

Defence Security

[This is a policy excerpt only. Contact the Security Officer at SO@griffith.edu.au to obtain a complete copy.]

- 1.0 Purpose
- 2.0 Scope
- 3.0 Policy Statement
- 4.0 Roles, responsibilities and delegations
- 5.0 Definitions
- 6.0 Information

1.0 Purpose

The Defence Industry Security Program (DISP) assists in securing Australian Department of Defence (hereafter referred to as “**Defence**”) capability through strengthened security practices in partnership with industry and enhances Defence’s ability to manage risk in the evolving security environment. The DISP also supports DISP members, such as universities and defence industries, in managing security risks.

Following Defence’s assessment of eligibility and suitability, Griffith University (hereafter referred to as “**the University**”) has been granted DISP membership at the following security levels, as defined under the Defence Security Principles Framework (DSPF):

Governance Security:	Level 1
Personnel Security:	Level 1
Physical Security:	Entry Level
Information and Cyber Security:	Entry Level

The University must continue to meet the ongoing eligibility and suitability requirements, as outlined in the DSPF to maintain its DISP membership.

The University has agreed to abide by the security provisions stated in the DSPF for designated facilities (hereafter referred to as “**Facility/Facilities**”), and which are reflected in this policy and its associated plans and procedures. Together these documents provide a working guide for University management and staff to implement security measures required by the DSPF.

2.0 Scope

This policy applies to all University staff working on or associated with Defence projects and/or working in the Facilities (hereafter referred to as “**Identified Personnel**”) and staff who are sponsored by the University to hold any level of Defence security clearance (hereafter referred to as “**Security Cleared Personnel**”).

The list of Facilities is maintained by the Security Officer.

For each Facility there are Facility-Specific Security Plan & Procedures which are to be read in conjunction with this policy.

3.0 Policy statement

This policy and its associated plans and procedures are developed and maintained by the SO to provide Identified Personnel with a guide to their individual security responsibilities.

Identified Personnel are required to read this policy annually as a reminder of their individual responsibilities. All Security Cleared Personnel must read this policy and the relevant Facility-Specific Security Plan & Procedures at the time of their introductory security briefing by the SO.

4.0 Roles, responsibilities and delegations

The University has staff performing the following Defence Security roles:

ROLE	CONTACT DETAILS
Security Officer (SO)	SO@griffith.edu.au
Chief Security Officer (CSO)	CSO@griffith.edu.au
Information Technology Security Officer (ITSO)	Contact the Security Officer for details

All communications and requests in relation to this policy are to be directed to the Security Officer.

5.0 Definitions

For the purposes of this policy and related policy document, the following definitions apply:

Contact	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.
Defence	Australian Department of Defence.
Facility/Facilities	Facilities which the University has designated as being governed by the Defence Security Policy and associated Procedures.
Facility-Specific Security Plan & Procedures	Operational guides that cover the Defence security plan and procedures specific to each Facility.
Identified Personnel	All University staff working on or associated with Defence projects and/or working in the Facilities.
Security Cleared Personnel	University staff who are sponsored by the University to hold any level of Defence security clearance.

Security Incident

Any unauthorised access to Facility/ies or information associated with Defence projects.

6.0 Information

Title	Defence Security Policy – Excerpt only
Document number	2023/0001236
Purpose	This policy and its associated plans and procedures are developed and maintained by the SO to provide Identified Personnel with a guide to their individual security responsibilities.
Audience	Staff
Category	Governance
Subcategory	Governance
UN Sustainable Development Goals (SDGs)	This document aligns with Sustainable Development Goal/s: 9: Industry, Innovation and Infrastructure
Approval date	26 February 2024
Effective date	1 March 2024
Review date	2025
Policy advisor	Export Control and Security Manager
Approving authority	University Council

13.0 Related Policy Documents and Supporting Documents

Legislation	<u>Defence Security Principles Framework</u>
Policy	N/A
Procedures	N/A
Local protocols	N/A
Forms	N/A