



# KeyPoint Managing Identities

eResearch Australiasia 2024



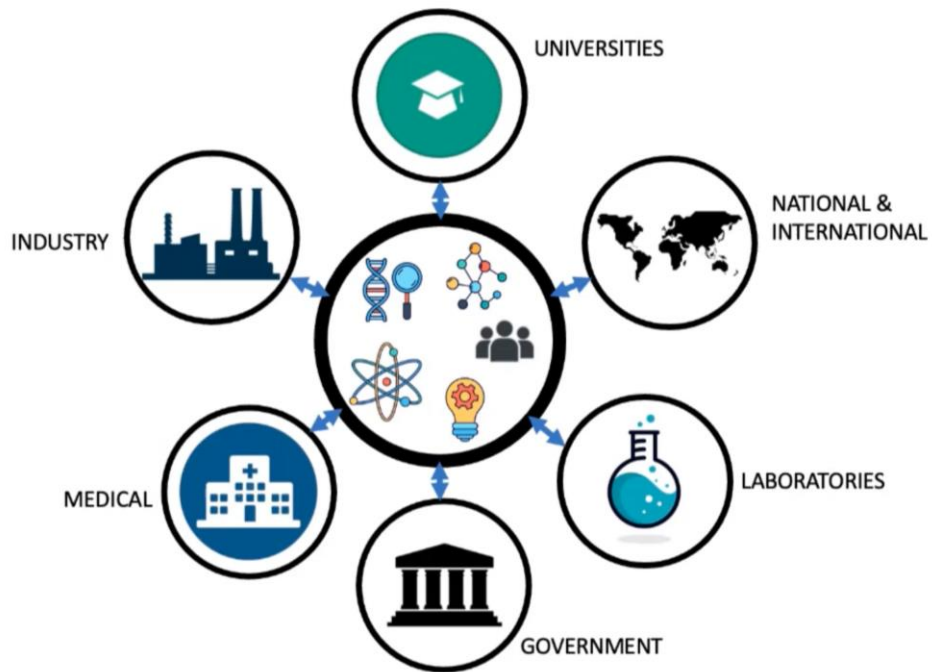
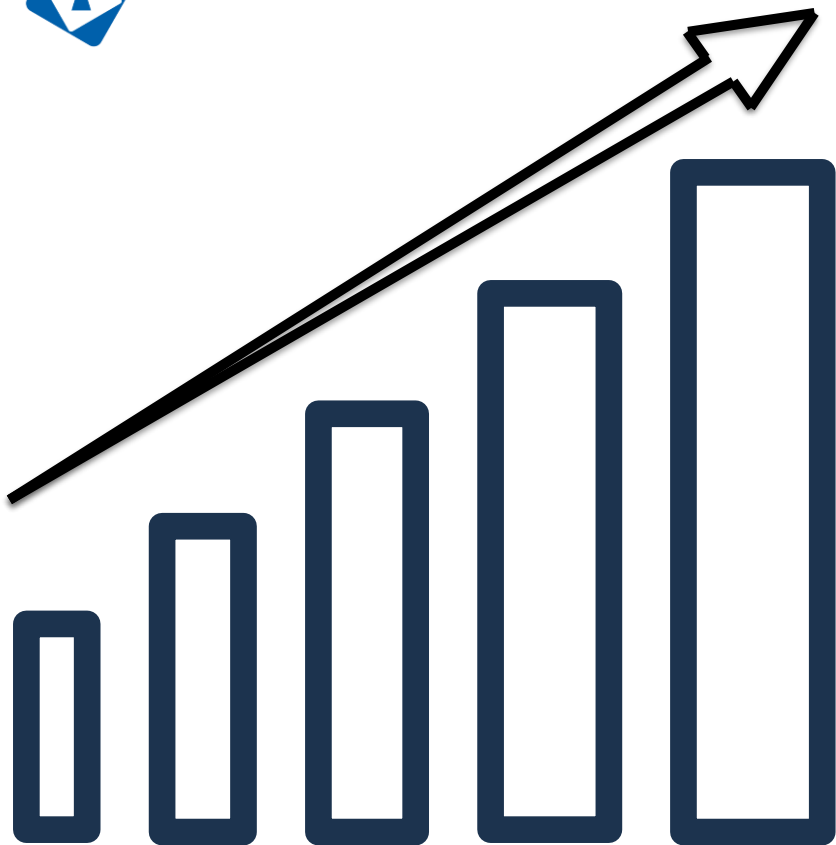


**30%**

Human Error

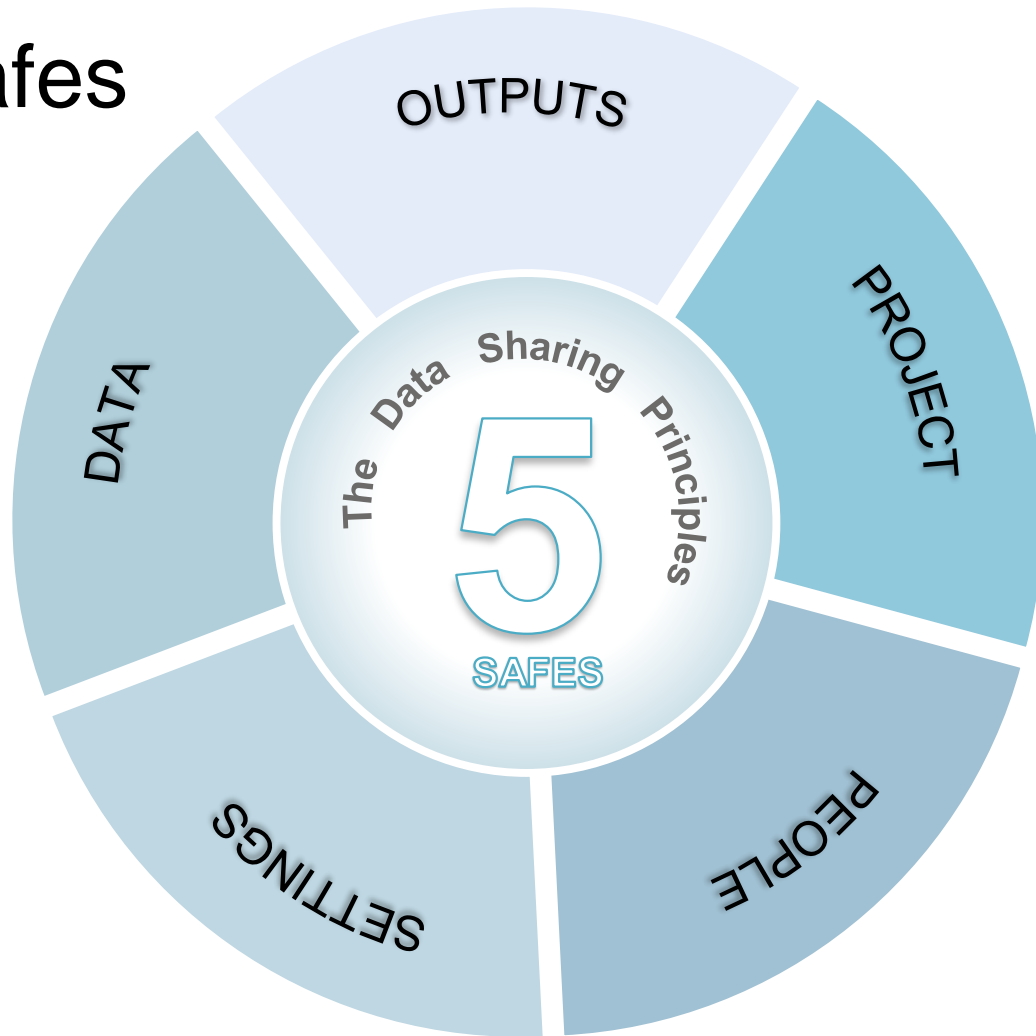
**70%**

Sent to the wrong person  
or  
unintended release





# 5 Safes





## Safe Projects

Defined Purpose

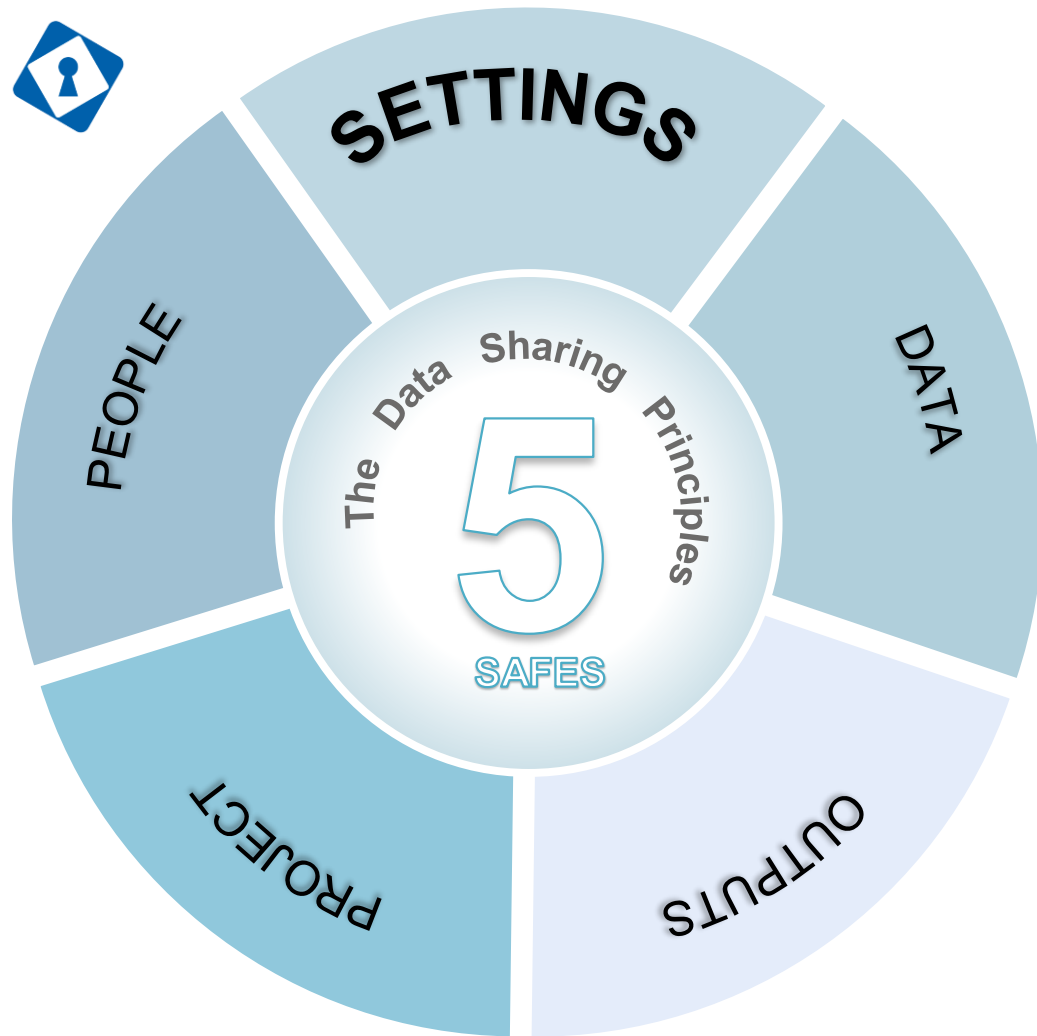
Data use is lawful and ethical

Sharing data is appropriate and authorised



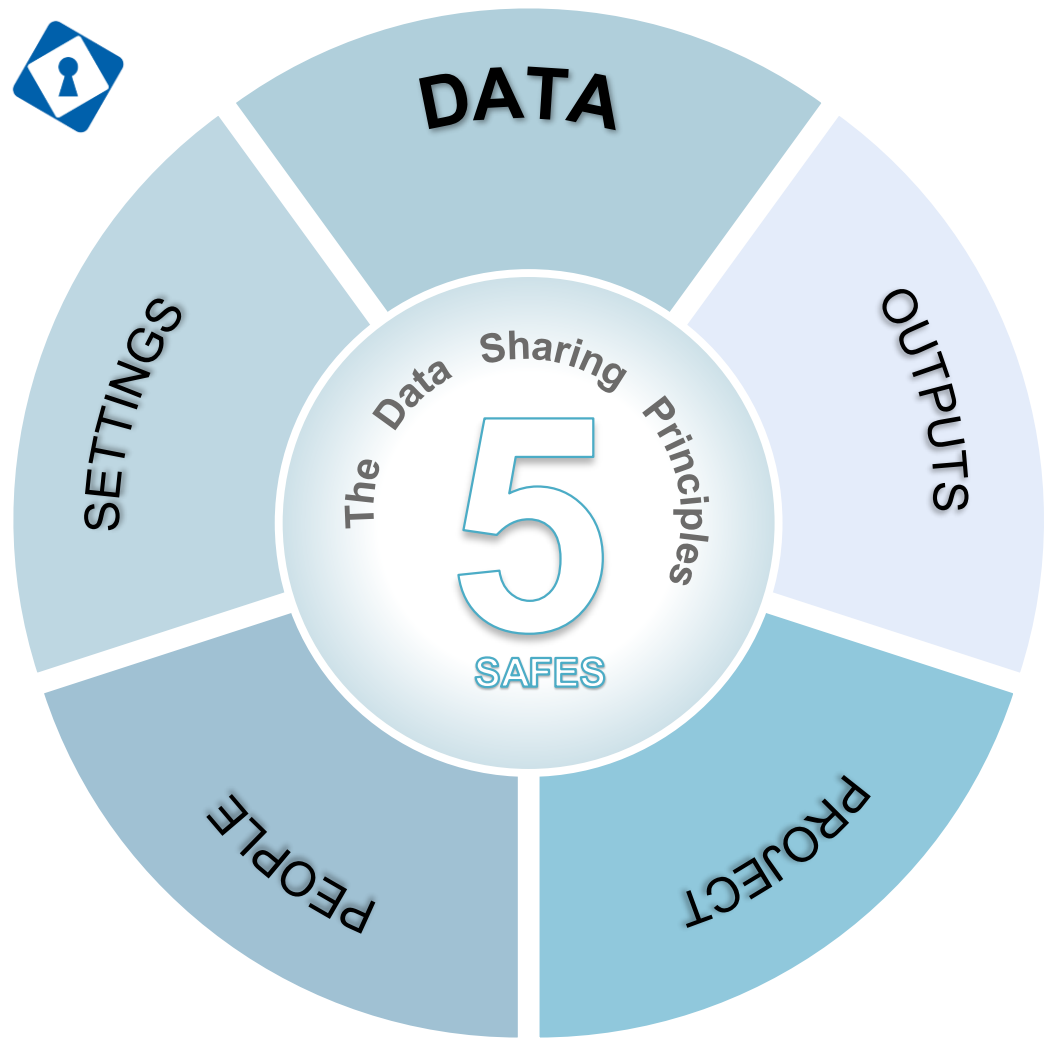
## Safe People

Sharing data is only to authorised people



## Safe Settings

Data is used in a safe and secure environment

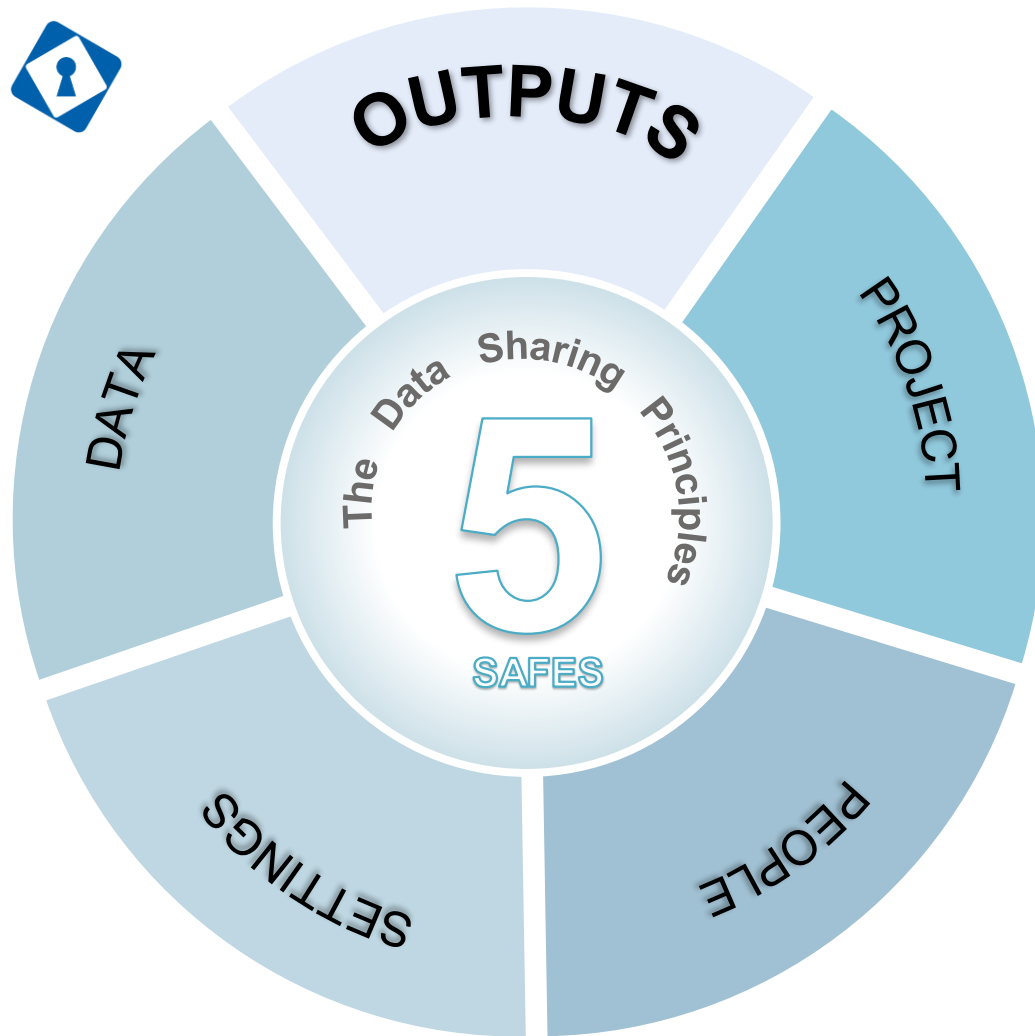


## Safe Data

Data has appropriate protections applied.

De-identified

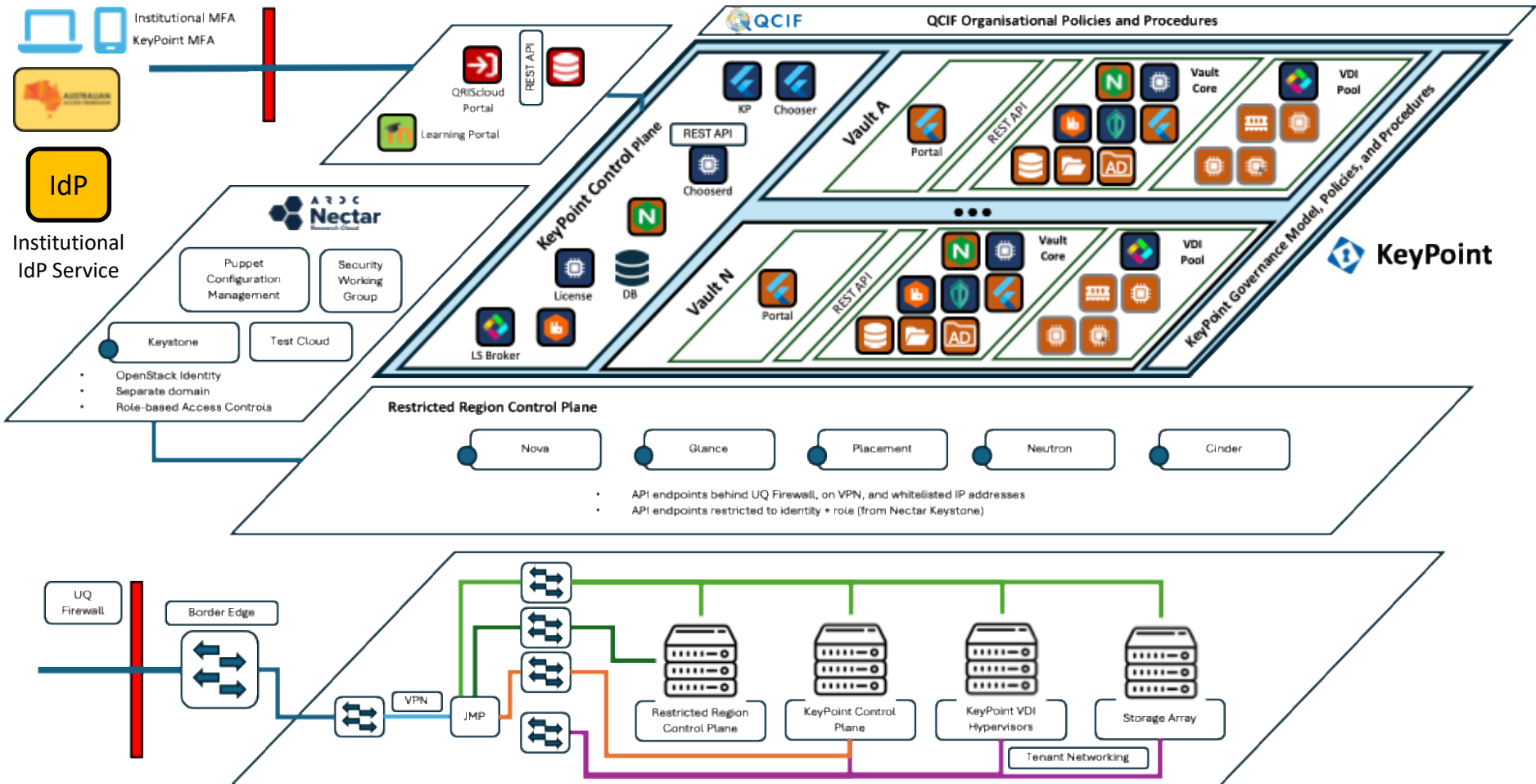
Anonymised



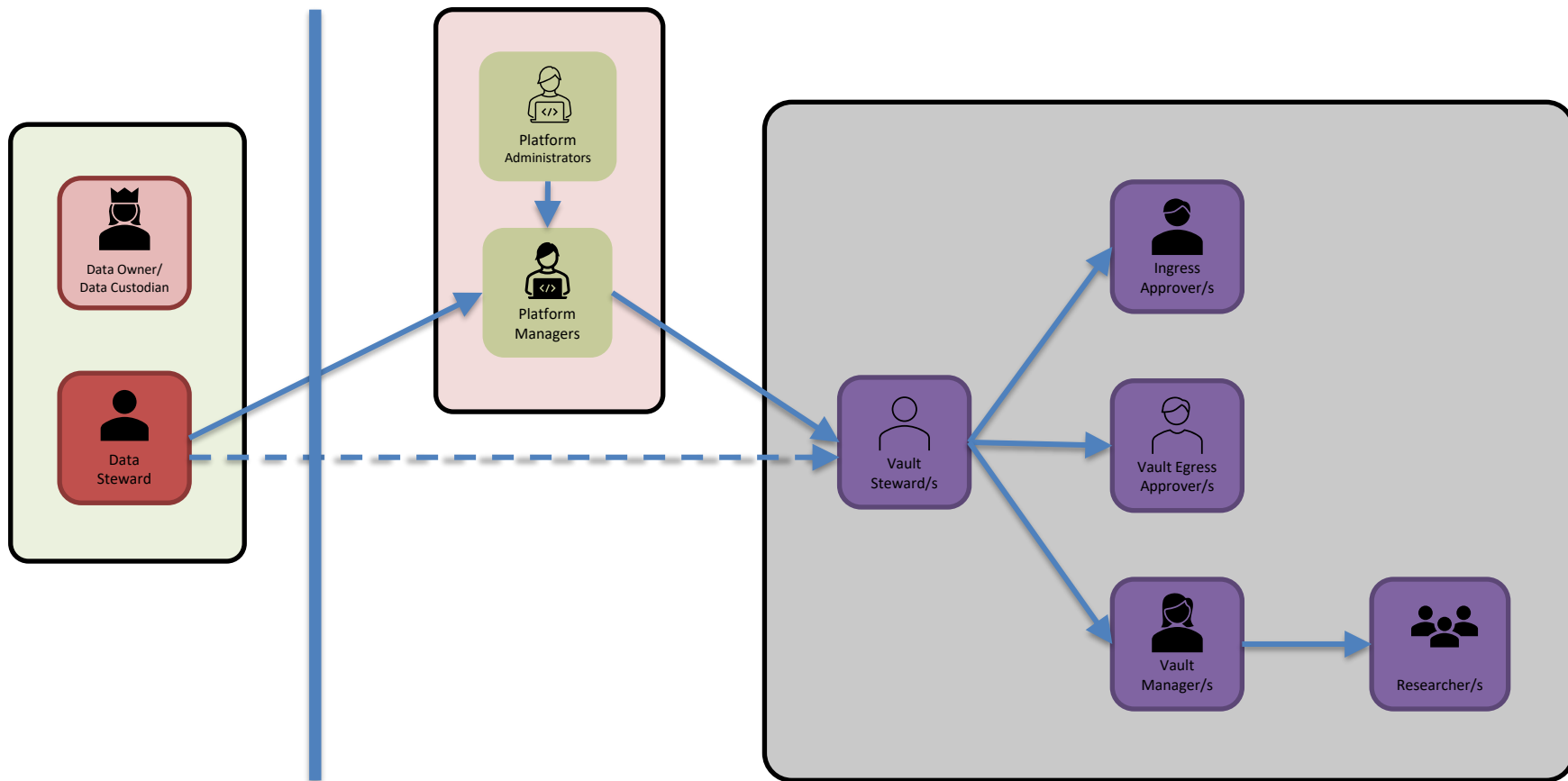
## Safe Outputs

The results of analysis  
cannot cause harm

Cannot identify individuals  
or organisations

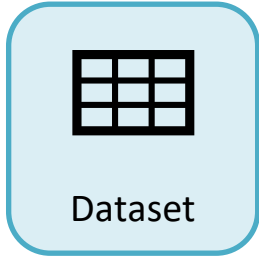
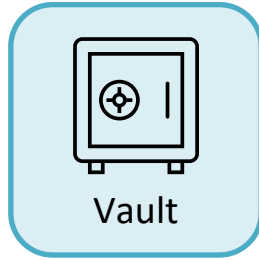


# Keypoint Roles



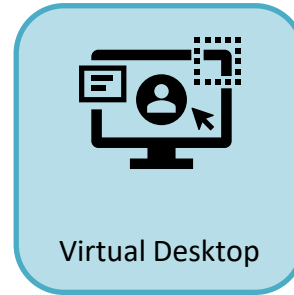


# Core objects in KeyPoint





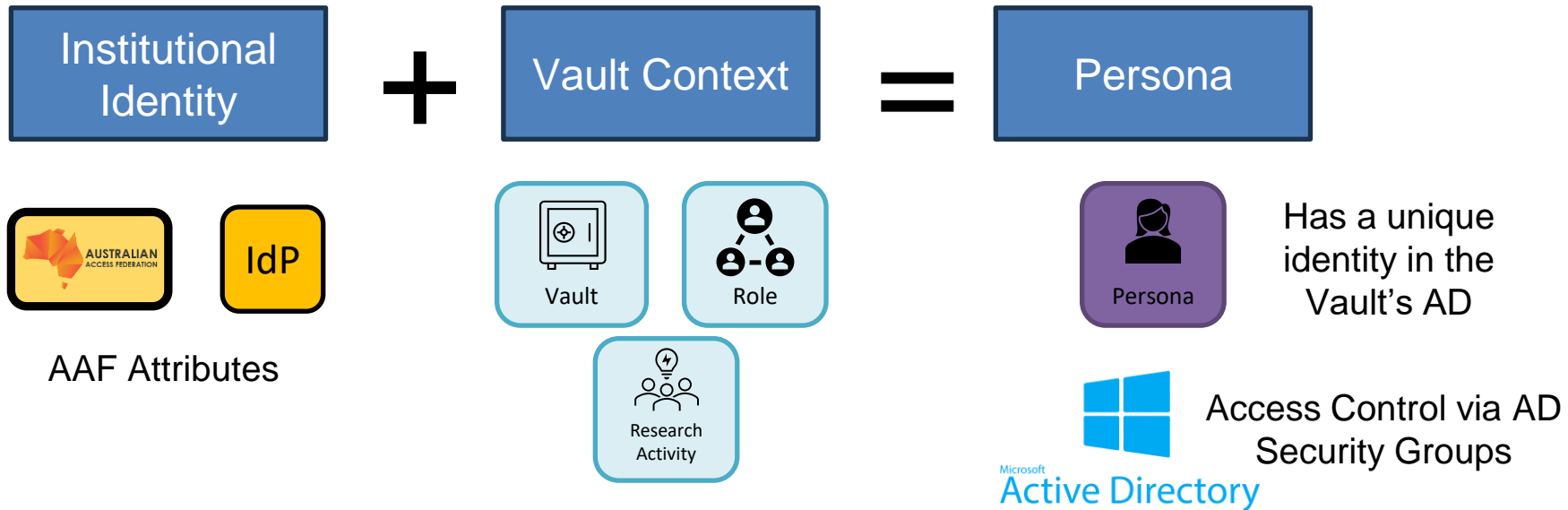
# Strict separation at the desktop



Only access the data that you are authorised to see based on:

- who you are, i.e. authenticated AAF identity
- your Persona, or context, when you launch a desktop, i.e. Vault, Role, Research Activity

# KeyPoint Personas



- Persona details abstracted away from an end-user
- KeyPoint controls Persona username and password – not known by an end-user
- KeyPoint UI is context sensitive and tracks which Persona is active for an end-user
- Persona has a Roaming Profile to follow it to Virtual Desktops



# KeyPoint Invitations



Invitation Link

Email address

+

Context

Vault  
Role

Research Activity

Accepted  
Invitation

Who was invited

+

Who accepted

Approved  
Invitation

AAF Attributes to Vault

AAF Attributes to Vault Context

Persona in Vault AD

Persona to AD Security Groups



# KeyPoint Access Gates

Gate 1: AAF and QRIScloud Account

Gate 2: Stage 1 Authorisation to use KeyPoint

Gate 3: Stage 2 Authorisation to see a Vault

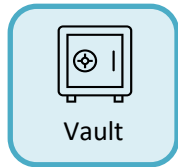
Gate 4: Access to use Data in a Research Activity

Gate 5: Continuous validation of authentication and authorisation

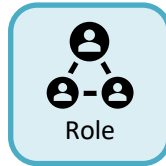
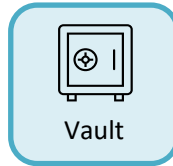


# KeyPoint – which modules know what

KeyPoint Portal



Vault Portal



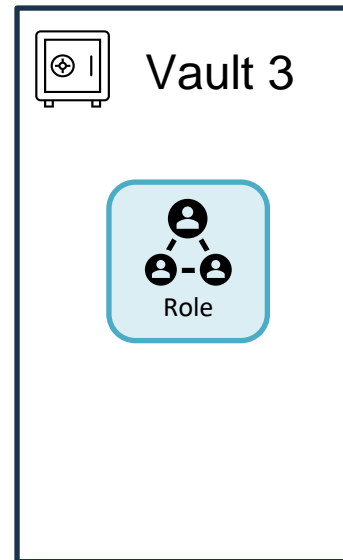
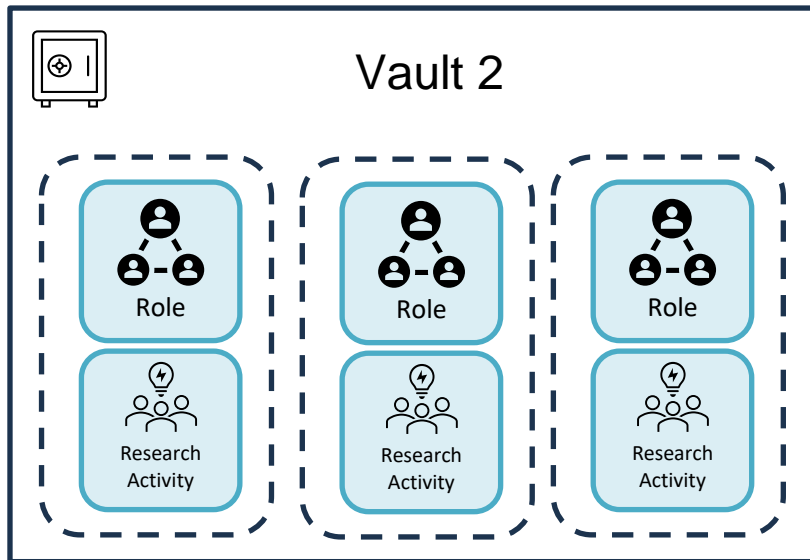
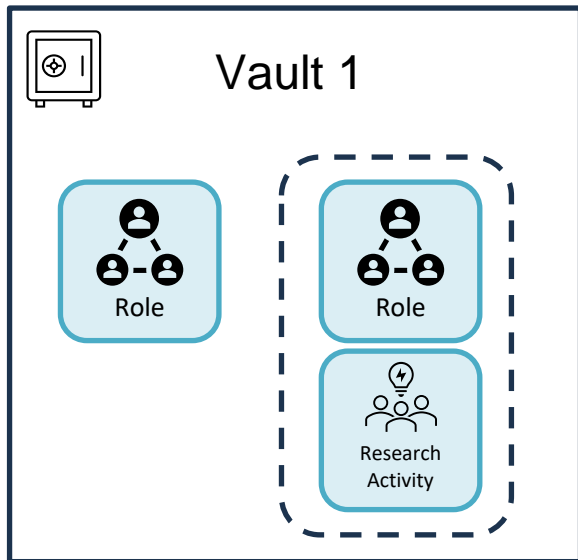
Vault Core



# KeyPoint identities



AAF Identity





# Summary

- AAF and institutional credentials are the basis for KeyPoint identities
- Robust invitation mechanism to bring someone into KeyPoint, in a specific context
- Context is comprised of Vault, Role, and optionally, a Research Activity
- The combination of AAF + Context defines a Persona
- A Persona is a unique identity in the Vault's AD
- AD lets us leverage security groups for access control



# Summary

- Persona details are abstracted away from an end-user
- KeyPoint controls Persona username and password – not known by an end-user
- KeyPoint UI is context sensitive and tracks which Persona is active for an end-user
- Each Persona has a Roaming Profile to follow it to Virtual Desktops
- One physical person can have many Personas in KeyPoint



Thank you