Solution Overview

One solution comprising multiple components to meet different use-cases.

Accommodates requirements for both hosted desktops and mobile desktops (laptops) with the ability to install and run non-approved software and collaborate more securely with people outside the university.

Secure Research Laptops (Phase 1)

Provides each researcher with a well secured research laptop:
- ITS-managed Windows, Mac and Linux Machines
- Includes a Virtual Environment that researchers can use, if required, within which they can install Virtual Machines (VM's with any OS) and install/run any software
- Place the research laptops in a segregated and heavily fortified network security domain

Secure Virtual Environment hosted in QM Data Centre (Phase 2)

Offers researchers Virtual Machines within the existing VDI Solution (VMware Horizon)
- Ability to deploy more resource-intensive VM's than laptops can support
- Allows collaborative use of data output with other researchers (both Queen Mary and external)

Benefits

- One overall solution to meet multiple needs
- Provides researchers with a choice of options available to use as required
- Use of existing VDI technology
- Enables researchers to move between options without the need to procure or replace the technology
- Enables ITS to implement and manage security controls across all technology and data flows
- Aims to provide researchers with all the software and collaborative freedom they require

Note: The solution is not Cyber Essentials compliant. QM should looking towards achieving ISO27001 for this service.