GRIFFITH UNIVERSITY

Local Protocol

Griffith Data Trust –Security Management Protocol

1.0 Purpose

This Local Protocol sets out the processes applicable for managing the security of any data obtained by the Griffith Data Trust, including its role as an Accredited User and Accredited Data Service Provider under the *Data Availability and Transparency Act 2022* (Cth) (DAT Act). The Local Protocol includes measures to minimise the risk of unauthorised access, sharing, or loss of data.

2.0 Scope

This Local Protocol applies to the Griffith Data Trust when handling data, including data obtained under legislation and in its capacity as an Accredited User and Accredited Data Service Provider under the DAT Act.

Local Protocol applies subject to any requirements of a Data Sharing Agreement, which will prevail over this document.

3.0 Local Protocols

3.1 Security governance

3.1.1 Guiding Principles

There are 5 principles that underpin the Griffith Data Trust's approach to security and guide how the Griffith Data Trust will make security decisions:

- Security is everyone's responsibility. Developing and fostering a positive security culture is critical to security outcomes.
- Security enables the success of the Griffith Data Trust. It supports the efficient and effective conduct of research and delivery of services.
- Security measures applied proportionately protect the University's people, information, and assets in line with assessed risks.
- The Griffith Data Trust owns its security risks and its impact on shared risks.

- A cycle of action, evaluation, and learning is evident in response to security incidents.

3.1.2 University security oversight

- The University Executive Group, through the Vice President (Industry and External Engagement) oversees Griffith Data Trust's governance, security, and compliance, based on the Annual Report from the Director of the Griffith Data Trust.

3.2 Security controls

Data security is prioritised by following a risk-based approach as outlined in Griffith's Information Management and Governance framework, implementing appropriate controls to secure data and minimise risk. The Threat and Risk Matrix details the risk and compensating, technical, process, and people controls in place to reduce risk. For further details, refer to the threat and risk matrix.

Note that additional or adjusted security control measures may be required for specific datasets, as determined by the data custodian in the data sharing agreement.

3.3 Facility access

Anyone requesting facility access must be referred to administrative staff. Only administrative staff can grant access to the facility.

All access requests require approval from the management team (listed in Appendix B). This team may impose certain restrictions at their discretion. For example, a research project brief with expedited ethics approval may need to be sighted before access is granted.

3.4 Facility maintenance

3.4.1 Access for routine maintenance

Access to perform routine maintenance is by appointment only, all workstations must be secured (i.e., locked) whilst non-security vetted personnel are present. Maintenance personnel (Griffith or external contractors) will be escorted by administrative staff. An estimate of the time needed to complete the work should be provided when booking. Maintenance work requiring an extension may need to be scheduled for weekends to avoid disrupting research activities.

3.4.2 Access for cleaning

The facility will be cleaned by the Lab Coordinator.

3.4.3 Emergency maintenance

In the event of an emergency where access to the facility is required, onsite security will use the call registers as listed in Appendix B.

3.5 Safety

3.5.1 Lone working / Out of hours working

Normal working hours for The Facility are weekdays 08:00 – 17:00. Out of hours include:

- 17:00-08:00 weekdays
- Weekends
- Public holidays

- Griffith University closure days.

Authorised users are permitted to work in the facility outside of regular hours by special arrangement with administrative staff and with written permission. The process is as follows:

1. Authorised users must submit a request to the Griffith Data Trust portal.
2. Administrative staff will email written permission for out of hours staff to campus-support-MG@griffith.edu.au with as much advance notice as possible. The approval template can be found in Appendix C.
3. Staff working out of hours must first check-in at the campus security office, showing their Facility ID and signing the sign-in sheet.

- Work in the facility during the allocated time slot only.

4. Sign out at the campus security office upon completion of work or at the end of the allocated time.

3.5.2 Monitoring

The facility alarm system will be monitored by Griffith Campus Security, with security following Griffith's Emergency Management Plan when responding to alarms being triggered.

3.5.3 Emergencies

All emergencies within the facility should be treated seriously. The emergency door release button, located in the facility, notifies Griffith Campus Security.

Administrative staff (call roster, Appendix B) will be notified of any incident as soon as practicable and escalate matters to the Director of the Griffith Data Trust as necessary. All emergencies will be logged and reviewed.

3.5.4 False Alarms

If an emergency door release is accidentally triggered, follow the instructions on the release panel to reset the alarm and contact campus security immediately to report the accidental release. Griffith Campus Security will verify the accidental alarm activation and the user's identification.

Griffith Campus Security will advise administrative staff of all alarm activations in a weekly report unless specified otherwise in this document.

3.5.5 During work hours plan

1. Griffith Campus Security receives notification of incidents (e.g., intruder alarm, emergency door release activation, fire alarm).
2. Griffith Campus Security Officers will follow the Emergency Management Plan or Crisis Management Plan, depending on the incident.

- Anyone working in the facility must evacuate during an emergency. Terminate work sessions and secure workstations where safe to do so.

3. See below for specific instructions on different types of incidents.

3.5.6 Intruder

Notify Griffith Campus Security immediately. Administrative staff should also be notified as soon as possible using the call roster in Appendix B. Administrative staff may provide CCTV footage of an event if requested.

3.5.7 Emergency door release button

When an emergency door release alarm is triggered, researchers and staff working in the facility must terminate their work sessions, secure the workstations (by locking the screens or logging out), and leave the facility as quickly as possible. Griffith Campus Security will follow Griffith's Emergency Management Plan.

3.5.8 Medical emergency

Any qualified first aider should attempt to stabilise the patient until medical services arrive. Administrative staff will escort medical services within the facility and ensure all other occupants are evacuated.

3.5.9 Fire alarm & drills

Occupants of the facility must follow the general Griffith University fire evacuation procedure Emergency information (griffith.edu.au). All activations of fire alarms should be treated as real.

3.5.10 Flood

Notify administrative staff immediately (via the call roster in Appendix B), secure workstations (by locking the screen or logging out) and evacuate the premises.

3.5.11 Power failure

The door access system will function for an additional period. After this time the Grand-Grand master key is the only way into the room. Administrative staff will check all rooms to ensure that no one is trapped, and that The Facility is secure.

3.5.12 After Hours emergencies

After hours emergency, contact the administrative team listed in Appendix B. If emergency access to the facility is required, Griffith Campus Security will call the listed numbers until contact is made. Security personnel must make every effort to ensure the security of M06 2.11a and 2.11b is kept intact.

3.6 IT system Hardware

3.6.1 Commissioning

All new equipment must be obtained in accordance with Griffith University's (GU) purchasing restrictions. To make a purchase, log into the Griffith staff portal, select "my finance page," then "purchases and payments," and "make and manage purchases".

All infrastructure purchased for the room will be assigned a Griffith and Digital Solutions Asset number, and have its lifecycle managed by the Griffith University asset management system.

Administrative staff will escort digital solutions staff delivering hardware to the room. This will be scheduled during a maintenance window to ensure no data is exposed during this period.

In accordance with Griffith University's Electrical Safety Procedure Electrical Safety Procedure (windows.net). Regular testing and tagging of electrical equipment are mandatory safety measures to protect users from electrical faults and deterioration that cannot be detected by visual inspection. Testing must be undertaken by a suitably qualified and licensed contractor or employee, in accordance with AS/NZS 3760.

3.6.2 Maintenance

Regular maintenance of the equipment located in the room will be required to keep the systems running. Regular maintenance includes:

- operating system updates
- antivirus updates
- application updates

Once a stable environment has been established, workstations will be updated every six months, or immediately if a critical security patch is released or new software applications are required. Any ad hoc software changes to the workstation environment require three weeks' notice.

Servers will be updated on an as-needed basis.

Dataset audits will be conducted annually on the anniversary of dataset creation to ensure dataset relevancy and dataset security requirements are still met.

3.6.3 Faults

Administrative staff should be notified of any fault to the environment via the Griffith Data Trust portal detailed in section 3.8.3. Any hardware that is to be removed from the room is to have all hard drives removed and cleansed according to the data destruction procedure defined as per section 3.6.4 'decommissioning'.

3.6.4 Decommissioning

1. Administrative staff must visually inspect televisions and computer monitors by turning up the brightness and contrast to the maximum level to determine if any information has been burnt into or persists on the screen.
2. Administrative staff must attempt to sanitise televisions and computer monitors with minor burn-in or image persistence by displaying a solid white image on the screen for an extended period.
3. Administrative staff must destroy televisions and computer monitors that cannot be sanitised.
4. To sanitise network devices, administrative staff must perform a full reset and load a dummy configuration file to confirm the reset was successful.
5. When decommissioning ICT equipment from service, all hard drives must be removed from the equipment prior to the equipment leaving the room.

Destruction of Hard Drives and Backup Tapes

A service that provides the following will be chosen for the destruction of hard drives and backup tapes:

- provision of a securable bin for storage of magnetic media
- pick-up and replacement of the securable bin on request
- data Destruction by degaussing of magnetic media to NSA standards
- environmentally friendly disposal of magnetic media in accordance with ISO 14001 audited processes
- government approved reporting, including serial numbers, time/date stamps, and operators' names, to verify the destruction of magnetic media. This will be accompanied by a Data Destruction Certificate.

3.6.5 Configuration of Assets

3.6.5.1 General principles

- All IT infrastructure, where possible will have their date/time set by a local authoritative source.
- Administrator accounts will have strong complex passwords. (Refer to Griffith University's Password management guidance Password management (griffith.edu.au) on password complexity).
- Administrative passwords will be unique and not used on any other external systems.
- Administration passwords will not be the same across separate services.
- Each administrator will have a unique and identifiable account.
- Administrator accounts will be used exclusively for administrative purposes.
- No anonymous access is permitted to the database.
- All default user accounts are to be deleted, disabled, or renamed where possible.

3.6.5.2 Database Servers

Raw data server
This server acts as a staging and anonymising server for incoming datasets and is only turned on when required.

Its primary function is to facilitate data ingestion processes specified by the data provider. Once completed, resulting data can be copied to the solution data server for end user access.

Solution data server
This server is the main storage server for production data. End users do not have direct access to query the primary databases stored on this server, however, administrative staff can provide access to extracts of this data upon request.

High Performance Computing (HPC)
From within the research workspace, researchers can submit computationally intensive jobs to the local HPC environment.

The batching system chosen for this HPC is PBS by Altair, closely resembling Griffith University's HPC to maximise support for The Facility.

Administration Servers
There will be multiple administration servers each of which will perform a group of specific functions. The operating system of choice for The Facility is Windows Server 2012 R2.

Each server's operating system is hardened to standard installation practices at Griffith University, including the disabling of unused services. Administrative functions required include:

- authentication services
- DHCP server
- DNS server
- audit logging
- backup
- Windows file share server
- authoritative time source
- physical access

3.6.6 Door access control and alarm system

The Gallagher door access control and alarm system will be installed in TER 2 to manage access to The Facility doors. The Gallagher Command Centre, located within the yellow zone, operates from a separate desktop PC.

3.6.7 Sheep dip

The Sheep Dip provides a dedicated, isolated platform to clear incoming data of viruses and malware. It's installed on an Apple Mac computer located inside the Yellow Zone, with multiple anti-virus solutions that are capable of:

- being independently updated
- scan removable media
- scan for both Windows and *nix virus and malware

3.6.7 Lab management PC

This management PC is located within the TER room and is used for the management of the infrastructure. Only administrative staff will have access to this PC.

3.6.8 Workstation Configuration

While the software configurations in the teaching and research zones are equivalent, access permissions to solution data are different. In the research zone, end users with appropriate privileges can query the solution data and submit jobs to the HPC. Workstations within the teaching zone only have access to data specifically shared for this purpose.

Data copied to all workstations for local processing is removed at the end of that session. Processed data can be retained by copying it back to the individual user space allocated on the administration servers.

All external media ports on workstations will be disabled in BIOS and physically disabled where possible. Additionally, the workstation BIOS will be password protected.

3.6.9 AV equipment in the Teaching Room

The teaching zone houses 13 single monitor workstations, and multiple wall mounted displays with the ability to display any of the workstation screens via a central “teacher pc” to which access is only granted to designated “teachers”.

3.7 IT Audit logging

All systems (where possible) will be set up to log events, and these logs will be captured and stored in a read-only central log system for auditability. Event logs will be regularly audited for signs of attempted or successful cyber intrusions.

- server authentication success / failures
- workstation authentication success / failures
- door swipe success / failures
- windows events on workstations and servers
- database interactions

3.8 Software Configuration

The following software is approved for use in the facility. Any new software introduced must be approved by the administrative team. Ad hoc changes to software on workstations require a minimum of 3 weeks’ notice, and a ticket must be raised in the ticketing system for approval.

3.8.1 Workstations

- Windows 10
- RStudio with R Libraries
- SPSS
- Mapinfo
- ArcGIS
- CrimeStat
- Deepfreeze
- Microsoft Office 2016
- Symantec Antivirus
- Adobe acrobat professional

3.8.2 Servers

- Windows 2012 R2
- RStudio
- MSSQL Server Enterprise (with audit enabled)
- PBS for windows

3.8.3 Ticketing System

The facility utilises the Web Help Portal for its ticketing system. Jobs can be submitted via the webform portal at **https://ridl-gdt.atlassian.net/servicedesk/customer/portal/.**

Submitting the form through the web portal creates a ticket in Jira. Requests logged in Jira are monitored by the Lab Coordinator and follow an approval workflow to completion.

All requests for changes to infrastructure or requests for data must be logged in the ticketing system. All requests will be responded to within 48 hrs. For emergency IT needs, please contact the administrative team as listed in Appendix B.

3.9 Back up

Each dataset or project should have defined backup requirements specific to its needs. This definition should contain the specified backup regime and data retention/archive for that project/dataset. All tape backups must have encryption enabled to protect the sensitivity of the data.

3.10 Security incident management

The Griffith Data Trust is responsible for identifying and managing information security risks relevant to the information it owns, manages, stores, and distributes (as per Griffith's Information Security Policy). It is our responsibility to follow Griffith's guidelines when reporting a suspected security incident by email to the IT Service Centre.

The GDT will provide as much information as possible, including:

- dates and times
- people and places involved
- known impacts
- any other background information or context

4.0 Information

Title	Griffith Data Trust – Security Management Protocol
Document number	Provided by relevant Policy team
Purpose	This Local Protocol sets out the processes applicable to the management of the security of the Griffith Data Trust, including to minimise the risk of unauthorised access, sharing or loss of data.
Audience	GDT Staff
Category	Academic
Subcategory	Research
UN Sustainable Development Goals (SDGs)	This document aligns with Sustainable Development Goal/s: 16: Peace, Justice and Strong Institutions
Approval date	October 2024
Effective date	October 2024
Review date	2025
Policy advisor	GDT Policy and Compliance Coordinator
Approving authority	Director, Griffith Data Trust

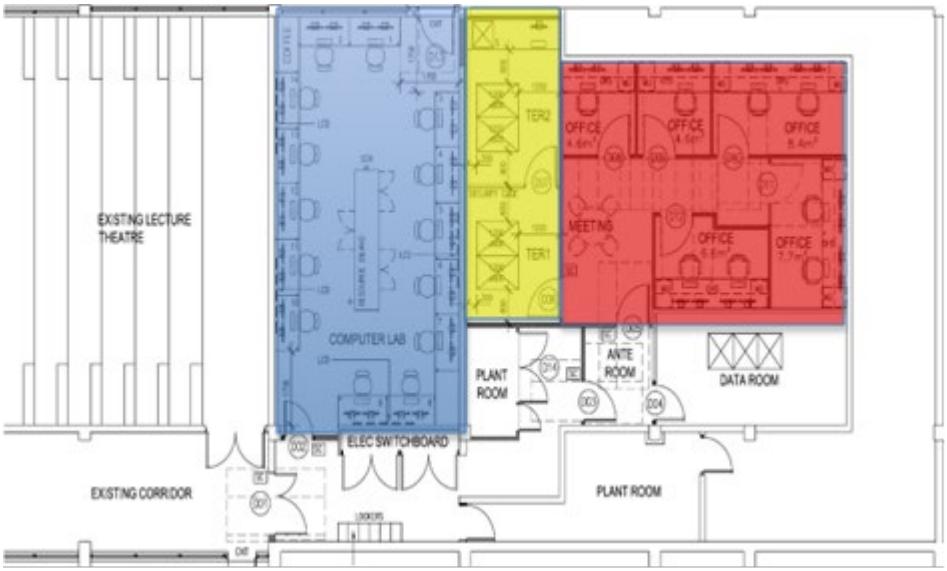
5.0 Related Policy Documents and Supporting Documents

Legislation	*Data Availability and Transparency Act 2022* (Cth) (DAT Act)
Policy	Griffith Data Trust Policy
Procedures	Griffith Data Trust Procedure Griffith University Electrical Safety Procedure Griffith University Emergency Management Plan Griffith University Crisis Management Plan
Local Protocol	Griffith Data Trust Committee Terms of Reference Griffith Data Trust Data Governance and Management Protocol Griffith Data Trust Data Extraction and Sanitation Protocol Griffith Data Trust Human Resource Skills and Capability Management Protocol
Forms	Academic Researcher Agreement Form General Staff Agreement Form

Appendices

Appendix A – Facility layout

Facility schematic showing access zones.



Appendix B – Contact Details

Administrative team

Name	Role	Telephone	Email
Shiela Villanueva	Griffith Data Trust Lab Coordinator	0466 208 059	s.villanueva@griffith.edu.au
Matthew Russell	Social Analytics Lab Coordinator	(07) 3735 5672	m.russell@griffith.edu.au

* Denotes primary lab manager

Management Team

Name	Telephone	Role	Email
*Tom Verhelst	0424 273 008	Griffith Data Trust Director	t.verhelst@griffith.edu.au
Charlotte Owona	0480 437 232	Griffith Data Trust Policy and Compliance Coordinator	c.owona@griffith.edu.au
Michael Townsley	(07) 373 51025	School of Criminology and Criminal Justice Professor	m.townsley@griffith.edu.au

* Denotes chair

Call Roster

Name	Role	Telephone
Shiela Villanueva	Griffith Data Trust Lab Coordinator	0466 208 059
Matthew Russell	Social Analytics Lab Coordinator	(07) 3735 5672

Appendix C – After Hours Work

Dear campus security,

Please be advised that <insert person full name> with ID number <insert Facility ID>, is permitted to work outside the normal operating hours of the Social Data Analytics Lab in M06 2.09 and 2.11. Expected working hours are between <insert start time> and <insert finish time> on/between the <insert date/date range>.

They have been informed to sign in at the campus security office showing their Facility ID prior to entering the facility and sign out prior to leaving campus.

Kind regards
Facility Administrative Team.