assess whether materials could identify individuals.

Approved outputs are released from the SRE.

Egress approver

Disclosure review during egress

During output review the Clinical Lead identifies a possible disclosure risk

Hospitalisations, by age bracket

Age Group	Region	Hospital Admissions (n)
75-84	Small rural area	15
85+		3

1. A table containing only 3 participants in a older age category (85+).
2. The team agrees to aggregate this category with the cell above to reduce the risk for re-identification in the data.
3. The Biostatistician requests egress of the updated table for publication.

Summary

Using a Secure Research Environment

Using the Five Safes Framework to evaluate project access and handling of sensitive data

Before publication, all outputs are reviewed by Clinical Lead to ensure no individual can be identified. Findings published with aggregated statistics. Small cell counts suppressed to maintain confidentiality.

Researchers in the project team were required to complete training on data confidentiality, statistical disclosure control, and secure handling of sensitive data.

Research purpose demonstrated public benefit and included costs of SRE in their funding budget. Ethics approvals & data access applications completed and documented in DMP.

Names, addresses, and other direct identifiers are removed. Geographical data is aggregated.

Data is accessed through a Secure Research Environment (SRE). No internet access, external storage or printing. All user activity, queries, and data exports are logged and monitored.

Description and information from the creators of the Five Safes framework
How Stats NZ uses Five Safes to manage access to integrated data in NZ

Secure research environment (SRE)

Project-specific virtual platform for the secure storage and analysis of sensitive data.

Security

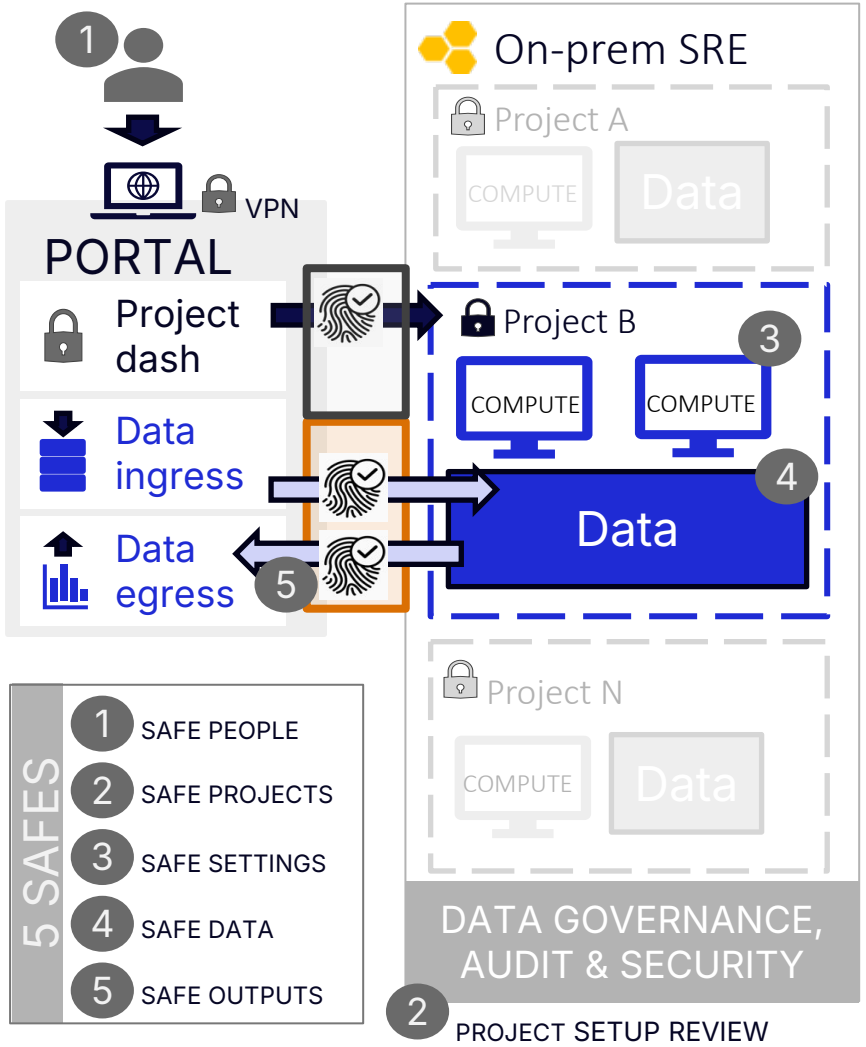
- Controlled access for authorised people
- Project data is encrypted
- Auditable data import, export and access

Collaboration

- Shared workspace for a project with data and analytical tools in one place

Compliance

- University approved for sensitive data
- Aligned with University security and governance standards



Research resources [Secure Research Environment (SRE)]

Waipapa Taumata Rau
University of Auckland

Questions? Get in touch...

researchdata@auckland.ac.nz

Thank you