Defence Export Controls Procedure

Section 1 - Purpose

(1) This Procedure outlines the processes and requirements to ensure that export-controlled activities undertaken by the University of Newcastle (the University) are managed in a lawful, safe, and responsible manner, consistent with:

a. Defence Trade Controls Act 2012;
b. Customs Act 1901;
c. Weapons of Mass Destruction (Prevention of Proliferation) Act 1995;
d. Defence and Strategic Goods List 2024 (DSGL);
e. Defence Act 1903 Amendment – Safeguarding Australia's Military Secrets Act 2024; and
f. Defence Export Controls Policy.

(2) This procedure supports the implementation of the Defence Export Controls Policy and should be read in conjunction with this document. The procedure details operational instruction for identifying, assessing, and managing export controlled activities.

Section 2 - Scope

(3) This procedure applies to all University staff, Researchers, affiliates, contractors, visitors, honorary appointees, and controlled entities who undertake activities that may involve export-controlled goods, software, or technology.

(4) In the context of this document, activities include, but are not limited to:

a. research and research training, consultancy and testing;
b. teaching and supervision;
c. collaboration with domestic and international partners;
d. procurement and contracting activities;
e. travel and fieldwork;
f. publication and dissemination of research; and
g. intangible supply including use of digital systems, including email, cloud-based platforms and screen share.

Section 3 - Document Specific Definitions

(5) In the context of this document, the following definitions apply:

a. "controlled technology" means technical data, designs, software, or know-how that is subject to export control under Federal legislation;
b. "Defence and Strategic Goods List (DSGL)" is the Australian Federal legislative instrument that identifies goods, software, and technology that are subject export controls;
c. "dual-use goods" are items, software or technology that have both the potential for civilian and military

applications.

d. “Export” includes any physical or intangible transfer of controlled goods, software, or technology to a person, organisation, or location outside Australia;
e. “export controls” means laws and regulations governing the transfer, supply, publication, or brokering of controlled goods, software and technology;
f. “intangible supply” means the non-physical transfer, disclosure, publication, access or brokering of controlled technology to another person outside Australia, or foreign nationals in Australia;
g. “Technology Control Plan” or “TCP” details the documented measures that will be used by the University to manage access to and handling of controlled technology;
h. “Researcher” is as defined by the Responsible Conduct of Research Policy.
i. “Responsible Export Controls Officer (RECO)” means the institution’s nominee who is responsible for export control oversight. At the University of Newcastle this is the Director, Research Ethics & Integrity.

Section 4 - Identifying Export Controlled Activities

(6) Individuals must undertake an initial self-assessment to determine whether their activity(s) may be subject to defence export controls (“export control/s”).

(7) This must occur prior to commencement of the activity (for example, but not limited to prior to grant award, procurement, collaboration, travel or dissemination). The Australian Department of Defence tool “Made AI” can be used to assist.

(8) Indicators within an activity that may suggest export controls apply include, but are not limited to:

a. working with or procuring goods, software, or technology that are listed on the DSGL;
b. sharing or granting access to controlled technology with international collaborators or foreign nationals;
c. providing training, supervision, instruction or technical assistance relating to controlled or DSGL-listed technology;
d. transferring controlled or DSGL listed technology including email, cloud storage, system access, or screen-sharing electronically (intangible supply);
e. travelling with controlled equipment, materials, software or technical data;
f. research or other activities involving dual-use goods with potential military applications.

(9) Where uncertainty exists, individuals must seek advice from exportcontrols@newcastle.edu.au prior to proceeding with the activity(s).

Section 5 - Referral and Assessment

(10) Activities identified as potentially export-controlled must be referred to the Responsible Export Controls Officer (RECO).

(11) The RECO must:

a. assess whether the activity involves DSGL-listed items;
b. determine whether a permit, exemption, or further review is required;
c. identify if AUKUS licence free conditions apply;
d. assess risk level and advise on required controls; and
e. maintain appropriate records of assessments.

(12) Activities must not proceed until authorised by the RECO.

Section 6 - Due Diligence

(13) Where export control risk is identified, a due diligence assessment must be undertaken. This will be conducted by the individual, in consultation with the RECO and National Security Compliance Manager.

(14) This assessment may include:

a. classification of goods or technology against the DSGL;
b. assessment of end-use and end-user;
c. sanctions and restricted party screening;
d. consideration of foreign interference and national security risks; and
e. identification of applicable international regulatory requirements.

Section 7 - Permits and Approvals

(15) Where required, permits must be obtained from the relevant regulatory authority prior to any export, supply, publication, or brokering activity.

(16) The RECO will submit permit applications and act as the University's liaison with regulators.

(17) No export-controlled activity may proceed without appropriate authorisation from the relevant regulatory authority.

(18) Individuals must comply with all permit conditions.

Section 8 - Technology Control Plans

(19) Where a permit is required, a Tehnology Control Plan (TCP) must be developed.

(20) TCPs must:

a. define access controls (physical, digital and personnel);
b. outline data storage and transmission requirements;
c. specify training and awareness requirements;
d. including monitoring and recordkeeping arrangements.

(21) TCPs must be developed using the University template by the project lead prior to commencement of the activity, and updated to reflect changes in the activity once implemented.

(22) The TCP must be endorsed by the RECO prior to the commencement of the activity.

Section 9 - Implementation and Compliance

(23) Individuals and project teams must:

a. ensure only authorised personnel access controlled technology;
b. comply with all permit and TCP conditions;

c. implement appropriate safeguards; and
d. complete required training.

Section 10 - Recordkeeping

(24) Records must be maintained for all export-controlled activities.

(25) Records must include:

a. the initial export controls self-assessment and any supporting information;
b. classification and due diligence outcomes;
c. permit applications, variations and approvals;
d. TCPs and associated documentation;
e. details of supply or transfer, including recipients and dates; and
f. training registers.

(26) TCP's must be provided to the RECO for central record keeping and oversight.

(27) Records must be retained for a minimum of five years after the activity in accordance with the Records Governance Policy.

Section 11 - Monitoring and Review

(28) The University will monitor compliance with this procedure through a combination of activity-level and institutional monitoring, including:

a. audits and periodic reviews, including targeted audits of higher-risk activities;
b. oversight of permits and Technology Control Plans (TCPs), including review of compliance with access controls, recordkeeping and monitoring arrangements specified in the TCP; and
c. reporting of suspected or actual non-compliance in accordance with the Compliance Management Framework.

(29) Monitoring activities will be proportionate to the level of export control risk and may include enhanced oversight of high-risk activities.

(30) Where monitoring identifies gaps, non-compliance or changes in risk, corrective actions may be required including updates to TCPs, additional controls, training, or escalation to be reviewed under the Research Breach Investigation Procedure.

Section 12 - Import of Controlled Items

(31) Procurement of items that may be subject to export or import controls must be referred by the project lead to the RECO for assessment prior to execution of contracts, importation, or signing of documentation including:

a. end-user certificates;
b. end-use statements or undertakings;
c. import or export licence documentation;
d. supplier export control declarations; or
e. contractual export control certifications.

(32) Following assessment, any approvals required for the import of controlled items and associated documentation must occur in accordance with the University's Procurement Policy, Delegation of Authority Framework, and associated procurement procedures, with advice from the RECO where export control obligations are identified.

Section 13 - Publication and Dissemination

(33) Prior to publication, presentation or other dissemination, individuals must consider whether the content includes controlled technology, including technical data, software, designs or know-how subject to export control legislation.

(34) Publication of DSGL Part 1 (military) technology requires a permit.

(35) Pre-publication of sharing of controlled technology, including sharing with collaborators, peer reviewers, publishers, or conference organisers, may constitute a regulated supply and must be referred to the RECO for assessment prior to sharing.

Section 14 - Training and Awareness

(36) The University will provide training and guidance to support compliance. This includes:

a. an export controls module available through Discover;
b. training resources provided by the Australian Department of Defence.

(37) Individuals are required to complete export control training when their activities involve handling any DSGL listed technology.

Section 15 - Breaches and Non-Compliance

(38) Suspected or actual breaches must be reported immediately to the Research Ethics and Integrity Unit and managed in accordance with the Compliance Management Framework, including recording in the University's Breach Register where required.

(39) Breaches will be managed in accordance with the:

a. Research Breach Investigation Procedure; and/or
b. Staff Code of Conduct and Compliance Management Framework.

(40) Activities must cease where a potential breach is identified, until assessed.

(41) Matters involving the safeguarding of Australia’s military secrets (SAMS) and any actual or suspected foreign interference must be escalated without delay to the National Security Compliance Manager.

Section 16 - Roles and Responsibilities

(42) Roles and responsibilities are defined in the Defence Export Controls Policy.

(43) Individuals are responsible for ensuring compliance with this Procedure.

Section 17 - Integration with other obligations

(44) Export control compliance must be implemented in coordination with other University regulatory and governance obligations. Activities captured under this Procedure may also trigger requirements under related frameworks and University policy, including:

a. sanctions and restricted party screening, including obligations administered by the Australian Sanctions Office (see International Sanctions Compliance Policy);
b. digital security requirements, such as data classification, secure storage, cloud residency controls, and encryption (see Digital Security Policy);
c. foreign engagement and foreign interference obligations including mandatory disclosures and approval process (see Foreign Interference Policy);
d. research integrity and human/animal ethics requirements relevant to the conduct, approval and oversight of research activities (see Responsible Conduct of Research Policy);
e. contracts and intellectual property requirements including publication rights, background intellectual property, confidentiality and contractual restrictions on dissemination or use (see Intellectual Property Policy);
f. procurement and contracting obligations including compliance with the Procurement Policy, tendering requirements, and approval and delegation frameworks (see Delegation of Authority Framework);
g. privacy and data protection obligations, where activities involve the collection, use or disclosure of personal information, including cross-border data transfers (see Privacy Management Plan and Data Governance Policy).

(45) Individuals must ensure that export-controlled activities are compliant with all relevant obligations and seek advice where intersections occur.

(46) This Procedure should be read in conjunction with:

a. Defence Export Controls Policy;
b. Responsibile Conduct of Research Policy;
c. Research Breach Investigation Procedure;
d. Digital Security Policy;
e. Procurement Policy;
f. Records Governance Policy; and
g. applicable Commonwealth legislation and regulatory guidance.

Status and Details

Status	Current
Effective Date	30th June 2026
Review Date	30th June 2029
Approval Authority	Academic Senate
Approval Date	3rd June 2026
Expiry Date	Not Applicable
Responsible Executive	Juanita Todd Deputy Vice-Chancellor (Research and Innovation)
Enquiries Contact	Jodie Marquez Director, Research Ethics & Integrity

Glossary Terms and Definitions

"University" - The University of Newcastle, a body corporate established under sections 4 and 5 of the University of Newcastle Act 1989.

"Risk" - Effect of uncertainty on objectives. Note: An effect is a deviation from the expected, whether it is positive and/or negative.

"Controlled entity" - Has the same meaning as in section 16A of the University of Newcastle Act 1989.

"Personal information" - Has the same meaning as in the Privacy and Personal Information Protection Act 1998 (NSW).

"Intellectual property" - Intellectual property (IP), as defined by the World Intellectual Property Organisation, refers to creations of the mind: inventions; literary and artistic works; and symbols, names and images used in commerce. Intellectual property is divided into two categories: Industrial property includes patents for inventions, trademarks, industrial designs and geographical indications; and Copyright covers literary works (such as novels, poems and plays), films, music, artistic works (e.g. drawings, paintings, photographs and sculptures) and architectural design. Rights related to copyright include those of performing artists in their performances, producers of phonograms in their recordings, and broadcasters in their radio and television programs.

"Research" - As defined in the Australian Code for the Responsible Conduct of Research, or any replacing Code or document.

"Staff" - Means a person who was at the relevant time employed by the University and includes professional and academic staff of the University, by contract or ongoing, as well as conjoint staff but does not include visitors to the University.

"Affiliate" - A person or organisation legally obligated to, or informally associated with the University. Categories of affiliates are outlined on the University website.

"Foreign interference" - Foreign interference occurs when activities are carried out by, or on behalf of, a foreign actor that are coercive, clandestine, deceptive or corrupting and are contrary to Australia's sovereignty, values and national interests.