INTRODUCTION

In completing an IT Security Risk Assessment, researchers should identify the IT security risks relevant to their research proposal and what controls are in place to mitigate those risks. While the following are a guide to identify the potential risks and controls, they are not exhaustive and researchers may need to consider additional risks or controls depending on their individual proposals. Not all risks or controls will be relevant to all research proposals and some controls may assist in mitigating multiple risks. The identified controls should be clearly articulated in the Ethics Application Form.

Data refers to research data provided by the Department of Health, an alternative source, or as collected by the researchers themselves.

TECHNOLOGICAL SECURITY

Potential Risks	Mitigating Control Examples
A. Researcher's organisation does not follow good IT security governance, resulting in poor IT security practices	1. The organisation's IT Security practices are regularly subject to internal, external or quality audits 2. The IT security environment is baselined against an appropriate standard eg. ISO 27001 3. An approved and up-to-date IT Security Policy is in place at the organisation 4. All users are required to adhere to an IT Acceptable Use Policy 5. All research personnel must sign a confidentiality agreement 6. Researchers are required to undertake regular IT security training 7. Researchers are required to undertake regular privacy training
B. Data sovereignty issues result in research data stored outside of Australia being exposed or lost	8. Data resides within Australia 9. Data is encrypted at rest 10. Hosting service does not have access to encryption keys
C. Data stored on a portable device is lost or stolen resulting in exposure or loss of data	11. Data will not be transferred physically via a thumb drive, an external drive or laptop 12. Portable drives and devices are physically secured when not in use 13. Data stored on portable drives and devices is encrypted 14. Audio/Video recordings are erased from the recording device as soon as the data is securely transferred to a secure location
D. Unauthorised access to researcher's personal computer results in exposure or loss of data	15. Personal computers are kept within a secure area with access restricted to researchers 16. All users are required to have a unique login and password 17. Sharing of logins and passwords between users is prohibited 18. Personal computer screens lock automatically after 5 minutes of inactivity

Potential Risks	Mitigating Control Examples
E. Unintended erasure or corruption of data	19. Data is regularly backed up to a remote secure location 20. Recovery of backups is regularly tested
F. Unauthorised access to backups results in exposure or loss of data	21. Backup of data is encrypted with access restricted to authorised IT personnel only
G. Personal computers or servers subject to ransomware, malware or virus attack resulting in exposure or loss of data	22. Application controls prevent the execution of unapproved or malicious programs 23. The latest versions of applications are used and promptly updated/ patched 24. User application hardening to block malicious content eg. web browsers configured to block Flash, adverts and Java 25. Microsoft Office macro settings are configured to only allow trusted macros 26. Personal computers and servers used are configured and maintained by the organisation 27. Operating systems are automatically or regularly patched and updated 28. Up-to-date anti-virus and anti-malware software is installed
H. Insecure remote access leads to unauthorised exposure or loss of data	29. Researchers are required to adhere to a remote access policy 30. Remote network access requires multi factor authentication (MFA) 31. Remote access utilises virtual private network (VPN) or similar for secure end-to-end connection 32. Sensitive data unable to be downloaded to client side through remote access
I. Insecure network results in unauthorised exposure or loss of data	33. Network activity and traffic is logged and actively monitored by IT personnel 34. The network is regularly scanned for internal and external vulnerabilities 35. The network is regularly subject to external penetration testing 36. External access to the network is restricted or blocked 37. The network is protected by a firewall that is actively managed 38. Network login passwords have adequate complexity requirements e.g. minimum number and enforced mix of characters 39. Passwords are regularly required to be changed and cannot be re-used 40. The network is segmented to deny or restrict traffic between computers unless required
J. Unauthorised access to data stored on a server results in exposure or loss of data	41. Entry to the physical location of the server is restricted to authorised IT personnel only 42. Access to data on the server is limited to authorised researchers only 43. Data stored on the server is encrypted at rest
K. Data is at higher risk of security breach by external party due to commercial or research value	44. Data is subject to enhanced security monitoring and controls 45. MFA required for all to access data

PHYSICAL SECURITY

Potential Risks	Mitigating Control Examples
L. Unauthorised access to hard copy files results in exposure or loss of data	46. Hard copies of data and related physical records are locked in secure physical record storage when not in use

TRANSPORT

Potential Risks	Mitigating Control Examples
M. Data is lost, corrupted or exposed while transferred to, by, or from the researcher	47. The secure electronic transfer of data should be via MyFT or similar 48. The emailing of data is not allowed 49. The faxing of paper-based records and/or data is not allowed
N. Data collected from research participants via an insecure mobile app is exposed or lost	50. Data on the app is encrypted at rest and only accessible to the user 51. App data is up-loaded to a secure server using end-to-end encryption 52. Data stored on the server is encrypted at rest and only available to the Researchers via end-to-end encryption
O. Insecure collection of survey data	53. Survey web server, and database server are separated, with the database behind a firewall 54. The download of the survey results is secure 55. Survey results are only accessible to the researchers 56. Survey results are securely erased from the survey platform after transferred to researchers

IDENTIFIABLE DATA

Potential Risks	Mitigating Control Examples
P. De-identified data is re-identified without appropriate approval	57. Research data is de-identified when linked and associated with a randomly assigned ID number 58. Data is de-identified and linked prior to be being used by researchers 59. Researchers do not have access to identifiable data
Q. Data not used for intended purpose	60. Researchers formally agree data is only to be used for the study authorised by HREC and by individuals identified in proposal 61. Researchers seek approval from HREC for any changes from the agreed intended use of the data
R. Identifiable data is reported publicly without consent	62. Researchers ensure data pertaining to a single or particular individual will not be reported 63. Researchers ensure identifiable data will not be reported

RETENTION AND DISPOSAL PLAN

Potential Risks	Mitigating Control Examples
S. Exposure or loss of archived data prior to disposal	64. The data and records created as part of the research, are Included in a defined retention and disposal schedule as part of a managed record keeping system 65. The retained data is encrypted and stored in a managed and secure environment 66. Access to the retained data is restricted
T. Inadequate data disposal process results in failure to dispose of data or exposure of data	67. There is a documented secure digital erase procedure 68. Disposal process includes secure disposal of backups 69. There is a secure disposal process for physical records 70. Researchers to inform HREC when the data is destroyed