DISP Handbook

Information Security Office

The Australian National University

Canberra ACT 2600 Australia

https://services.anu.edu.au/business-units/information-security-office

CRICOS Provider No. 00120C

Table of Contents

Chapter 1: DISP Security Program Procedural Guidance....3

Purpose....3

Overview....3

Scope and Inclusion....3

Standards....3

Governance....5

Breaches and non-compliance....8

Chapter 2: DISP Physical Security....9

Aims and Objectives....9

Scope and Inclusion....9

Roles and Responsibilities....9

Policy Statement....9

Chapter 3: DISP Personnel Security....14

3.1 DISP Employee Screening....14

3.2 DISP Personnel Travel....15

Chapter 4: DISP Information and Cyber Security....17

4.1 Application Control....17

4.2 Privileged Access Management....18

4.3 Vulnerability and Patch Management....21

Appendix A: Resources....26

Definitions....26

Legislation....26

Appendix B: DISP Personnel Private Travel....28

Appendix C: DISP Personnel Official Travel....30

Chapter 1: DISP Security Program Procedural Guidance

Purpose

This Handbook outlines The Australian National University's ('the University's) ongoing Defence Industry Security Program ('DISP') responsibilities to ensure that DISP membership is upheld.

Overview

The DISP assists in securing Defence capability through strengthened security practices in partnership with industry and enhances Defence's ability to manage risk in the evolving security environment.

The University must continue to meet the ongoing eligibility and suitability requirements, as outlined in the Defence Security Principles Framework (DSPF) *Principle 16* and *Control 16.1 Defence Industry Security Program* to maintain DISP membership. This Handbook provides a *'working guide'* for the University Information Security Office and all relevant personnel to implement security measures required by the DSPF.

The University has applied for DISP membership at the following levels:

- Governance Security: Level 1
- Personnel Security: Level 1
- Physical Security: Entry level
- Information & Cyber Security: Entry level

This Handbook also exists to improve transparency, to support the audit and assurance activities for DISP membership and to streamline the University's efforts in communicating with Defence Industry Security Office (DISO) during an audit.

Scope and Inclusion

This Handbook applies to the University's DISP personnel who are working on projects that require DISP membership.

This Handbook also applies to the physical location listed under the University's DISP membership – the ANU DISP location at the Physics Building, Building #160, 60 Mills Road, Acton ACT 2601.

Standards

DISP Responsibilities

1. The position of Chief Security Officer (CSO) is held by the University's Chief Information Security Officer (CISO) and therefore they maintain the ability to implement policy and direct resources. They have obtained and maintain a minimum Baseline Security Clearance.

    Name: Suthagar Seevaratnam

    Email: ciso@anu.edu.au

2. The CSO is responsible for oversight of, and responsibility for, security arrangements and championing a security culture at the University. The CSO is accountable for ensuring:
    a. All obligations contained in the DISP principle and control policy documents for their level of membership are met.
    b. An appropriate system of risk, oversight and management is maintained.
    c. DISP reporting obligations are fulfilled, including the DISP Annual Security report annually from the date membership is granted.
    d. Any sensitive and classified materials entrusted to the University are safeguarded at all times.
    e. Security Officer(s) are appointed to develop and implement the University's security policies and plans, on the CSO's behalf.
    f. The DISP Annual Security Report is reviewed by Council through the University's Audit, Risk and Management Committee (ARMC) and all recommendations are implemented within agreed timeframes; and
    g. Any change in Foreign Ownership Control and Influence (FOCI) status of the University is reported to Defence via the *FOCI Declaration webform (AE250-1)*.
3. The Security Officer (SO) is responsible for the development and implementation of the DISP security policies and plans and acts on behalf of the CSO. The SO is an Australian citizen and maintains a minimum Baseline Security Clearance as appropriate with the level of DISP membership.

    Name: Amy Holland

    Email: DISP@anu.edu.au
4. The SO is responsible for:
    a. The development and application of DISP security policies and plans within the University.
    b. Ensuring sensitive and classified materials entrusted to the University are always safeguarded.
    c. Maintaining the Designated Security Assessed Position register.
    d. Maintaining the Security Governance Register (SGR).
    e. Facilitating annual security and insider threat awareness training of relevant personnel.
    f. Reporting security incidents, fraud incidents, and contact reports, in accordance with Defence requirements; and
    g. Yearly assurance activities to support the CSO.

Governance

Security Policies and Plans

5. This Handbook is maintained by the SO to provide all DISP relevant and Defence cleared staff with a guide to their individual security responsibilities.

6. All relevant staff are required to read this Handbook annually as a reminder of their individual responsibilities and sign the declaration.

7. DISP personnel must abide by the applicable local security instructions.

Security Risk Assessments (SRAs) & Security Risk Register (SRR)

8. The University maintains SRAs to identify and manage risks. Additionally, a more specific SRA is maintained relating to any Defence contract the University is working on. The University's SRAs are conducted in accordance with the Risk Management Policy and Risk Management Framework. The SRAs are located in the University's Information Security Office in a Governance Risk and Compliance system.

9. Complementary to the SRAs, the SRR, located in the University's Information Security Office in the Governance Risk and Compliance system, captures the risk response to threats for specific assets or operations.

Security Governance Register (SGR)

10. An SGR is maintained by the SO in the Governance Risk and Compliance system to capture all matters of security interest to the University.

Delegated/ Required Security Assessed Positions Register (DSAP/ RSAP)

11. Personnel must be security cleared to the level of classified information or assets they are required to access or the level of responsibilities they hold.

12. The SO is responsible for identifying positions, maintaining a register of those positions, and assuring those personnel are suitable to access:

    a. Classified information, materials, and assets.

    b. Defence/Industry entity ICT systems; and

    c. Classified areas.

13. The University DSAP/RSAP register is located within the SGR.

Foreign Ownership Control and Influence (FOCI)

14. The University is obligated to report all potential or actual changes to their Foreign Ownership Control and Influence status. The SO reports all FOCI changes by submitting the AE250-1 webform to DISP.info@defence.gov.au.

Annual Security Awareness Training

15. The University requires all staff to complete Cybersense security awareness training as part of their induction.

16. An additional security awareness and insider threat awareness training module is completed by DISP Personnel at the time of onboarding and once annually. A record of this training is maintained by the SO in the SGR.

17. In certain circumstances, Defence may require relevant university staff to complete the Defence annual Security Awareness course (available through Campus Anywhere) in addition to the training provided by the University.

Overseas Travel - Security Cleared Personnel

18. All DISP personnel contemplating business or private overseas travel, are to notify the SO. The SO briefs the employee prior to travel, debriefs the employee upon their return, completes contact or security concern reports and enters details in the SGR as per Chapter 1 clause 4 of the DISP Handbook. All DISP Personnel travelling on official ANU business must also adhere to the University's Travel policy and procedure.

Contact Reporting

19. DISP personnel are responsible for contact reporting. A contact is any suspicious or nefarious activity where an employee communicates with representatives of foreign countries; extremist or subversive groups; criminal groups; or political or issue motivated groups or individuals, including the media.

20. Espionage represents a threat to the security of Defence and Defence industry. Foreign Intelligence Services (FIS) personnel are skilled in the exploitation of relationships and aim to recruit people with legitimate access to their target area.

21. Private and official contacts, particularly social contacts, are used by foreign representatives to glean information of possible intelligence value or to make character studies of Australian official or businesspeople.

22. Security cleared staff or those engaged in a Defence project must be aware of the possibility of such contacts being made and report them to the SO.

23. Any contact, either in Australia or overseas, which is considered to have security significance, is reported immediately to the SO who completes and submits *Form XP188 - Security Incident Report* and sends to DS&VS Security Incident Centre – security.incidentcentre@defence.gov.au.

Security Incident Reporting

24. University Staff and students are responsible for reporting security incidents. The SO will take necessary action to immediately correct any security deficiencies or any matters which are likely to pose a direct security risk to university staff, students, or classified material, or which threaten to reduce the level of protection being afforded to classified material in the University's custody.

25. The SO reports all security incidents in accordance with the DSPF by submitting *XP188 - Security Incident Report* to security.incidentcentre@defence.gov.au and adds an entry within the SGR.

Security Clearances

26. Security cleared personnel must meet their ongoing responsibilities as clearance holders. See the Australian Government Security Vetting Agency (AGSVA) website at http://www.defence.gov.au/agsva for responsibilities, including reporting of any change of circumstances.

Defence Official Information

27. Defence official information is classified in accordance with the Australian Government Security Classification System (AGSCS) and protected in a manner that prevents unauthorised access by or disclosure to, those who do not have a need-to-know and the appropriate security clearance. Classified information must be released in accordance with DSPF Principle 10 Classification and Protection of Classified Information.

28. The University holds AGSCS information up to OFFICIAL: Sensitive at the ANU DISP location. Personnel use security classifications for the purpose of protectively marking official information.

29. DISP personnel using classified material ensure that there is no deliberate or casual inspection, or oversight by unauthorised persons. All classified material is to be secured in an approved security container when not in actual use or under direct supervision of an appropriately cleared person with a need-to-know.

Security Officer Training

30. CSO and SO are required to undertake the Security Officer Training course provided by DS&VS. The course provides a general understanding of the security environment and responsibilities of CSO and SO.

Defence Online Security Dashboard

31. Security Officers for DISP members with Governance Security Level 1 to Level 3 membership may apply for access to the Defence Online Services Domain (DOSD). There are two useful tools supported on the DOSD: the DISP Security Portal, and the Security Officer Dashboard.

32. The Portal provides access to the DS&VS Toolkit, a declassified version of the DSPF, and other security tools and advice via the internet rather than via the Defence Protected Network.

33. DS&VS will facilitate **DISP Security Portal** access for the SO at the time DISP membership is granted.

34. Further access to the DISP Secure Portal is requested by submitting the SCS 001 DISP Portal Access Request form to dsvs.awareness@defence.gov.au. The SCS 001 is located on the DISP website or the DISP Portal.

35. Security Officers may apply for access to the **Security Officer Dashboard** (the Dashboard). The Dashboard is where the SO requests and manages security clearances for their personnel.

36. Access to the Dashboard is requested by submitting the *SVA 016* Security *Officer Dashboard Request* form to agsva.crm@defence.gov.au. The SVA016 is available at http://www.defence.gov.au/AGSVA/resources/sva016-request-security-officer-dashboard.pdf located on the DISP website or the DISP Portal.

Random Security Checks

37. To ensure compliance with the DISP minimum security requirements, Defence will conduct random and targeted security spot checks of the University. This may include but is not limited to, a review of the entity security policies and plans, personnel, information and physical security arrangements and security registers.

38. The SO is also responsible for undertaking random security checks to help ensure that:

    a. classified material is properly protected; and

    b. all personnel are adhering to all security requirements.

39. A record of random security checks is recorded within the SGR.

Annual Security Report (ASR)

40. The DISP ASR is completed by the CSO and submitted annually to DISP.info@defence.gov.au within ten business days of the original date membership was granted.

41. The DISP ASR is reviewed by the University's Audit, Risk and Management Committee (ARMC) and all recommendations are implemented within agreed timeframes.

Breaches and non-compliance

42. Failure by staff to abide by this Handbook and the regulations outlined in the DSPF may result in DISP membership being terminated and the cancellation of any contracts the University may have with Defence.

43. The University investigates unauthorised use of the University's IT and information infrastructure. Identified breaches of this Handbook and related documents are investigated under the following:

    a. *Information Infrastructure and Services Rule 2020*;

    b. ANU Code of Conduct;

    c. *Discipline Rule 2021*; and/or

    d. Security of Critical Infrastructure Act 2018.

Chapter 2: DISP Physical Security

Aims and Objectives

As a DISP member, the University must detail physical security measures in place at any facility listed within their membership. Physical security measures help deter, detect, and delay any potential security threats to university facilities. By providing a safe and secure environment it will prevent or mitigate threats against Defence data and information used and stored at our facilities.

The purpose of this chapter is to outline the framework for the management of physical security at the ANU DISP location – The Physics Building (Building #160, 60 Mills Road, Acton ACT 2601) as listed under the University's DISP membership.

Scope and Inclusion

This chapter applies to the ANU Physics Building (Building #160, 60 Mills Road, Acton ACT 2601) and all staff, students and third parties utilising the relevant sections of this building. The Security - buildings and site policy also applies to this building.

Roles and Responsibilities

The University has established security standards within its grounds and in buildings, that are appropriate to effectively manage personal, property and security risks. The following sections detail responsibilities for various aspects of security management.

ANU Security:

1. The University has established a central security unit (ANU Security) within the Facilities and Services Division. The role of this area is to oversee security on site, while also monitoring internal security within buildings by use of the electronic access system, fire system, closed circuit television and building management systems.
2. Other functions of ANU Security include:
    a. Managing initial response to site emergencies.
    b. Management of the after-hours call out list for areas.
    c. Site patrols, including locking up of designated areas.
    d. After-hours management of the University switchboard.
    e. Conduct of security risk audits in accordance with AS4360 and the Commonwealth Protective Security Manual 2005, where applicable.

Policy Statement

Inductions

3. Work Health and Safety (WHS) inductions, including asset management and hazardous area access, are performed for all staff with a requirement to work at the Physics building. There are primarily two safety/security zones managed through Tier 2 and Tier 3 inductions. Tier 3 zones

are nested within Tier 2 zones. Tier 2 zones have a single engineering control for safety systems. Tier 3 zones may have additional engineering controls specific to the type of hazard.

Visitors to DISP-identified areas in the ANU Physics Building #160

4. Any visitors to the ANU Physics building #160 are not permitted access to DISP material and zones until their identity and "Need to Know" has been established.
5. The University records all visitor access to DISP-identified areas. All visitor requests are vetted by the Director. All visits are for a timed period.
6. An authorised person escorts all visitors.
7. Visitors passes are to be:
   a. Worn at all times.
   b. Collected at the end of the visit.
   c. Disabled on return or when the period of visit has expired.

Access Control

8. Electronic access controls are fitted on designated entry and exit doors.
9. Areas that use the electronic access systems identified by the University the following applies:
   a. The Director, Facilities and Services, has established specifications for the electronic system in accordance with the system standards adopted by the University.
   b. The system is monitored by Facilities and Services (ANU Security) on a 24-hour/7-day basis.
   c. Individual access profiles are determined by the relevant area management, in accordance with the security standards established for that building. Physics management has authority to review individual access.
   d. Access to the University Physics building Tier 2 and Tier 3 zones is restricted to authorised personnel.
   e. Physics Management controls the authorisation of personnel through training and competency.
10. Access passes are used at the Physics building within the Tier 2 and Tier 3 zones. DISP personnel are responsible for:
    a. Ensuring the safekeeping of their access pass.
    b. Always wearing their pass visibly within the workplace, ensuring the photograph can be clearly seen.
    c. Reporting loss of their pass to the Security Officer (SO) and ANU Security.
    d. Ensuring that no other person has possession, use or access to their ID or access pass.
    e. Challenging anyone not known to them in the facility that is not wearing a pass.
    f. Returning the ID or access pass to the SO or ANU Security on expiration of the pass, cessation of the requirement to enter any premises requiring the pass, or termination of employment.

11. Electronic access cards are to be considered a "Security Key" and are recorded in the Security Governance Register (SGR) by the SO. The SO conducts an annual audit to account for all university access cards.

Keys

12. A key register in combination with key safe and auditing is maintained within the SGR by the SO containing details of all facility keys, security containers, and keys for the ANU DISP location.
13. An audit of the facilities keys is performed bi-annually (twice a year).
14. Issuing of master keys is limited to essential personnel (as a guide, no more than two master keys for an area should be issued). A master key for the area is supplied to and held by ANU Security for extraordinary use only.
15. Unauthorised duplicate keys are not to be made without prior authorisation from the SO and ANU Security.
16. Security keys to security containers are held only by authorised and appropriately security cleared Personnel. Keys to containers holding classified material are regarded as having the same classification as the material held in the containers and are protected accordingly.
17. The loss or compromise of a security key is reported to the SO and ANU Security and subsequently in accordance with DSPF Principle 77 Security Incidents and Investigations, form XP188 Security Incident Report is to be filled out.

Security Containers

18. While the University currently has no requirement to maintain security containers as part of the University’s DISP membership, should this requirement arise;
    a. All official and classified material must be stored in approved security containers.
    b. Access to the containers shall be limited to the approved custodian/s.
    c. The SO is to record details of the security containers, their locations, and their custodians in the SGR.

Alarms

19. All alarms are monitored and linked to a pre-determined response.
20. All alarm incidents and responses at the DISP location are reported to the SO and recorded in the SGR.
21. The University uses appropriately trained staff as privileged operators of the alarm system.
22. Any default user codes are to be removed from alarm systems.
23. Alarms are tested regularly and maintained to ensure their continual operation.
24. ANU Security has a 24x7x365 on-premises centre monitoring alarms and other security controls centrally.

Closed Circuit Television (CCTV)

25. The purpose of closed circuit television is to monitor activities within buildings and on site, and where appropriate record events for subsequent investigation or reference to police.

26. The Director, Facilities and Services, is responsible for defining the system specifications for closed circuit television and approving the installation of new systems within buildings and across campus.

27. The University complies with all relevant jurisdictional legislation as well as Commonwealth legislation, including Australian Standard AS4806 Set:2008, governing CCTV usage.

28. The University must advise staff and visitors that CCTV is in use on the premises.

29. Any person requesting CCTV footage will be required to send a written request to the SO or ANU Security.

30. Destruction of CCTV footage is done in accordance with relevant laws and regulations.

Guards

31. Contracted guards are licensed in the Australian Capital Territory as per the *Security Industry Regulation 2003*.

32. When members of the public are disgruntled, immediate assistance is sought via ANU Security.

After Hours Contacts

33. All areas nominate officers as after-hours contacts in the event of emergency. Areas are responsible for ensuring an up-to-date contact list is provided electronically to Facilities and Services (ANU Security) each time staff or delegation arrangements change.

Close of Business Security Check

34. Where classified information is contained, a security check is conducted at close of business daily, to ensure that all classified material is secured in approved security containers and the Physical Security Zones perimeter is secure. The close of business check procedure performed at the ANU DISP location is below:

35. Personnel must ensure the following at the Close of Business:

    a. Sensitive or security classified information is stored appropriately and is not left unattended on a desk or printer.

    b. Desk is clear of documents to avoid sensitive or classified information being left out in the workplace.

    c. Laptops and other electronic media storing security classified information are secured.

    d. Official information has been disposed of appropriately, including checking waste-paper bins.

    e. Whiteboards and other displays do not show any security classified information.

    f. Vaults and containers are locked.

g. Windows and doors are locked.

h. Container keys are secured.

i. Keys are not left in doors and drawers at the end of the day or for any extended periods of time.

j. All systems are logged off and, if required, machines are switched off.

Emergency Procedures

36. In the event of a fire, civil disturbance or other occurrence which requires evacuation from the facility, where practicable, security cleared staff prior to leaving:

    a. Take action to secure all classified material in security containers.

    b. Assume personal charge of the classified material and retain it until relieved of the responsibility by the custodian or SO.

    c. It may be necessary that access by emergency personnel is granted under escort by appropriately security cleared staff.

Security Risk Assessments

37. The University conducts risk assessments as required, including lighting audits and internal security reviews. The responsibility for managing site assessments resides with the Director, Facilities and Services. From time to time, the University may also elect to commission external audits of campus security arrangements, including arrangements established in specific areas.

38. The University complies with all requests from The Defence Security and Vetting Service to audit physical control measures in place at the location/s listed on the University's DISP membership.

39. Where appropriate, the University area can seek the assistance of the Director, Facilities and Services, in completing a risk assessment for their area.

40. Any additional physical security measures introduced must be consistent with University policies, the Protective Security Policy Framework (PSPF) and relevant ACT and Commonwealth legislation.

Chapter 3: DISP Personnel Security

3.1 DISP Employee Screening

Aims and Objectives

The objective of this chapter is to inform DISP personnel of additional employee screening requirements to work on Department of Defence projects and/or research.

Scope and Inclusion

This chapter applies to all prospective and current staff working on or being engaged to work on DISP Projects.

Roles and Responsibilities

Background checks are managed by the Human Resources Division contacted at backgroundchecking@anu.edu.au

Process

1. Current and prospective DISP Personnel are required to undergo employee screening to be eligible to work on any Department of Defence projects as per the DISP requirements.
2. All employee agreements and job advertisements contain necessary terms and conditions reflecting security obligations and employee screening checks required for employment.
3. All screenings are confidential and are not disclosed to any individual, except to the extent necessary on a need-to-know basis.
4. Employment with the University for the purpose of Defence projects or research is not confirmed without confirmation of successful background checking and, as such, all offers of employment are contingent on the successful completion of background checking.
5. Where an employee screening check revels a disclosable outcome or raises concerns about an applicant's suitability for the position offered, the Background Checking Committee review the outcome, and makes recommendations to the action required.
6. The Background Checking Committee is comprised of the Director, Human Resources (Chair), Chief Operating Officer, Deputy Vice-Chancellor (Student and University Experience), the Registrar (Division of Student Administration and Academic Services) and University General Counsel (or Nominee).

Implementation

7. As outlined in the Appointments policy and Background checking procedure, all prospective University staff undergo both a Reference Check and a Working With Vulnerable People Check (WWVP) Check. The WWVP check includes the following:
    a. An identity check requiring 100 points of ID.
    b. Address history checks for a minimum of five years.

c. National police check.

8. In addition to this, in order to meet DISP requirements in accordance with the AS 4811:2022 workforce screening principles, all prospective or current DISP Personnel are required to undergo the following additional checks:

   a. Retrospective media check.

   b. Police History check.

   c. Employment History Confirmation.

   d. Education Based Qualification check.

9. Prospective or current staff who are made an offer for a new or existing position on a Department of Defence project may also be required to hold an Australian Security Clearance. If so, this should be outlined in the terms of the contract with the Department.

10. The cost for all screening checks is borne by the University.

11. The cost for Security Clearances is covered but the local area or partnering agency.

3.2 DISP Personnel Travel

Aims and Objectives

The objective of this chapter is to outline the University procedures surrounding travel for DISP personnel.

Scope and Inclusion

As a DISP member, the University is required to;

a. Brief and debrief DISP personnel prior to and on return from overseas travel.

b. Provide advice on device responsibilities, privacy, and security risks to travelling DISP personnel.

c. Report any security concerns/incidents to relevant parties.

d. Ensure records of travel briefing, debriefing and contact reports are maintained.

Roles and Responsibilities

The roles and responsibilities of the person travelling, and the SO are outlined in the process below. Specific details for private travel are at Attachment B and specific details for official travel are at Attachment C.

Process

12. All DISP personnel contemplating business or private overseas travel are to notify the Security Officer.

13. All DISP personnel are to be aware of security risks relevant to their travel destination and remain aware of their security responsibilities.

Pre-Travel Briefing

14. All DISP personnel are to complete a Change of Circumstances Notification form (SVA003) as travelling overseas is considered a change in personal circumstances.

15. The Security Officer must brief the DISP Personnel prior to travel. The briefing process is determined based on whether the travel is private or official as per the processes at Attachment B and Attachment C.

Post Travel Briefing

16. All DISP personnel returning from private or official overseas travel are to be debriefed upon return.

Contact Reporting

Any contact or security concern identified during the debriefing which is considered to have security significance, requires the Security Officer and traveller to complete and submit Form XP188 - Report of Security Contact Concern and send to DS&VS Security Incident Centre - security.incidentcentre@defence.gov.au.

Chapter 4: DISP Information and Cyber Security

The University maintains compliance with cyber security accreditation standard: Essential Eight (ASD Top 4) for ICT systems used for Defence research or projects. This includes the following top four strategies:

a. Patch Applications

b. Patch Operating Systems

c. Restrict Administrator Privileges

d. Application Control

4.1 Application Control

Aims and Objectives

The purpose of this Chapter is to define the University's governing framework for the implementation and maintenance of application control measures across the DISP workstations and servers. By identifying, testing, and approving applications prior to deployment within the University's IT environment, this ensures the confidentiality, integrity, and availability of DISP systems and data is upheld.

Scope and Inclusion

Unauthorised applications pose a significant security risk as malicious applications can severely damage the University's systems and data integrity, impacting research efforts and core university functions. Application control is used to mitigate or eliminate the risk associated to the use of unauthorised or malicious applications and protect against malicious code (also known as malware) executing on systems. Application control is one of the Australian Cyber Security Centre's (ACSC) Essential Eight controls for preventing cyber security incidents.

The University must maintain compliance with the Essential Eight requirements for application control to be compliant with obligations as a DISP member.

This Chapter applies to all DISP personnel, and servers and workstations relevant to DISP or Defence work or projects.

Exemptions

1. The only exemptions to this Chapter are those approved under the Procedure: Information technology local administrator privileges for local administrator privileges to their device. Users with local administrator privileges are advised of their responsibilities as part of this procedure including acceptable use of local administrator access and ensuring no security controls are removed.

Roles and Responsibilities

2. System and application owners are responsible for ensuring the maintenance and implementation of application control tools and rulesets on servers and workstations.

Principles

3. The University has developed and maintains a set of application control rules enforced using an automated tool, to ensure only approved applications are allowed to execute on workstations and internet-facing servers.
4. Application control rules are reviewed on a minimum annual basis.
5. The application control rules are implemented, maintained, or updated, when appropriate, through the Change Advisory Board (CAB).
6. The application control tool generates event logs detailing allowed and blocked executions to assist in the identification of malicious attempts to execute code.
7. Application control procedures are documented in line with this Chapter.

4.2 Privileged Access Management

Aims and Objectives

The purpose of this section is to outline the University's Privileged Access Management (PAM) governance framework for restricting and controlling the use of privileged administrator accounts for DISP Personnel.

Scope and Inclusion

Restricting administrative privileges is one of the most effective mitigation strategies for ensuring the security of systems. Without restrictions, users with administrative privileges for operating systems and applications can make significant changes to their configuration and operation, bypass critical security settings and access sensitive information.

Restricting the use of administrative privileges makes the University's online environment more stable, predictable, and easier to administer and support, as fewer users can make significant changes to the University's operating environment (whether intentional or not).

This Chapter applies to all DISP personnel that require privileged access to University systems and personnel in roles involved in the management and security of these accounts.

Exclusions

8. This Chapter excludes the use of local administrator accounts. The process and requirements for this account type are in the Information Technology local administrator privileges procedure.

Roles and Responsibilities

9. System owners:
   a. Maintain a list of privileged account users for their systems.
   b. Implement and maintain a system access approval process.
   c. Ensure that users with elevated or privileged access are provided with adequate training and support on the use of privileged accounts and the security of information assets.

d. Ensure that privileged accounts are kept to a minimum and only used for essential administrative tasks.
e. Ensure that privileged accounts are controlled and accountable.
f. Regularly review and remove or suspend privileged accounts in accordance with clause 25 and 26.

10. Users

a. Comply with security and password requirements, as set out in the Authentication for access to University resources procedure, and maintain confidentiality of account credentials.
b. Ensure the security of the account and access, and report any identified risks to the system owner.
c. Only use privileged accounts for administrative purposes, i.e., no web browsing or email access occurs while logged in with this access.
d. Privileged account holders must report any security concerns associated with their account or the systems they access by emailing it.security@anu.edu.au.

Principles

11. This document outlines security controls required for ensuring authorisation of access, and privileged users' responsibilities. It also defines the rules for handling exceptional situations through the use of special accounts.

12. Security controls for the management of access must be defined, implemented, maintained, and monitored to protect the information assets and the (ICT) systems supporting the University.

13. This Chapter will ensure:

a. Procedures supported by formal processes are implemented; ensuring access to ICT systems and information assets is authorised, provisioned, maintained, and reviewed appropriately.

b. Technical controls are implemented; ensuring access controls are streamlined across all systems and information repositories.

c. ICT system rules governing credential management, privileged accounts, and ongoing management meet minimum requirements of the ISM guidelines for system hardening.

d. Records relating to privileged accounts, changes and removal are documented and maintained for management review and audit purposes.

e. Privileged accounts are subjected to regular review and audit, with any non-conformances managed appropriately in a timely manner.

f. DISP Personnel and users with privileged access to DISP materials are provided with security briefings upon induction and on an annual basis, which outlines their individual responsibilities relating to the use of their account, access credentials and the protection of the information assets they have access to.

Privileged Access Management

14. Privileged administrator permissions are only granted to those with a valid business requirement, these may include the following;
    a. Change key system configuration settings.
    b. Change security controls.
    c. Access to audit and security monitoring information.
    d. Access to data, files and accounts used by other users, including backups and media.
    e. Access to troubleshoot a system.
15. Privileged account holders are assigned a dedicated privileged account that is only to be used for administrative tasks requiring privileged access.
16. A unique username is used to identify the privileged account holder and distinguish that account from non-privileged accounts issued to the user.
17. Privileged account users must protect their account credentials and not share them with other users.
18. Multi-Factor Authentication (MFA) must be used to authenticate a privileged account, where available.
19. Privileged accounts follow the least privilege security model and are restricted to only allow the specific functions required to be performed and cannot browse the web or access email.
20. The number of personnel with a privileged account is limited to the minimum required to administer the Universities network and system.
21. Privileged access must be reviewed and revalidated on an annual basis.
22. Formal procedures and processes must be documented and implemented for privileged administrator access.
23. To prevent unauthorised access and breaches of privileged access rights, the allocation and use of privileges must be controlled through the formal authorisation process.
24. Visiting and Honorary Appointments (VaHA's) required to have a privileged account must adhere to these requirements and conditions.

Removal or Suspension of privileged access

25. Privileged access is removed in any of the following circumstances;
    a. When there is no longer a legitimate business requirement (e.g. when personnel change duties).
    b. When the account holder ceases employment with the University.
    c. Malicious activity is detected on the account.
    d. Account closure is requested.

    e. The account reaches its expiry date.

    f. The account is inactive for 45 days.

26. Privileged accounts are amended in circumstances such as change of role.

Emergency access to systems

27. Emergencies would occur when access to the system cannot be gained via normal authentication processes, such as due to misconfigurations of authentication services, misconfigurations of security settings or due to a cyber security incident.

28. In an emergency, a Break Glass account can be used to gain access. As Break Glass accounts generally have the highest level of privileges available for systems, extreme care should be taken to both protect them and to monitor for any signs of compromise or abuse.

29. Break Glass accounts will not be directly attributable to an individual, and systems may not generate event logs. Additional controls should be implemented to maintain the system's integrity.

30. Administrative activities performed using a Break Glass account should be identified and documented in support of change management processes and procedures. This should include the individual using the break glass account, the reason for using the account and any administrative activities performed using the break glass account.

31. To assist with incident response activities, it is important that Break Glass event logs are centrally stored and protected from unauthorised modification and deletion, monitored for signs of compromise and actioned when cyber security events are detected.

4.3 Vulnerability and Patch Management

Aims and Objectives

The purpose of this section is to outline the University's Patch Management governance framework to ensure patches are applied in a timely manner to remain compliant with the relevant frameworks whilst minimising risk of unexpected outages and impacts on ICT systems.

Scope and Inclusion

Applying patches or updates is critical to ensuring the ongoing security and availability of applications, drivers, operating systems, and firmware that support the core functions of the University. Patching operating systems and patching applications form two of the Australian Cyber Security Centre's (ACSC) Essential Eight security controls for mitigating cyber security threats.

The University must maintain compliance with the Essential Eight requirements for patching operating systems and applications to be compliant with obligations as a DISP member.

This Chapter applies to all DISP personnel, and servers and workstations relevant to DISP or Defence work or projects.

Exemptions

32. In some instances, installing patches is neither appropriate nor necessary. Exceptions may include:

    a. Simple components that have no known vulnerabilities and have not had a release for a period of time.

    b. Components that release multi versions within a short period of time and have no known vulnerabilities.

    c. The risks of not patching are sufficiently low, including instances where compensating controls exist.

33. Should the system owner choose not to patch, then this decision is made immediately visible to the Director, ITS and the Chief Information Security Officer.

34. Exemptions must be reviewed regularly to ensure there are no changes to the threat level represented by the decision to not patch.

Roles and Responsibilities

35. System Owners and Application Owners:

    a. Comply with the requirements outlined in this Chapter.

    b. Establish and operate a patch management plan for each system.

    c. Remain accountable for patching their services.

    d. Report exemptions to the Director, Information Technology Services, and the Chief Information Security Officer.

    e. Ensure the removal/ replacement of products that are no longer in support.

36. Director, Information Technology Services (ITS)

    a. Ensure patch management plans are reviewed, approved, and integrated into the enterprise's ICT function. In the case of externally hosted services, incorporate patch management into contracts with the relevant external party.

    b. Where appropriate, reprioritise the deployment schedules in response to imminent threats and notify system owners.

37. Information Security Office:

    a. Ensure patch compliance amongst system owners.

    b. Maintain a register of critical and internet-facing systems and assets.

    c. Maintain a record of exemptions to this Chapter and ensure remediation.

    d. Provide monthly patching reports to the ITS Executive.

System Inventory

38. ICT systems, components, applications, operating systems, hardware, equipment etc. are inventoried and categorised according to their criticality.

Vulnerability/Patch Identification

39. A vulnerability scanner is used as per the below table frequencies to identify missing patches or updates for security vulnerabilities in applications and operating systems.

Service	Frequency
All Internet facing	Daily
Office Suite, Web browsers, email clients, PDF software, security products, operating systems, drivers, firmware, and other ICT systems.	Weekly
All other applications	Fortnightly

40. Where vulnerability scanners cannot be used, system owners should refer to vendor documentation on how to identify patching levels and conduct manual audits instead. This should be reflected in the patch management plan.

41. System Owners are subscribed to vendor email alerts (where possible) and check vendor websites regularly.

Patch Prioritisation and Deployment

42. Patches for security vulnerabilities are prioritised based on the risk and operational requirements of the service. If the service is internet facing and/or an exploit exists, the risk will be higher, and timeliness of the patching reflects this. These patches are recognised at the University as critical.

43. The following tables identify critical patch timeframes;

    a. If an exploit exists;

Service	Patch Timeframe
All internet facing	48 Hours
Office Suite, Web browsers, email clients, PDF software, security products, operating systems, drivers, firmware, and other ICT equipment.	48 Hours
All other applications	4 weeks

    b. If an exploit does not exist;

Service	Patch Timeframe
All internet facing	2 weeks

Service	Patch Timeframe
Office Suite, Web browsers, email clients, PDF software, security products, operating systems, drivers, firmware, and other ICT equipment.	2 weeks
All other applications	4 weeks

44. The timing of all other patches takes into account:
    a. Operational impact of the service if unavailable.
    b. Threat risk rating of the service; and
    c. The sensitivity of the information stored in the service.

45. Non-critical patches are deployed on a schedule that minimises the impact on the function of the service.

46. For the deployment of non-critical patches across large groups of services, or for complex services with multiple environments (such as test, development, and production), the patch management plan spreads the patching across available maintenance windows to ensure all levels are updated monthly.

47. A centralised and managed approach is used to patch or update applications, drivers, operating systems, and firmware.

48. An approach for patching or updating applications and drivers that ensures the integrity and authenticity of patches or updates, as well as the processes used to apply them, is used.

49. The Chief Information Security Officer or Director, ITS may, at their discretion, require any or all system owners to patch the services under their control within a defined timeframe, in response to an imminent threat which indicates this response.

50. Patches are always added to a change and go through the Change Advisory Board (CAB). Security patches that do not fit into established release cycles are considered Emergency Changes by the Change Advisory Board (CAB) and require approval by the Director, ITS.

Mitigations

51. In some instances, a security patch may not be available; mitigations/ temporary work around advice from vendors or trusted authorities may provide protection until a patch is made available.

52. Patches should always be applied when available as a follow up activity.

Unsupported products

53. Applications, operating systems, network devices, security products and other ICT equipment that have reached end of life support from the vendor are removed or replaced.

Reporting

54. Patching is reported to CAB including progress, successes, and failures in accordance with each systems patch management plan. Automated tools are used where practical, to assist with this reporting. Monthly patching reports are provided to the ITS Executive.

Appendix A: Resources

Definitions

Please refer to the University Information Security Glossary for general definitions.

ANU DISP location: The Physics Building (Building #160, 60 Mills Road, Acton ACT 2601)

AS 4811-2022: A workforce screening standard published by Standards Australia. This document sets out requirements and guidance for the development of organization-specific workforce screening principles, policies and processes. Pre-employment screening, in line with AS 4811-2022 Employment Screening standard, is essential for DISP membership at Entry Level and above.

Defence Industry Security Program (DISP): The Defence Industry Security Program (DISP), managed by the Defence Industry Security Office (DISO), supports Australian businesses to understand and meet their security obligations when engaging in Defence projects, contracts and tenders. It is essentially security vetting for Australian businesses. Further information is available at https://www.defence.gov.au/security/industry.

DISP Personnel: Staff and students who are working on projects that require DISP membership.

Employee Screening: The process of verifying certain information provided by a candidate.

Least Privilege Security Model: Only give a user or group the minimum level of permissions needed to perform a given task.

Qualification Checking: Confirmation from a relevant institution that a prospective or current staff member has completed the qualifications required for the position or the qualifications they have declared to be in receipt of.

Reference Check: A confirmation of employment, performance and conduct check from a current or former employer.

Retrospective Media Checking: An investigation into an applicant's public claims of achievement, social media, awards and other publicly available information.

Tier 2: Tier 2 induction focusses on Compliance Training, which entails general building safety, electrical, fire and security alerts/actions. This is applicable to all staff, students and visitors entering office spaces and space adjoining hazardous areas. As with all zoned areas only personnel with current training status are given security card access to zones requiring Tier 2 training.

Tier 3: Tier 3 induction focusses on Work Safety Proficiency Training specifically for areas zoned as hazardous environments, such as laboratories and workshops. Training at this level requires specialised and regular training courses including competency assessment. Hazards operated in zones requiring Tier 3 inductions often have several levels of engineering controls.

Working with Vulnerable People Check (WWVP): Established under the *Working with Vulnerable People (Background Checking) Act 2011*, and is aimed at reducing the risk of harm or neglect to vulnerable people. The Act requires anyone who works or volunteers with vulnerable people to have a background check and to be registered.

Vulnerable person: Is a child or an adult who is disadvantaged or accessing a regulated activity in relation to the disadvantage.

Legislation

a. Australian National University Act 1991

b. Information Security Manual

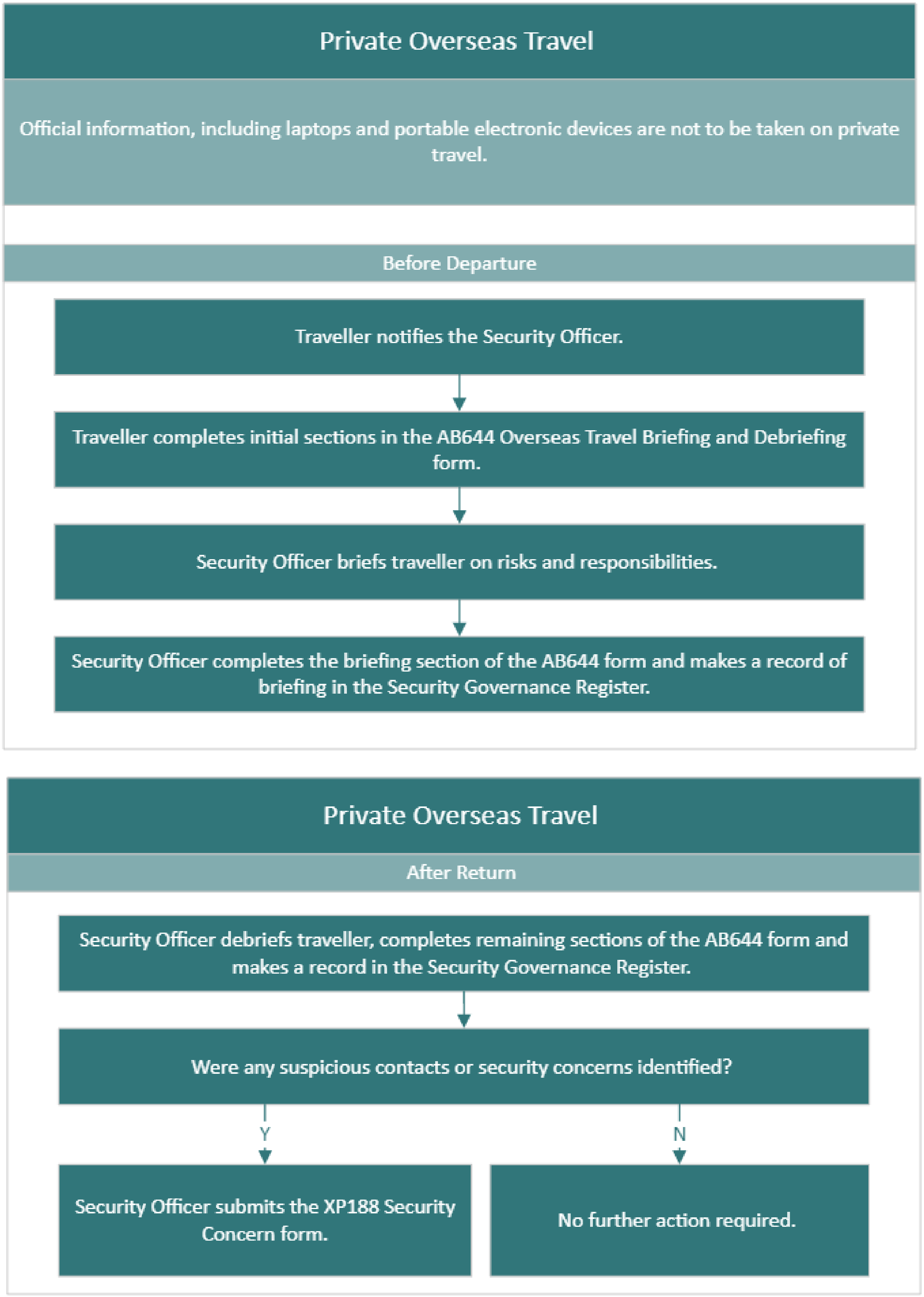
c. Australian Government Protective Security Policy Framework

d. Privacy Act 1988

e. Telecommunications Act 1997

f. Telecommunications Regulations 2021

Appendix B: DISP Personnel Private Travel



Private Overseas Travel

Official information, including laptops and portable electronic devices are not to be taken on private travel.

Before Departure

Traveller notifies the Security Officer.

Traveller completes initial sections in the AB644 Overseas Travel Briefing and Debriefing form.

Security Officer briefs traveller on risks and responsibilities.

Security Officer completes the briefing section of the AB644 form and makes a record of briefing in the Security Governance Register.

Private Overseas Travel

After Return

Security Officer debriefs traveller, completes remaining sections of the AB644 form and makes a record in the Security Governance Register.

Were any suspicious contacts or security concerns identified?

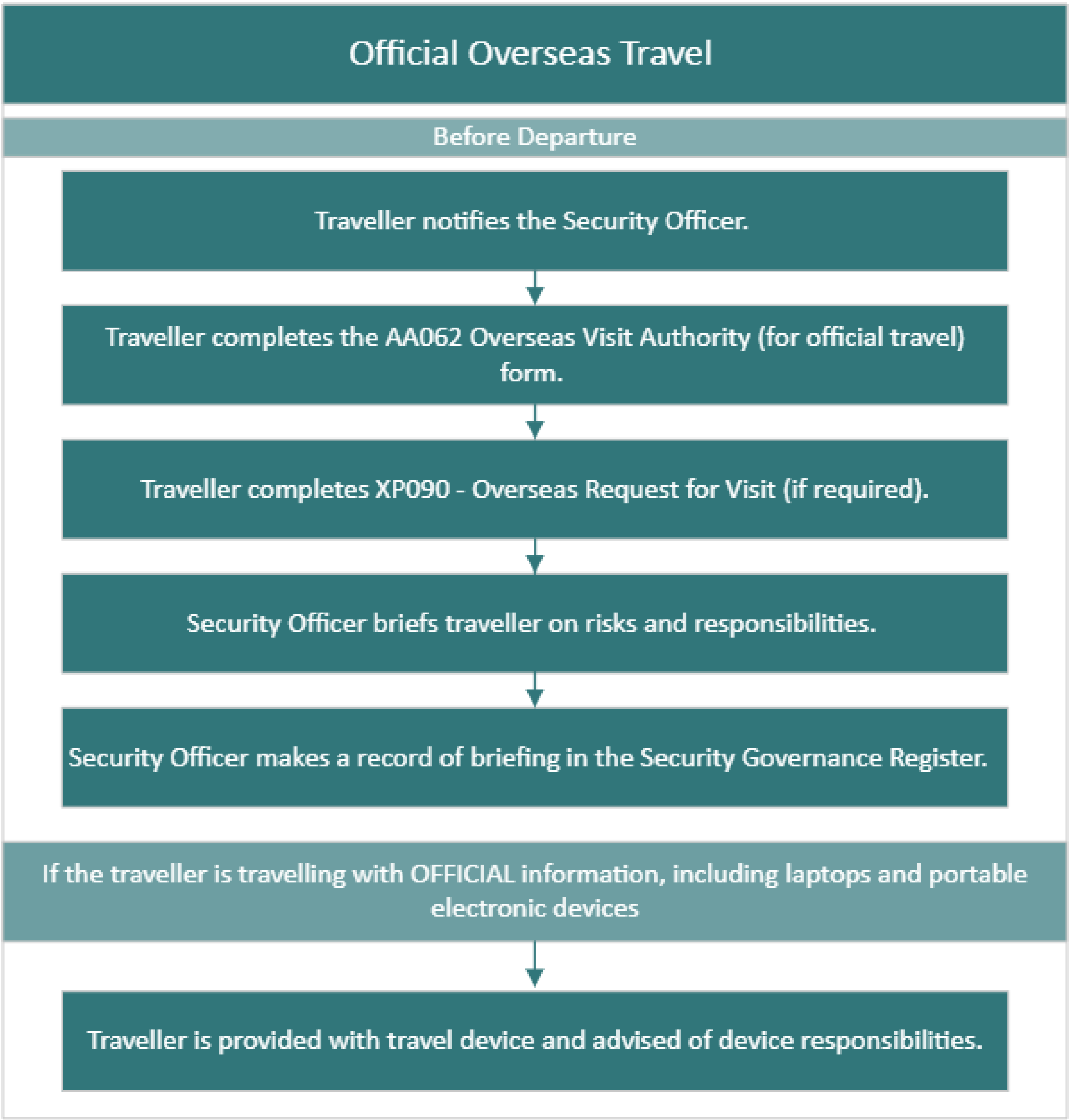
Security Officer submits the XP188 Security Concern form.

No further action required.

Figure 1: Private overseas travel briefing workflow

1. All DISP personnel that are planning private overseas travel are required to complete *an Overseas Travel Briefing and Debriefing form (AB644)*, available from the Security Officer before and on return from travel.
2. The Security Officer must brief the DISP Personnel prior to travel, including the following:
    a. Inform themselves about their destination via the Department of Foreign Affairs and Trade (DFAT) travel advisory (Smart Traveller) website.
    b. Suspicious contacts and security concerns:
        i. A suspicious contact is any suspicious or nefarious activity where the traveller communicates with representatives of foreign countries; extremist or subversive groups; criminal groups; or political or issue motivated groups or individuals, including the media.
        ii. Espionage represents a threat to the security of Defence and Defence industry. Foreign Intelligence Services (FIS) personnel are skilled in the exploitation of relationships and aim to recruit people with legitimate access to their target area.
        iii. Private and official contacts, particularly social contacts, are used by foreign representatives to glean information of possible intelligence value or to make character studies of Australian officials or business people.
    c. Personal device hardening recommendations.
3. After the briefing, the Security Officer is required to provide a certificate of Security Advice Given for Overseas Travel to the person travelling.
4. Personnel travelling are required to acknowledge, sign, and return the Certification of Security Advice Given for Overseas Travel to the Security Officer.
5. The Security Officer is to make a record of the briefing by adding an entry in the Security Governance Register (SGR).
6. Security Officer ensures debriefing section of the form Overseas Travel Briefing and Debriefing (AB644) Is completed for private travel.

Appendix C: DISP Personnel Official Travel



Official Overseas Travel

Before Departure

Traveller notifies the Security Officer.

Traveller completes the AA062 Overseas Visit Authority (for official travel) form.

Traveller completes XP090 - Overseas Request for Visit (if required).

Security Officer briefs traveller on risks and responsibilities.

Security Officer makes a record of briefing in the Security Governance Register.

If the traveller is travelling with OFFICIAL information, including laptops and portable electronic devices

Traveller is provided with travel device and advised of device responsibilities.

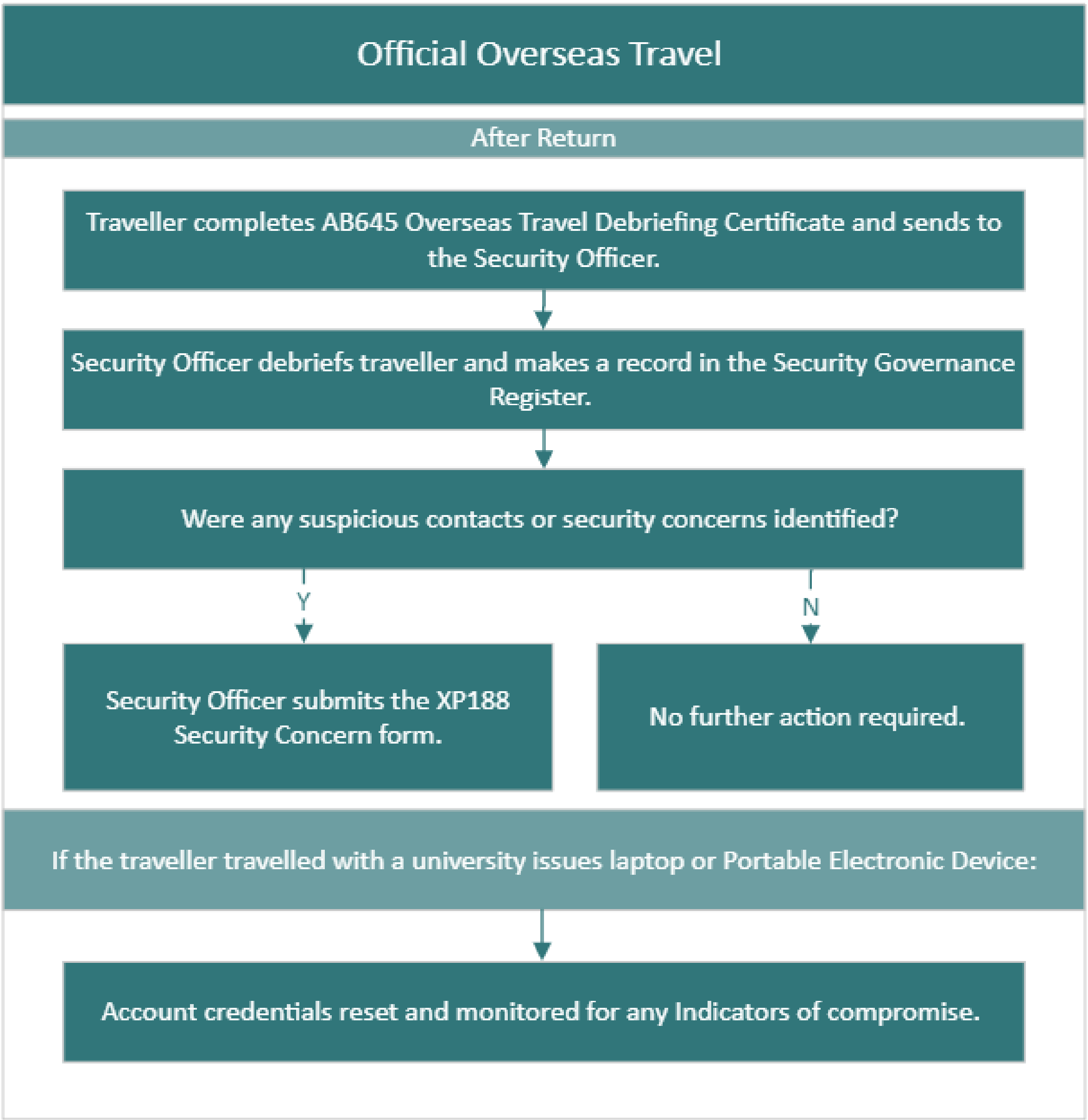

Official Overseas Travel
After Return
Traveller completes AB645 Overseas Travel Debriefing Certificate and sends to the Security Officer.
Security Officer debriefs traveller and makes a record in the Security Governance Register.
Were any suspicious contacts or security concerns identified?
Y
N
Security Officer submits the XP188 Security Concern form.
No further action required.
If the traveller travelled with a university issues laptop or Portable Electronic Device:
Account credentials reset and monitored for any Indicators of compromise.

Figure 2: Official overseas travel briefing workflow

1. All DISP personnel that are planning overseas official travel are required to notify the Security Officer and complete an Overseas Visit Authority for official travel form (AA062); and any other applicable forms required by the ANU for officers travelling on official University business.

2. If travelling to any country with which Australia has a Security of Information Agreement or Arrangement (SIA), or for overseas travel that may involve classified discussion, the employee completes and submits to the Security Officer, Form XP090 Overseas Visit/Posting – Security Clearance Advice.

3. The Security Officer briefs the employee, including the following:

    a. When travelling ensure that official visits to allied facilities are conducted in accordance with bilateral security responsibilities and hosting country business processes.

b. Suspicious contacts and security incidents:

   i. A suspicious contact is any suspicious or nefarious activity where an employee communicates with representatives of foreign countries; extremist or subversive groups; criminal groups; or political or issue motivated groups or individuals, including the media.

   ii. Espionage represents a threat to the security of Defence and Defence industry. Foreign Intelligence Services (FIS) personnel are skilled in the exploitation of relationships and aim to recruit people with legitimate access to their target area.

   iii. Private and official contacts, particularly social contacts, are used by foreign representatives to glean information of possible intelligence value or to make character studies of Australian official or business people.

c. Inform themselves about their destination via the Department of Foreign Affairs and Trade (DFAT) travel advisory (Smart Traveller) website.

d. Confirmation on whether the traveller is required to travel with OFFICIAL information, including University issued laptops and portable electronic devices. If so, the traveller is provided a device from the dedicated travel pool of hardened devices and briefed on their device responsibilities:

   i. Advised on how to apply and inspect tamper seals to key areas of mobile devices.

   ii. Ensure mobile devices are always kept within your possession and not left in checked-in luggage, hotel rooms or safes.

   iii. Ensure the credentials for the mobile devices are not stored with the device, e.g. laptop bags.

   iv. Disable any communications capabilities of mobile devices when not in use, such as cellular data, wireless and Bluetooth.

   v. Do not use public Wi-Fi networks.

   vi. Use encrypted messaging apps for communications instead of using foreign telecommunication networks; and

   vii. Report the potential compromise of mobile devices, removable media, or credentials as soon as possible.

   viii. Any additional device requirements as per the *Defence Security Principles Framework, Principle 44, Annex B to Overseas Travel – Travelling with Portable Electronic Devices and Media.*

4. If travel was Official, Overseas Travel Debriefing Certificate (AB645) is completed by the traveller and sent to the Security Officer.

5. If a university device was issued:

   a. Device is collected from the traveller.

   b. User credentials used with mobile devices, including those used for remote access to the University systems are reset.
   c. Accounts are monitored for any indicators of compromise, such as failed logon attempts.

6. The Security Officer debriefs personnel and covers the following:
   a. Travel Procedures:
      i. Visa - How and by whom the visa was obtained? Were any probing questions asked about employment?
      ii. Entry and exit procedures – What occurred? Did officers/officials conduct any searches? Were documents examined out of sight? Was there any suspicious or concerning interactions with officers/officials?
      iii. Travel arrangements – Was travel undertaken alone or with an organised party? Was there contact with officials or tour guides in the country and, if so, was there anything about their behaviour to indicate they may have had an intelligence function? Was any special attention directed to the traveller or to other members of the organised party?
   b. Accommodation:
      i. Where did the traveller stay?
      ii. How and by whom was the accommodation arranged?
      iii. Was there a choice in accommodation?
      iv. Did any hospitality staff appear to behave in an unusual manner?
         a. Were any occurrences of eavesdropping or searches of luggage or rooms observed? Was the traveller carrying official information?
         b. Was the official information appropriately stored and/or accompanied?
         c. Was the official information left unattended in the traveller's hotel room at any time during the stay?
         d. Was the traveller's room cleaned or serviced while the traveller was absent?
   c. Contact with other travellers or non-locals living in the country.
      i. Was there any contact with tourists who did not seem to be genuine (e.g.) people in their tour group. other hotel guests, other attraction visitors etc.)?
7. A record of debriefing is made by the Security Officer in the Security Governance Register.