SA NT DataLink
Security Manual -Overview

Organisation: SA NT DataLink, University of South Australia
Issue Date: 15th July 2019
Version: v1_06

For any queries, contact chris.radbone@unisa.edu.au .

DOCUMENT HISTORY

File Details

File Location	SA_NT_DataLink/SA_NT_DataLink/Policy_Procedure/Security/Security_Manual/

Document Revision/Release Status

Version	Date	Summary of Changes	Author / Editor	Quality Review
v0.01	15/10/09	Initial draft by Chris Gascoigne	Chris Gascoigne	John Barratt
v0.02	15/01/10	Updates from John Barratt. Review of security functional roles, and structure of the document by Chris Radbone	Chris Radbone	Chris Gascoigne
v1.01	22/01/10	Endorsement by SA NT DataLink Steering Committee, with agreement to proceed with Information Security ISO 27001 certification.	Chris Radbone	Chris Gascoigne
v1.02	23/10/13	Replace reference to Australian Government PROTECTED Security Manual (PSM) with the PROTECTED Security Policy Framework (PSPF) and update the responsible people.	Chris Radbone	Rob Smetak
v1.03	11/02/15	Security Policy Review	Wayne Kloeden	Chris Radbone
v1.04	19/07/16	Minor updates from Policy Review	Chris Radbone	Rob Smetak
v1.05	30/06/17	Amended name of ‘Research and Analysis’ to ‘Data Integration Unit’, and added Proper and Ethical Use	Chris Radbone	Rob Smetak
V1.06	30/11/18	Updated diagram in Figure 1 and Appendix A (including corresponding notes)	Matthias Schneider	Tony Woollacott
V1.06	30/06/19	Updated – Chief Security Officer, Chief Information Security Officer, “PROTECTED”, “OFFICIAL: Sensitive”, “Baseline” level	Md Shafiqur Rahman Jabin	Chris Radbone

Next Document Review Date: July 2019

Authorisation

Role	Name & Position Title	Signature	Date
Director	Andrew Stanley Director SA NT DataLink		15/07/2019

Security Classification

Document Originator/Owner	Security Classification
SA NT DataLink	OFFICIAL

TABLE OF CONTENTS

1 INTRODUCTION AND BACKGROUND

1.1 Purpose

The *SA NT DataLink Security Manual – Overview* provides an understanding of the security measures and promotes improved security awareness by clarifying 'what' needs to be done to ensure that an appropriate level of security is applied to all aspects of SA NT Datalink operations and activities.

The *Australian Government Protective Security Manual - Controls* provides the basis for the design and implementation of security measures within the SA NT DataLink environment; describing *how* the security measures are to be implemented and *who* is responsible for complying and maintaining them.

1.2 Scope

All activities of the SA NT DataLink come under the authority of the *SA NT DataLink Information Security Management System (ISMS),* including personnel, physical, data and information security, access and use of SA NT DataLink resources.

The Information Security Manual is organised into the following sections designed to provide clear and concise direction and expectations to all personnel involved in SA NT DataLink.

1. Information Security Management System (ISMS);
2. Definitions and Abbreviations;
3. Risk Assessment Methodology;
4. Security Risk Assessment & Treatment;
5. Site Security Plan;
6. Risk Management Plan
7. Information and Security Policy;
8. Security Incident Detection and Response;
9. System Usage, Confidentiality Agreements & Maintenance Requirements;
10. Associated Security Standard Operating Procedures.

1.3 What is Data Linkage?

Data Linkage (also known as record linkage) brings together or links records of an individual, household, business unit or other entity from a number of data sources.

The occurrences of individual transactions of services or records of activity for people are able to be compared by the Data Linkage Unit, in accordance with the 'separation principle'. Using personally identifying variables provided by various data custodians without the content information from each transaction, the records that are deemed to match for the same person able to be linked and considered to belong to the same person, in a combination of deterministic and probabilistic matching algorithms.

1.4 What is SA NT DataLink?

SA NT DataLink is the operational body of the SA NT Data Linkage Consortium responsible as the authorised data linkage facility for South Australian and Northern Territory. The consortium consists of member organisations who have signed the Joint Venture Agreement, which established the formal Governance required to operate the authorised Data Linkage System for South Australia and the Northern Territory.

The privacy protecting processes and practices used at SA NT DataLink have been established in agreement with the Privacy Committee of South Australia and the Northern Territory Information (Privacy) Commissioner.

A short-animated YouTube video describes the SA NT DataLink privacy PROTECTED data linkage system at: www.youtube.com/watch?v=vLYGcbxrIPA

1.5 SA NT DataLink Purpose

SA NT DataLink facilitates approved data access for policy analysis, evaluation and research. It has been established as a trusted party authorised to link data and manage the protection of privacy and confidentiality.

The purpose of SA NT DataLink is to provide policy makers and researchers with the best possible information and evidence through providing the capability to conduct analysis on multiple datasets in a privacy protecting manner. Instead of researchers needing to undertake relatively expensive – and often biased – surveys or having to opportunistically engage with the data custodians, the SA NT DataLink's service builds capacity, knowledge of the datasets and facilitates approved access to de-identified linked data. The 'separation principle' pioneered in Western Australia ensures the highest standards of security and the protection of individual confidentiality and privacy.

1.6 History of SA NT DataLink

The SA Department for Health and Wellbeing (SA Health) and the NT Department of Health are the respective lead agencies in each jurisdiction. SA NT DataLink is legally administered by the University of South Australia and is housed in a secure environment within the SAHMRI building in South Australia. In 2013 the South Australian Health and Medical Research Institute (SAHMRI) and the Health Consumer Alliance of South Australia (HCA SA) joined the SA NT Data Linkage Consortium.

In May 2009 SA NT DataLink was legally established through a joint venture agreement with a consortium of major funders and data providers, the SA Ministers for Health, Education, Mental Health and Substance Abuse, Early Childhood Development, Families and Communities, Housing, Ageing, Disability, and Aboriginal Affairs and Reconciliation, the Northern Territory of Australia, the Cancer Council of South Australia, the Motor Accident Commission, and SA's three public Universities - University of Adelaide, Flinders University and University of South Australia.

In November 2009 SA NT DataLink Unit was officially launched by the SA Minister of Health Hon John Hill, the NT Minister of Health Hon Kon Vatskalis, and the SA Minister for Early Childhood Development and Aboriginal Affairs and Reconciliation Hon Jay Weatherill, and the Executive Director South Australian Department of Education and Children's Services Ms Liz Furler.

SA NT DataLink receives further funding from the Australian Government through support from the Population Health Research Network (PHRN) National Collaborative Research Infrastructure Strategy (NCRIS) to increase the research infrastructure capacity around Australia using privacy protecting data linkage methodologies.

1.7 SA NT DataLink Organisational Structure

In accordance with the SA NT Data Linkage Consortium (Joint Venture) Agreement, the SA NT DataLink Steering Committee has the overall governing role and responsibility for SA NT DataLink. Refer to joint venture agreement for more detail.

Due to datasets being provided by private, State, Territory and Commonwealth and non-government organisations, the SA NT Data Linkage Consortium Steering Committee have classified the Master Linkage File and all data associated with its creation and maintenance, at the 'PROTECTED' level [1]

[1] Australian Government Protective Security Policy Framework, Feb 2019 https://www.protectivesecurity.gov.au/information/sensitive-classified-information/Pages/default.aspx

The Data Linkage Unit has the highest level of security within the SA NT DataLink, operating in accordance with the 'PROTECTED' security classification. The Data Linkage Unit is staffed and operated exclusively by SA Health seconded personnel who are responsible for receiving personally identifying demographic information and authorised to link data and operate on Identity Management Function (IMF) from each organisation's data. The Data Linkage Unit is physically and electronically separate with the data on a standalone environment, not connected to any network or inter-web. Under the authority of Data Custodians, the Data Linkage Unit create Project specific linkage keys and maintain the enduring Master Linkage File (MLF).

SA NT DataLink is comprised of five operational functions, namely:

(1.) Data Linkage Unit
(2.) Client Services – Metadata & Research
(3.) Data Integration Unit
(4.) Administration and Financial Management
(5.) Capacity Building

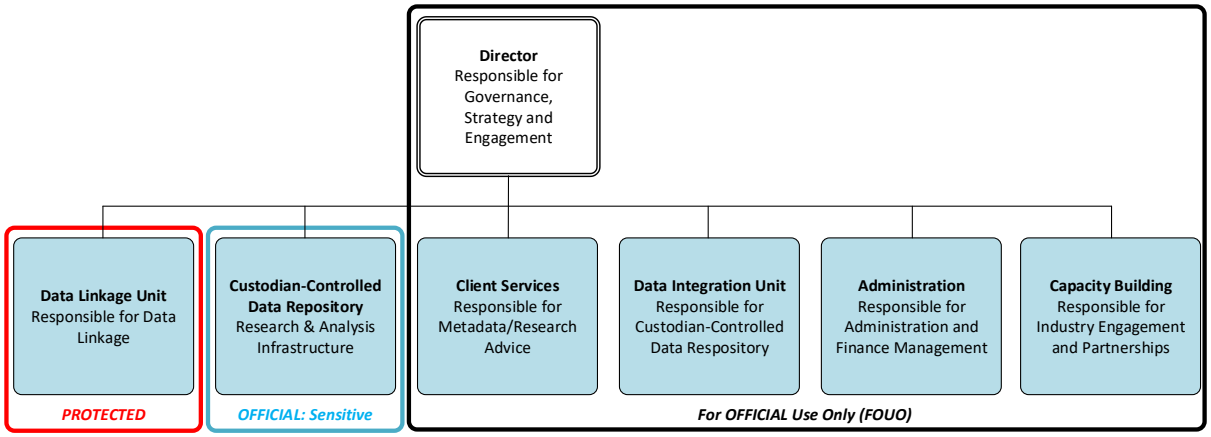

Figure 1: SA NT DataLink Operational Functions and Corresponding Security Classifications

The Data Linkage Unit staff operate in a secure PROTECTED Area specifically designed and operated to protect the data provider into the data linkage system; he Data Integration Unit staff who are responsible for the quality checking and secure access for Research and Analysis are physically located in an area classified at the 'OFFICIAL: Sensitive' level and have secure access to de-identified data (aggregated data without any identifying fields). All other functions and associated personnel are physically located in the 'For Official Use Only' area. The accommodation is designed with a security-in-depth 'onion' approach in that a person has to move through a number of layers with escalating security requirements to achieve access to the higher security levels.

1.8 Information Security and Privacy Protection – Design Principles

Privacy protection underpins all of SA NT DataLink's activities and processes. SA NT DataLink's systems and protocols are based on the highest ethical and privacy standards. Strong security measures and controls have been implemented to prevent inappropriate use or disclosure of personal information held or controlled by SA NT DataLink.

The main design principles are:

- Physical restriction preventing unauthorised access to data containing confidential or private information;

- Separation of roles and responsibilities that make it impossible for any individual other than the data custodian to have access to identified personal and service data;
- All data access and use must be approved by the respective data custodians;
- Only de-identified link (e.g. data) provided by the SA NT DataLink to researchers and policy analysts by the Data Linkage Unit; Data custodians are responsible for authority of releasing their de-identified data direct to the researchers or policy analysts; these data are only provided after the necessary ethics and custodian approvals are obtained.
- Approval for data custodians to releases their data to SA NT DataLink, and the ability for the Data Linkage Unit to receive and undertake linkage with the data in the SA NT DataLink system, requires appropriate approval from the Privacy Committee of South Australia - who endorsed SA NT DataLink's privacy protection protocols in June 2008; in accordance with the Government of South Australia's Information Privacy Principles (IPP's) [2], in accordance with the Information ACT 2002 (NT), Public Sector (Data Sharing) Act 2016 (SA) or the Privacy Act 1988 (Cth)

1.9 Proper and Ethical Use of Data

- SA NT DataLink personnel and Researchers are responsible for using data, information and computing resources in an effective, ethical and lawful manner.
- SA NT DataLink personnel are responsible for safeguarding SA NT DataLink controlled information and the physical assets that store this information.
- SA NT DataLink personnel and Researchers will not be granted access to the SA NT DataLink information and systems without written authorisation and without first reading and signing appropriate agreements.

2 SECURITY BENCHMARKS

The security benchmarks used for SA NT Datalink are the current versions of the:

- Australian Government Information Security Manual (April 2019)
- Protective Security Policy Framework (PSPF) including associated guidelines (Australian Government)
- Information Security Management Framework (ISMF) (South Australian Government)
- *AS ISO/IEC 27002:2005* Information Security Standard Code of Practice
- *ISO 27799:2008* - Health informatics - Information security management in health using ISO/IEC 27002.

The Australian Government comprehensive PSPF provides polices, risk evaluation and associated guidance and the minimum standards for SA NT DataLink's information security addressing potential business impacts from current and future security risks.

2.1 Scope of Security Classification

The security requirements on IT systems, premises and personnel specified in the *SA NT DataLink Security Manual* are focussed on the protection of data classified 'PROTECTED'.

[2] Information Privacy Principles Instruction May 2009,

www.premcab.sa.gov.au/pdf/circulars/Privacy.pdf

In accordance with the PSPF[3] Australian Government business impact levels, the Master Linkage File is assessed by the SA NT DataLink Steering Committee as 'Medium up to High Risk' with a resultant 'PROTECTED' level security confidentiality classification. The Master Linkage file is marked PROTECTED, compared to 'OFFICIAL: Sensitive'[4] for individual files or aggregated de-identified data. This aligns to the definition of sensitive information in Section 6 of the Privacy Act 1998 (Cth).

The Steering Committee's High Risk assessment is supported by the importance of managing aggregated identified data from multiple agencies where erosion of trust, consequences to the public and exposure to legal proceedings is critically important and to be avoided.

2.2 Information Security Standards and Reference Material

The University of South Australia and the South Australian Health and Medical Research Institute have provided the secure physical environment and IT systems to enable handling and storage of the classified data in accordance with the requirements defined in the PSPF. On behalf of the multiple Agencies providing data to SA NT DataLink, the security is reviewed through the IT Security Team.

The information security requirements detailed in the PSPF and its supporting document, Australian Government Information Security Manual (ISM), are consistent with South Government's Information Security Standards, specifically the *Information Security Management Framework* (ISMF) and its associated international standards for Information Security, ISO 27001.

3 RISK ASSESSMENT AND MANAGEMENT

The identification and treatment of potential risks affecting the storage, transfer, delivery and use of SA NT DataLink's operational and strategic activities are managed in the one risk management process, incorporating risks from Information Security, Physical and Asset Management, and Human Resources including Worker Health and Safety.

3.1 Risk Assessment

Risk assessments were undertaken when establishing SA NT DataLink, and are regularly undertaken to identify potential threats to the SA NT Datalink systems, processes and overall information environment with consideration of internal, external and naturally occurring incidents. The process for monitoring risks is part of the ongoing operational management, with High and Extreme Risks presented and reported through to the Steering Committee. Potential impacts and likelihood of each risk occurring are determined, with identification of possible countermeasures to reduce or mitigate the likelihood and/or the impact.

Based on the initial risk assessment and the implementation of risk mitigation and treatment measures, subsequent risk assessments are required to be undertaken and the residual risks monitored on an ongoing basis. The SA NT DataLink Consortium Executive Committee are responsible for reviewing the business and security risk.

[3] Protective Security Governance Guidelines Business Impact Levels, 2019, https://www.protectivesecurity.gov.au/information/sensitive-classified-information/Documents/infosec08-table2.pdf

[4] Information Classification System, Feb 2019, https://www.protectivesecurity.gov.au/information/sensitive-classified-information/Pages/default.aspx

3.2 SA NT DataLink Risk Management Plan

SA NT Datalink's risk management is conducted on a continuous basis and is based upon the ISO 31000:2009. It encompasses the following activities:

- Context and establishment
- Risk Identification
- Risk Analysis
- Risk Evaluation
- Risk Treatment
- Risk Monitoring

The SA NT DataLink Risk Management Plan showing the Extreme and High Risks will be presented to the SA NT DataLink Security Committee and reported to the Steering Committee. As SA NT DataLink or consortium partners identify new risks or controls affecting the information systems, process and environment, the risk documentation is updated to reflect the change. A complete risk assessment is to be conducted annually.

The Chief Information Security Officer (CISO) is responsible for ensuring that the security risk assessment documents and processes are updated and remain current, reporting through the Security Committee to the SA NT DataLink Steering Committee.

The risk monitoring activity is defined in the *SA NT DataLink Risk Management Plan* and reflects the outcomes of all security risk assessment activities. The key objective is to ensure that the risk management process is regularly undertaken, risks updated, and timely and appropriate actions are undertaken to address identified risks.

4 PHYSICAL SECURITY

The *SA NT DataLink Security Manual* contains the *Site Security Plan* which details the necessary security services and protection mechanisms required to securely operate SA NT DataLink system and apply the necessary level of protection to classified information and processes.

The actual measures deployed and maintained by University of South Australia for SA NT Datalink are documented in the *Site Security Plan,* a plan that covers all locations that house equipment used by SA NT DataLink.

4.1 Physical Security Measures

SA NT DataLink, University of South Australia and SAHMRI comply with the physical security requirements for a 'Partially Secure' or Zone-2 areas. The additonal physical and IT security measures in the Data Linakge Unit provides a level of protection for data classified at the 'PROTECTED' level in Zone-3 PROTECTED area, as defined within the Australian Government PSPF.

In accordance with the Australian Government's Protective Security Policy Framework (PSPF) and associated guidelines and Physical Security 'Controls', a "security-in- depth" approach is used with a series of physical and electronic barriers to prevent unauthorised access and transmission of PROTECTED data. This approach sets in place mechanisms to detect and respond to security breaches within an acceptable timeframe.

The 'PROTECTED' area houses all IT equipment used by the Data Linkage Unit, and complies with the minimum physical security requirements for an Intruder Resistant Area, as follows:

Walls must extend from the base of the floor to the underside of the above slab or secured roof structure,

The roof and floor must be concrete slabs that form part of the existing structure,

All points of entry into the room must be secured and the perimeter doors electroncially monitored and controlled. The access control system is used to restrict entry.

Double cylinder deadlock mortise locks must be used to secure the area during non-operational hours and when it is unoccupied for extended periods,

Ducts, service risers and other openings that pierce the room's perimeter are appropriately secured by barriers are required to be constructed from AS1304:1991 F81 steel mesh welded into steel frames. The steel frames must:

- Be constructed of steel angle with minimum dimensions of 30mmx30mmx3.5mm, Have a continuous perimeter, and
- Be fixed to the walls and underside of the roof at a maximum of 500mm centre with either:
    - 25mm welds; or
    - tamper resistant 6mm diameter bolts (bolts can be made tamper resistant by welding them to the frame).

All IT storage devices containing information classified at the 'PROTECTED' level must be housed in Class 'C' containers, and all IT storage devices and media containing information classified at 'OFFICIAL: Sensitive' level and 'For Offical Use Only' must be housed in an approved lockable commercial grade cabinets.

4.2 Site Security Plan

The *Site Security Plan* is a controlled document describing the physical security required for the buildings that house the information stores and IT equipment used to process data for SA NT DataLink. The plan documents how the proposed measures and procedures will reduce the risks to an acceptable level and includes the following:

The location and nature of the site,

The security classification of information to be stored, handled, processed or otherwise used in each part of the site,

Any other resources that will be on the site,

An indication of the required security designation of each distinct area in the site,

The protective measures required for

- the site as a whole,
- particular areas within the site (for example, part of a floor which will hold information of a higher classification than the rest of the site),

The differing measures that will be required for

- operational hours,
- non-operational hours,
- storage, handling and processing of security classified information, and
- security classified or otherwise sensitive discussions and meetings.

The *Site Security Plan* also includes system security plans; one for the 'PROTECTED' area and the other for the 'OFFICIAL: Sensitive' area. The *Site Security Plan* details the following:

- All IT and related equipment involved in the storage and processing of security classified information,
- The high-level security architecture and specific policies that are to be enforced within the system, and for each interconnection, and
- How the relevant policies and controls detailed in the risk management plan will be implemented.

5 INFORMATION AND TECHNOLOGY SECURITY

The *SA NT DataLink Security Manual* includes the *Site Security Plan* which details the necessary security services and physical protection mechanisms required to securely operate the SA NT DataLink IT data and information appropriately, and the framework and Technology Security (refer to section 4 - *Physical Security* above for further details).

As a baseline, the required level of security is achieved by implementing a minimum set of security controls to protect against the most common threats, with additional controls implemented for technical and non-technical safeguards.

Technical controls relate specifically to the provision of Information and Technology services. Non-technical controls are of a general nature and include those that provide physical, administrative/procedural and personnel security.

Controls will perform one or more of the following functions:

Deter – Avoid or prevent the occurrence of an undesirable event,

Protect – Safeguard the information assets from adverse events,

Detect – Identify the occurrence of an undesirable event,

Respond – React or counter the adverse event, and

Recover – Restore the integrity, availability and confidentiality of information assets to their expected state.

The combination of the above types of security measures will achieve an effective level of security known as 'Security-In-Depth', where each control provides further resistance to a threat with the aim of minimising the impact and/or likelihood of that threat.

5.1 Technical Control Measures

The following list defines typical security baseline' IT control measures implemented as part of the systems deployed by University of South Australia for SA NT DataLink:

- Content controls (for malicious code, inappropriate content, etc.);
- User activity and event logging;
- Intrusion detection;
- Access controls;
- User authentication;
- Encryption;
- Firewalls;
- Redundancy and backups;
- Operating system and application hardening (ie. configuration to restrict services/open ports 5); and
- Environmental controls within IT areas.

The following specific control is deployed were determined during the risk assessment and design activities;

The SA NT DataLink Information Security Management System (ISMS) is located in a secured location, with restricted access. This is used for the following purposes:

1. Storage and auditing of log files;
2. Security administration, including management console for security components;
3. Audit the controls for transferring data from one party to another; and
4. Security configuration checks and auditing.

5.2 Information Flows

Appendix A provides a high-level diagram of the data flows required within the IT environment.

The only encrypted and password PROTECTED information is transfer from the 'PROTECTED Area' with secure transfer between the Data Custodian and the Data Linkage Unit using approved electronic file encryption transfer technology or safe hands. All information flaws must be authorised, and encryption of data transferred is required.

Identified PROTECTED data will not be transferred to the 'OFFICIAL: Sensitive' environment, unless it has been approved and checked independantly.

Data Custodians and the Data Linkage Unit are obligated under formal and legal agreements to not release PROTECTED classified data without authorisation, and to personnel protect all data provided by Data Custodians.

The University of South Australia do not require access to 'PROTECTED' data to fulfil their security consulting and contractual IT service obligations. Approved Researchers and Analysts will only require access to 'OFFICIAL: Sensitive', de-identified data for their approved use. This approach will enhance the level of security that can be applied to the Data Custodians and Linkage Unit data by minimising the number of people

[5] Leaving unnecessary services and open ports on IT devices can result in compromise through exploitation of inherent vulnerabilities in the services.

requiring access to 'PROTECTED' level data. The guiding principle used by SA NT DataLink for creating a more secure environment, and thereby reducing the risk level, is to limit availability or access to the to those with a 'need to know' [6].

5.3 Non-Technical Control Measures

The required non-technical control measures associated with the IT environment are specified at section 4 - *Physical Security,* section - and section 10 - *Administrative/Procedural Security.*

5.4 Information and Security Policy

The *SA NT DataLink Information and Security Policy* supports the *SA NT DataLink Security Manual* by specifying the protocols and expected activities and actions. The following table provides an overview of the sections and content included in the *SA NT DataLink Information and Security Policy*.

ID	Security Control	Scope
1	Information Security Management System	An overview of Information Security Manual
2	Definitions and Abbreviations	Maintenance and important definitions and abbreviations for Information Security Manual
3	Risk Assessment Methodology	SA NT DataLink Security Risk Management – Checklist of Controls
4	Security Risk Assessment and Treatment	Findings of the risk assessment conducted for SA NT DataLink in accordance with the methodology outlined in the Risk Management Framework
5	Site Security Plan	Application and maintenance of an appropriate level of security within the physical and the information communications technology (ICT) and data security environment with SA NT DataLink.
6	Risk Management Plan	Risk assessment and continuous management and monitoring the overall level of security risk and maintaining an acceptable level of risk throughout the SA NT DataLink environment.
7	Information and Security Policy	Defining the policies for the University of South Australia in collaboration with SA Health, to implement the physical, logical and information technology security requirements and controls to support the SA NT DataLink business objectives and operating environment.
8	Security Incident Detection, Response and Forensics	Security auditing, security breach detection and response, incident reporting and forensic evidence requirements.
9	System Usage, Confidentiality Agreements and Maintenance	Defining the confidentiality agreements that are to be read and signed by personnel requiring access to the SA NT DataLink information and environment.
10	Security Standard Operating Procedures	Ensuring the ongoing security of the measures deployed within the SA NT DataLink Information and Technology environment

[6] Australian Government Protected Security Manual (2006) paragraph C2.4.

5.5 Secure Gateway

While the 'PROTECTED' environment only receives data via the 'safe hands' method rather than automated electronic file transfers, and it is on a stand-alone Network, with no direct external electronic connections, and no special gateway architecture is required.

Restricted physical access to the 'PROTECTED' and 'OFFICIAL: Sensitive' area is provided via SAHMRIs building access protocols, monitoring and tracking who has access to this area. Access to data is agreed by Data Custodians on a case by case basis.

Gateway-specific contributing policies, designs and management plans are not necessary while "safe hands" is the only method of data delivery and receipt into the PROTECTED Area and Network.

If the method of data delivery is changed, the need for gateway management and delivery methodology will need to be revisited.

6 SECURITY INCIDENT DETECTION AND RESPONSE PROCEDURE

The security incident response procedure documents the steps to be taken when a security incident is suspected to have occurred. This procedure covers the following issues:

- Incident identification,
- Incident containment, including minimising the impact, classification, forensics, investigation and notifying affected parties,
- Incident eradication,
- Incident recovery, and
- Follow-up, including preventing re-occurrences and disciplinary actions

The security incident response procedure includes a forensic review, which is needed to ensure that potential evidence associated with an incident can be handled such that it will be admissible in a court of law, if required at a later stage. The forensic review details the necessary evidence handling process, covering the following:

- Evidence collection rules,
- Chain of custody, and
- Controlling and recording access.

7 SYSTEM USAGE AGREEMENTS

SA NT DataLink must ensure that every person working in either the 'PROTECTED' or 'OFFICIAL: Sensitive' environments understand their security responsibilities and signs a suitable usage / confidentiality agreement indicating their acceptance of all associated responsibilities.

There are three levels of personnel accessing the PROTECTED and OFFICIAL: Sensitive data and information systems environment, which are:

1. SA Health employees working in the PROTECTED area,
2. University staff working on an ongoing basis and part of the SA NT DataLink staff, providing technical system support to SA NT DataLink, and OFFICIAL: Sensitive data in the Data Integration Unit.
3. Contactors employed by the University to undertake work of a technical nature for SA NT DataLink.

Only after signing the relevant Non-Disclosure Deeds and Usage Agreement(s) and gaining appropriate clearances can the personnel be provided with a password to access the system(s).

8 SECURITY STANDARD OPERATING PROCEDURES

Security Standard Operating Procedures (SSOPs) are instructions to all staff, administrators and managers on the procedures required to ensure the secure operation of SA NT DataLink is undertaken in accordance with the SA NT DataLink Security Policy. The primary function of the SSOPs is to ensure the effective implementation of and compliance with the *SA NT DataLink Security Manual*.

The SSOPs are provided for the following functional roles and reflect the different security responsibilities:

- Chief Information Security Officer (CISO),
- Chief Security Officer (CSO),
- IT User Access Administrator,
- Database Administrator,
- Gateway / System (Network and Hardware) Administrator,
- SA NT DataLink personnel, including Data Linkage Unit personnel and Contractors, and
- SAHMRI Building Security and University of South Australia Security Officers.

9 PERSONNEL SECURITY ACTIVITIES & RESPONSIBILITIES

9.1 Security Vetting

The *SA NT DataLink Information and Security Policy* defines the high-level access controls and usage requirements, covering the following areas:

- Personnel vetting,
- Non-disclosure agreements,
- Usage agreements,
- Roles and responsibilities,
- Security awareness training and briefings,
- Reporting security incidents and breaches, and
- Disciplinary action.

In accordance with the PSPF and the required security protocols which have been implemented for managing Commonwealth Data, all personnel handling Commonwealth data classified at the 'PROTECTED' level require security vetting and clearance up to the 'Baseline' level prior to being granted access, as agreed with the Data Custodians.

The SA NT Data Linkage Consortium Steering Committee has agreed that personnel accessing PROTECTED or OFFICIAL: Sensitive data must sign the non-disclosure deeds and usage agreements and require DHS (formally DCSI) Child-Related Employment Clearance. The DHS Child Related Clearance exceeds the National Police Check and relevant Risk Assessment that includes all spent convictions and charges [7]. The Steering Committee decided that until higher levels of vetting are required for the unit by a data custodian, that vetting in the form of a current DHS child-related screening including national police check, will suffice for all SA NT Datalink personnel accessing data clearance.

[7] SA Department for Communities & Social Inclusion (DCSI)
http://screening.dcsi.sa.gov.au/screening-process/types-of-screening/child-related-employment

Personnel with access to SA NT Datalink data that is classified up to the 'OFFICIAL: Sensitive' level will not undergo a security clearance at the 'Baseline' level. Vetting in the form of a current DHS Child Related Clearance check will be required to check the security of all SA NT Datalink personnel.

All personnel involved in SA NT DataLink will be required to sign a *SA NT DataLink Staff Confidentiality Acknowledgement* form prior to being granted access to any sensitive information.

All personnel involved in SA NT DataLink will be made aware of their security responsibilities. Personnel security roles and responsibilities have been outlined in section 9 - *Personnel Security Activities & Responsibilities* and the requirements for the security awareness program have been outlined in section 11 - *Security Awareness Program.*

Personnel are required to report any suspicious activity, and disciplinary action will be taken against individuals responsible for compromising security. Details of these requirements are defined in the Security Incident Detection and Response Procedure.

9.2 Security Activities

Figure 1 and Appendix A provides a diagram of SA NT DataLink Security Functional roles.

The SA NT DataLink CISO is responsible and will oversee the performance of the following security related activities for SA NT Datalink:

- Security Management,
- Database Administration,
- Security Analysis/Review,
- Gateway / System (Network and Hardware) Administration, and
- User Administration.

Note that even though a single person may fill these roles, the individual responsibilities of each of the activities have been specified separately in this framework document.

9.3 Delegates

In certain situations, there may be a requirement to appoint a delegate to be responsible for the security activities.

The appointment of delegates should only be made by the CISO. The CISO must provide the delegate with a clear understanding of the responsibilities associated with the appointment.

9.4 Security Responsibilities

In general, all SA NT DataLink personnel will be responsible and held accountable for the compliance to the *SA NT DataLink Security Manual* and associated procedures. Whilst the CISO is responsible for maintaining the *SA NT DataLink Information and Security Policy* and associated procedures, all personnel are required to be aware and actively manage security risks. In fostering the required security environment and systems, the CISO will ensure the following key activities are conducted:

Planning and Assessment – Maintain all security-relevant policies, plans and procedures;

Enablement – Provide the SA NT DataLink with security-enforcing and security-supporting functionality, knowledge, skills and processes;

Education – Educate all relevant personnel on security issues, policies and requirements to which they must comply;

Operation – Complete all security tasks required to maintain the security of SA NT DataLink IT and information resources;

Verification – Monitor and verify compliance to security policies;

Audit – Log file review;

User Provisioning – Maintain user accounts; and

Incident Response – Respond to reports of irregular system behaviour, unauthorised system access and inappropriate user activities.

Position descriptions for the security roles should be documented, in accordance with SA Health, University of South Australia, and SA NT DataLink Human Resources requirements.

9.4.1 Security Management

The SA NT DataLink CISO role has ultimate responsibility for maintaining the security of SA NT Datalink system including building, personnel and IT. In SA NT DataLink, the CISO role will report to the SA NT DataLink Director.

The responsibilities of the CISO role are to:

- Develop and maintain all security-related principles, policies and procedures,
- Provide SA NT DataLink with security-enforcing and security-supporting functionality, knowledge, skills and processes,
- Identify, assess and manage all security risks,
- Investigate, respond to and report on security incidents,
- Educate personnel on the relevant security issues, policies and procedural requirements with which they are to comply,
- Presenting new users with the Usage Agreement and obtaining sign-off prior to allowing the user to access SA NT Datalink systems/information, and
- Actively lead and facilitate the risk assessment and risk management reporting activities, in conjunction with members of the Security Committee.

9.4.2 Database Administration

The responsibilities are to:

- Create and maintain code to provide the desired views and linkages with the data entrusted to SA NT DataLink by Data Custodian.
- Define the database views to be used by the researchers, and
- Assess the effectiveness of security solutions that are in place.

9.4.3 Security Analysis/Review

The responsibilities are to:

- Analyse and assess compliance with the SA NT DataLink Information and Security Policy
- Verify system and component configurations
- Develop, optimise, implement and audit the security log files
- Ensure compliance by third parties with the security obligations of SA NT DataLink.

9.4.4 Gateway / System (Network and Hardware) Administration

The responsibilities are to:

- Manage and maintain security processes,
- Assess the impact of configuration changes on the security of components,
- Assess the effectiveness of security solutions that are in place,
- Deploy new security solutions in accordance with direction from the CISO and/or the Director SA NT DataLink, and

- Advise and assist Information Systems staff in addressing technical security issues.

9.4.5 User Administration

The responsibilities are to:

- User account creation allowing personnel access to information systems,
- Complete user administration tasks, in accordance with SA NT Datalink Information and Security Policy, and
- Conduct security reviews of user access privileges and profiles, and report potential and identified problems to the SA NT DataLink the SA NT Datalink Chief Information Security Officer.

9.5 Additional Security-Related Responsibilities

There are a number of additional roles relevant to the security of the SA NT Datalink Information environment. The security-relevant activities of the additional roles are as follows:

SA NT DataLink Director as the Chief Security Officer (in accordance the PSPF) is responsible for:

- Approving updates, the SA NT DataLink Security Manual, including the SA NT DataLink Information and Security Policy
- Ensuring reporting of any security incidents to Data Custodians and the SA NT DataLink Consortium Steering Committee, in accordance with the contractual obligations.

University of South Australia Security Officers are responsible for protecting personnel, and assets within the University' control.

The South Australian Health and Medical Research Institute (SAHMRI) building security are responsible for protecting the personnel and assets with SAHMRI.

All of the security-relevant activities conducted by these parties are to be in accordance with the SA NT DataLink Security Manual and the SA NT DataLink Information and Security Policy, supporting procedures, and the direction of the CISO.

10 ADMINISTRATIVE/PROCEDURAL SECURITY

Administrative and procedural security measures are defined in section *9 Personnel Security Activities & Responsibilities*. The effectiveness of these measures is based on personnel appropriately interpreting and implementing the documented processes, hence personnel security is essential in supporting administrative security.

The *SA NT DataLink Security Manual* addresses ten main areas, namely:

1 Information and Security Management System (ISMS)
2 Definitions and Abbreviations
3 Risk Assessment Methodology
4 Security Risk Assessment and Treatment
5 Site Security Plan
6 Risk Management Plan
7 Information and Security Policy
8 Security Incident Detection and Response
9 System Usage, Confidentiality Agreements and Maintenance Requirements
10 Associated Security Standard Operating Procedures

10.1 Security Awareness Training Package

The security awareness training package includes the following components:

- Security awareness checklist for SA NT DataLink personnel, and
- Security awareness checklist for personnel working in the 'PROTECTED' Area.

Refer to section 11 - *Security Awareness Program* for further details of the security awareness training program required for SA NT DataLink.

10.2 Document Management

10.2.1 How the documents fit together

The *SA NT Security Manual* comprises the Security Overview, which is 'For OFFICIAL Use' and is available as an open document to Data Custodian and other to demonstrate SA NT DataLink's commitment to security and protecting privacy, and the information security management practices. The remaining sections in the *SA NT Security Manual* are 'OFFICIAL: Sensitive', noting some of the security configuration setting and details are classified as 'PROTECTED'.

10.2.2 Document Ownership

The owner of the *SA NT Security Manual* is the CISO, and is responsible for ensuring that it is maintained, approved and distributed, under the authority of the Director SA NT DataLink.

10.2.3 Document Approval

Typically, the approver is the SA NT Datalink Director, with peer review provided by the SA NT Data Security Committee, with assurance on behalf of the SA NT DataLink Consortium member organisations provided independently by the SA Department for Health and Ageing (SA Health) IT Security Advisor.

10.2.4 Document Maintenance

The *SA NT Security Manual* will be formally reviewed annually, with sections updated as required on a basis of needs. The security risks identified and updated in the *SA NT DataLink Risk Management Plan*.

10.2.5 Document Distribution

The distribution of the full *SA NT Security Manual* is restricted and controlled by the CISO.

Policy statements and supporting procedures should only be distributed to personnel with a 'need to know'.

The CISO is responsible for distributing and communicating new versions of the Security Manual documents as they are approved.

When security documentation is distributed it should be accompanied with a reminder of the associated non-disclosure requirements.

10.2.6 Document Hierarchy

The diagram provided at Appendix B shows the hierarchy of the SA NT DataLink security documentation.

11 SECURITY AWARENESS PROGRAM

Security awareness is recognised as an important factor in maintaining a security culture of compliance and effectiveness across the organisation.

The CISO is responsible for training personnel on Information Security principles, and ways to safeguard potential vulnerabilities of sensitive systems and information to which they have access for their role in SA NT DataLink. Such training will be designed specifically for employee functions, including system administrators and system users.

The CISO is responsible for documenting, implementing and maintaining a security awareness program. This program comprehensively addresses relevant information security concerns associated with the SA NT DataLink.

The CISO ensures the security awareness program educates personnel on issues and procedures that affect their duties and working environment, such as:

- Security features and limitations specific to SA NT DataLink's systems and applications to perform their duties,
- Relevant and new security issues and vulnerabilities,
- Circumstances that constitute a security breach, violation or concern, and
- Procedures for reporting security breaches, violations or concerns.

The security awareness will be demonstrated through such means as:

- Usage Agreements,
- Confidentiality Agreements,
- Documented information security briefings,
- Security notices, pamphlets, posters, and signs,
- Security videos, and a
- Program of security training, including checklists.

The CISO will be responsible for conducting security briefings with personnel and contractors who will be required to access SA NT DataLink data and information systems. These briefings are to advise of:

- The access requirements of their employment or contracted position,
- Their authorised security level,
- Their responsibilities for safeguarding classified information and assets,
- Consequences of failure to safeguard classified information and assets,
- Relevant security and privacy legislation applicable to their duties, and
- Relevant corporate security rules and regulations.

The CISO will conduct security briefings individually where possible, and issue a current document outlining the contents of the briefing in the form of a checklist, the date given, to be signed as indication of the receipt, understanding and agreement of the issues discussed in the briefing.

12 APPENDIX A - HIGH-LEVEL DATA FLOW DIAGRAM

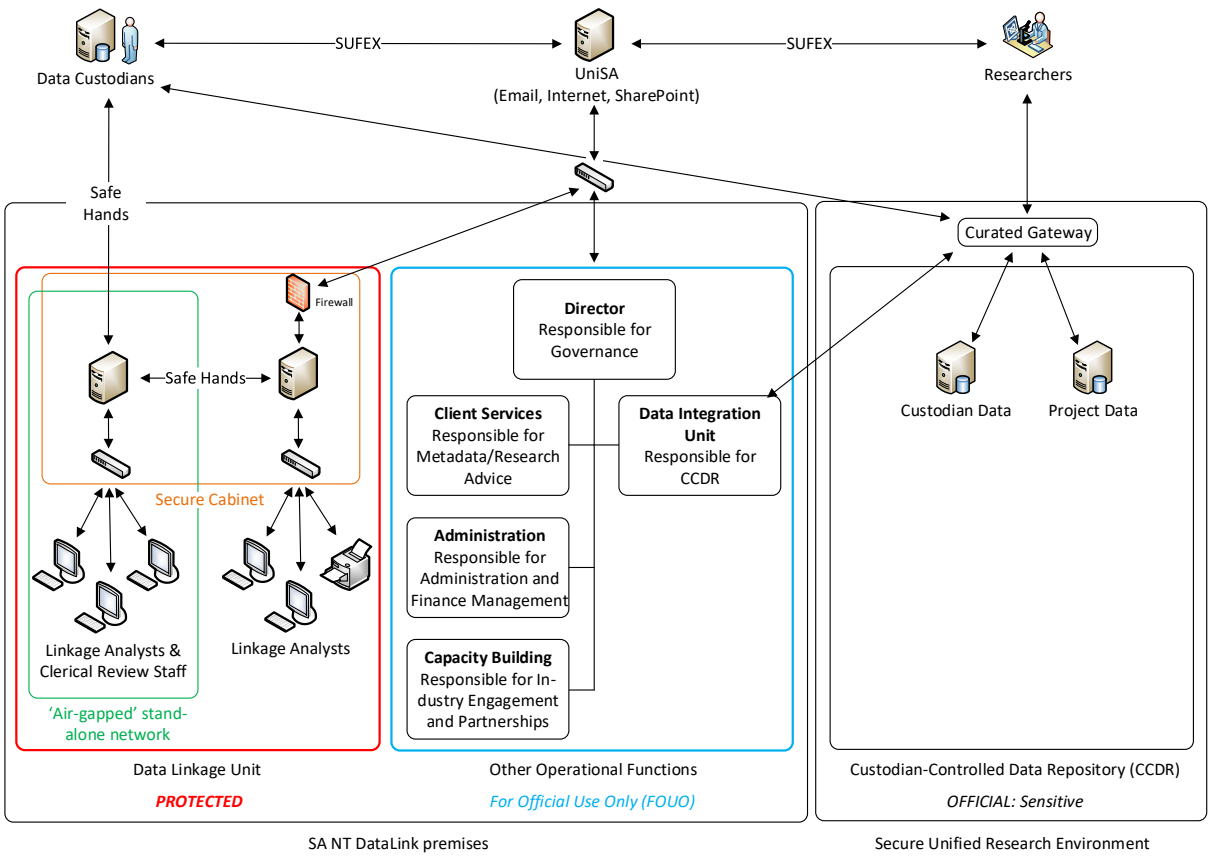

Figure 2: High-Level Data Flow Diagram and Corresponding Security Classifications

Notes:

1 The classification process will increase the protection afforded to Data Custodian and Data Linkage Unit data by implementing the 'need to know' principle, whereby the number of people with access to data classified at the 'PROTECTED' level is minimised.

2 The SA NT Datalink is secured in accordance with 'intruder resistant' requirements, as a minimum. The preferred and target level of physical security is 'partially secure'.

3 The 'PROTECTED' environment is physically separated from the 'OFFICIAL: Sensitive' environment, and access tightly controlled.

4 The Secure Unified Research Environment (SURE) provides the secure platform to manage data classified as 'OFFICIAL: Sensitive' in the Custodian-Controlled Data Repository (CCDR). All data transfer into and out of the CCDR are managed by the Curated Gateway, controlled by the Data Integration Unit. Researchers are granted access to the approved project data only in private sub-workspaces in the CCDR. Data custodians are able to access to their respective datasets in private sub-workspaces within the CCDR.

APPENDIX B - SECURITY DOCUMENT HIERARCHY