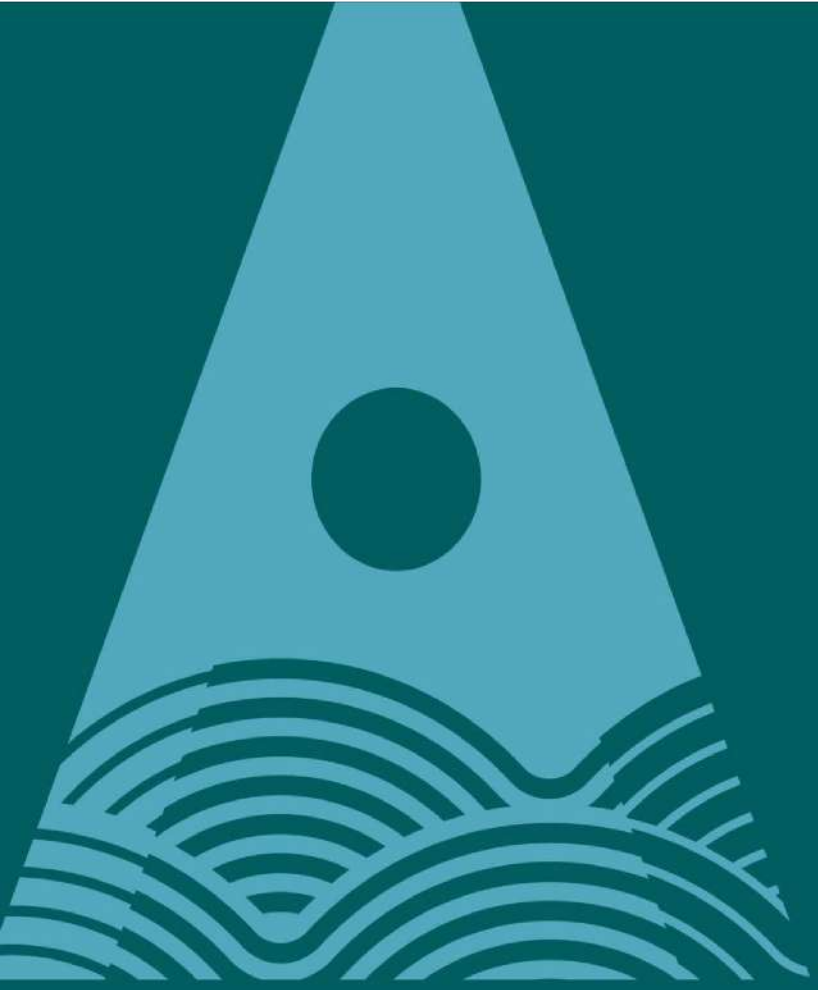


Ollscoil
Teicneolaíochta
an Atlantaigh

Atlantic
Technological
University

Policy for the Control of Exports
Version 1.0

Revision History:

Version Number/ Revision Number	1.0
Date of this revision:	03 November 2025
Date of next review:	03 November 2026
Revision Date	03 November 2025
Summary of Changes	New Policy
Changes Marked	N/a

Consultation History:

Number/ Revision Number	1.0
Consultation Date	May to July 2025
Names of Parties in Consultation	Acting Vice President of Research, Heads of Research and Legal, Corporate Governance Team, University Planning Team (UPT), Unions (FORSA, SIPTU, TUI, UNITE)
Summary of Changes	New Policy developed in collaboration

Approval:

This document requires the following approvals:

Version:	1.0
Approved By:	Governing Body
Date:	03 November 2025
Approved By:	Audit and Risk Committee (ARC)
Date:	21 October 2025
Approved By:	University Planning Team (UPT)
Date:	19 August 2025

Quality Assurance:

Date Approved	03 November 2025
Date Policy to take effect:	03 November 2025
Date Policy to be reviewed:	03 November 2026
Written by:	Research Compliance Coordinator & Integration Project Manager Research and Innovation (TU RISE)
Approved by:	Governing Body, ARC, UPT
Approving Authority	Governing Body
Head of Function responsible	Chief Officer, Research, Innovation and Engagement
Reference Documents:	Control of Exports Act, 2023 Regulation (EU) 2021/821 of the European Parliament of 20 May 2021 - EU Regulation - 2021/821 EU Commission Recommendation 2021/1700 of 15 September 2021

Document Location:

Website – Policies &Procedures	Yes
Website – Staff Hub	Yes
Website – Student Hub	No
Other: - Internal Use Only	No

This Policy was approved by the Approving Authority on **03 November 2025**. It shall be reviewed and, as necessary, amended by the University annually or at such a time as is deemed necessary or if there has been a material change to any legislation or national guidelines informing this policy area. All amendments shall be recorded on the revision history section above.

Note: Prior to publication and dissemination of policies and procedures, documents must be reviewed for accessibility as part the University's commitment to Equality, Diversity, and Inclusion (EDI). Further advice on accessibility can be obtained from the EDI Team.

Table of Contents

1. Introduction

1.1 The European Union (EU) has established export control legislation and export control lists (i.e. controlled items) that regulate and restrict the export and 'movement' of certain tangible and intangible goods and items, technology, software, or knowledge within EU Member States and/or to third countries, where necessary.

1.2 Controlled items refer to certain goods and items, technology, software, or knowledge that are subject to restrictions under EU and national export control legislation. These controlled items are classified and categorised into four key export control lists.

1.3 Export controls are part of a broader national and international framework designed to safeguard national, international and regional security; prevent terrorism; curb the proliferation of weapons of mass destruction and protect human rights (EU 2021/1700).

1.4 Export controls also promote the sharing of research, academic freedom, and free exchange of ideas in a legal, safe, and responsible manner.

1.5 In terms of the current export control legislative framework, there may be specific export licensing requirements for exporting certain sensitive goods and items, technology, software or knowledge (i.e. controlled items) to other destination countries or end-users. In addition to this, export controls may also trigger the application of export trade restrictions, sanctions, embargoes and other regulatory trade sanctions measures which may apply to specific destination countries affecting exports of controlled items.

1.6 The Department of Enterprise, Tourism and Employment (DETE) is the national competent authority in the Republic of Ireland. Its Trade Licensing & Control Unit is the authorising unit for the export authorisation applications system in terms of regulatory and legislative requirements.

1.7 Export controls can significantly impact the university's operations both directly and indirectly. This is especially true for research organisations and researchers who are more likely to work with and have access to controlled

items, particularly dual-use controlled items that are contained in the EU Dual-Use List.

1.8 In today's globally connected research landscape, it's increasingly common for academics and institutions to work on innovative technologies that may fall under export control regulations, especially those classified as dual-use controlled items and technologies that can serve both civilian and military purposes.

1.9 Dual-use export controls exist to govern activities involving items (materials, equipment, software and technologies) which can be used for both civil and military purposes and possibly associated with the creation of conventional military items or the proliferation of nuclear, radiological, chemical or biological weapons, also known as weapons of mass destruction, and their delivery systems such as missiles and drones (EU, 2021/1700).

1.10 Although dual-use controlled items are civilian and commercially available, they can also be adapted for military use or in the development of weapons. This makes them susceptible to potential misuse, and if acquired by the wrong hands, it could threaten international peace and security. For this reason, both EU and national legislation have been established to govern the export of these controlled items.

1.11 The range of dual-use controlled items in the Dual-Use List is extensive and covers 10 categories. Some examples include, but are not limited to, nuclear materials, facilities, and equipment; special materials and related equipment; electronics; computers; sensors and lasers; marine, and aerospace etc. However, all export control lists are reviewed and updated annually by the EU Commission to reflect emerging technologies and evolving geopolitical developments. Therefore, the most current versions of the lists should be consulted to ensure compliance.

1.12 Additionally, researchers are more likely to collaborate with, exchange and share export-controlled items, particularly dual-use controlled items that are contained in the Dual-Use List, with other researchers, research organisations or entities within EU Member States and/or to third countries.

Consequently, researchers may require an export authorisation (i.e. licence) from the Trade Licensing & Control Unit of the Department of Enterprise, Tourism and Employment (DETE) and should refer to the relevant EU and national export control legislation for further guidance.

1.13 As a research organisation, the university is committed to complying with all applicable EU, national, and international laws, and regulations for the control of exports.

1.14 This policy is designed to ensure that the university and its members (including but not limited to, staff, faculty, researchers, contractors, visiting scholars, and other third parties who access any ATU campuses and facilities) understand their responsibilities related to the control of exports and take appropriate measures to prevent unauthorised exports, transfer, disclosure or access of controlled goods and items, technology, and information that are listed in all the export control lists respectively.

1.15 For the policy, all references to researchers include principal investigators (PIs) and other individuals (e.g. research students and staff) engaged and involved in the research project.

2. Purpose of Policy

2.1 This policy is intended to allow the university to identify, manage and mitigate risks associated with the export of controlled items, including but not limited to, research activities, knowledge, and equipment, and to also facilitate compliance with EU, national and international export control regulations and legislation.

2.2 It outlines the standards, processes, procedures and university-wide roles and responsibilities that have been put in place for export control compliance focusing on those areas with exposure to controlled items. This policy should be read together with the university's Internal Compliance Programme (ICP) for export controls for reference.

2.3 Prior approval or an export authorisation (i.e. licence) may be required by the Department of Enterprise, Tourism and Employment (DETE) before

there is any ‘movement’ or export of any controlled items as reflected on any of the export control lists, within the Customs Territory of the Union (i.e. EU Member States) and/or to third countries as necessary.

2.4 Furthermore, it is also important that prior due diligence checks on the end-users and consignees are conducted before any export, as they may have trade restrictions or sanctions as noted in the EU sanctions map.

2.5 All exporters (researchers included) must screen and vet any research partners, end-users and consignees by conducting thorough due diligence checks to confirm their identity, and affiliations, and to further ensure that they are not subject to any trade sanctions or restrictions. This requirement safeguards against unlawful collaboration and breaches of export control or trade sanctions, mitigates reputational and legal risks, and helps ensure that no exports directly or indirectly support weapons development, military activities, other high risk activities, or any associations that could pose a risk to peace, security, or human rights. Refer to Appendix F which outlines guiding points to assist in understanding due diligence and partner vetting obligations.

2.6 This policy contains helpful resources and information for university members to understand and determine their export control obligations.

3. Definitions

“Authorisation”: Licence (EU, 2021/1700).

“Basic scientific research”: Experimental or theoretical work undertaken principally to acquire new knowledge of the fundamental principles of phenomena or observable facts, not primarily directed towards a specific practical aim or objective (EU 2021/1700).

“Consignee”: First recipient abroad of the item(s) to be exported. This may be where the item remains in which case the consignee will be the end-user (EU 2021/1700).

“Controlled items”: EU and any applicable national export control lists maintained by Member States (containing controlled goods and items, technologies, software, and knowledge). The EU export control lists are as follows: a) EU Common Military List (EU); b) EU Dual-Use List/Regulation (EU); c) EU Anti-Torture List/Regulation (EU); d) Non-Military Firearms (Civilian Firearms) List/Regulation (EU). National control lists can be accessed through the European Commission’s official compilation.

“Customs territory of the Union”: Customs territory of the Union within the meaning of Article 4 of the Regulation (EU) No 952/2013 of the European Parliament and of the Council of 9 October 2013 laying down the Union Customs Code (1): OJ L 269, 10.10. 2013, p.1 (‘the Union Customs Code’) (EU, 2021/1700).

“Diversion risks”: is the potential that controlled items may be transferred or shared intentionally or unintentionally to unauthorised end-users, for unauthorised purposes, or to unauthorised destinations.

“Dual-use items”: Items, including software and technology, which can be used for both civil and military purposes and includes items which can be used for the design, development, production or use of nuclear, chemical or biological weapons or their means of delivery, including all items which can be used for both non-explosive uses and assisting in any way in the manufacture of nuclear weapons or other nuclear explosive devices (EU, 2021/1700).

“Dual-Use List”: The Dual-Use List is a detailed inventory of items, software, and technologies that are subject to export controls due to their potential for both civilian and military applications. On 8 September 2025, the European Commission adopted a Delegated Regulation updating the EU dual-use export

control list in Annex I of Regulation (EU) 2021/8212. For the latest update see https://eur-lex.europa.eu/ (EU definition).

"End-user": The final recipient abroad of the item(s) to be exported (EU, 2021/1700).

"**EU Common Military List":** Common Military List of the European Union with equipment covered by Council Common Position 2008/944/CFSP defining common rules governing the control of exports of military technology and equipment. The list is updated annually. For the latest update, see https://eur-lex.europa.eu/ (EU, 2021/1700).

"Export controls regimes": Multilateral arrangements seeking to prevent the proliferation of nuclear, biological, and chemical weapons and their means of delivery as well as to prevent the destabilizing accumulation of conventional arms and dual-use items, e.g. by establishing lists of items which should be under control. The export control regimes refer to Nuclear Suppliers Group (NSG), Zangger Committee (ZC), Missile Technology Control Regime (MTCR), Australia Group (AG) and Wassenaar Arrangement (WA) (EU, 2021/1700).

"Exporter": Any natural or legal person or any partnership that:

- At the time when the export declaration or the re-export declaration or an exit summary declaration is accepted, holds the contract with the consignee in the third country and has the power to determine the sending of the items out of the customs territory of the Union; where no export contract has been concluded or if the holder of the contract does not act on its own behalf, exporter means the person who has the power to determine the sending of the items out of the customs territory of the Union.
- Decides to transmit software or technology by electronic media including by fax, telephone, electronic mail or by any other electronic means to a destination outside the customs territory of the Union or to make available in an electronic form such software and technology to natural or legal persons or to partnership outside the customs territory of the Union.

- Where the benefit of a right to dispose of the dual-use item belongs to a person resident or established outside the customs territory of the Union pursuant to the contract on which the export is based, the exporter shall be considered to be the contracting party resident or established in the customs territory of the Union.
- Any natural person carrying the dual-use items to be exported where these dual-use items are contained in the person's personal baggage within the meaning of point (a) of Article 1(19) of Commission Delegated Regulation (EU) 2015/2446 (2): OJ L 343, 29.12.2015, p.1. - (EU, 2021/1700).

"Export":

- An export procedure within the meaning of article 269 of the Union Customs Code;
- A re-export within the meaning of Article 270 of the Union Customs Code; a reexport also occurs if, during a transit through the customs territory of the Union according to point (11) of Article 2 of the EU dual-use Regulation, an exit summary declaration has to be lodged because the final desperate destination of the items has been changed;
- An outward processing procedure within the meaning of Article 259 of the Union Customs Code;
- Transmission of software or technology by electronic media, including by fax, telephone, electronic mail or any other electronic means to a destination outside the customs territory of the Union; It includes making available in an electronic form such software and technology to natural or legal persons or to partnerships outside the customs territory of the Union; it also includes the oral transmission of technology when the technology is described over a voice transmission medium (EU, 2021/1700).

"Intra-EU transfer or transfer": Movement or transmission of a dual-use items listed in Annex IV to the EU dual-use Regulation from a supplier in one EU Member State to a recipient in another EU Member State (EU, 2021/1700).

“Intangible goods”: Technology, knowledge, software, data, or ‘tech know-how’ related to the development, production or use to any of the controlled items and goods, equipment, components, samples, materials software, data, or technology that are export controlled (i.e. controlled items). This includes technology in the form of technical data (e.g. blueprints, drawings, software code, manuals, engineering designs, design concepts etc.) or technical assistance delivered through non-physical or electronic means (e.g. meetings, videos, television, email etc).

“In the public domain”: Technology or software which has been made available without restrictions upon its further dissemination (Copyright restrictions do not remove technology or software from being ‘in the public domain’)- (EU, 2021/1700).

“Listed dual-use items”: Dual-use items that are listed in Annex I to the EU dual-use Regulation (EU, 2021/1700).

“Non-Listed dual-use items”: Dual-use items that are not listed in Annex I to the EU dual-use Regulation and that can become subject to export controls (catch-all controls). It includes items that are (just) below the technical thresholds in Annex I to the EU dual-use Regulation (EU 2021/1700).

“Proliferation”: Flow of items (including software and technology) from countries that possess these items to countries that do not and that are seeking to gain access to these items for use in Weapons of Mass Destruction programmes (EU, 2021/1700).

“Research organisations”: Research-performing entities that are active in the academic or research sector, irrespective of their legal status (organised under public or private law) or way of financing, and whose primary goal is to independently conduct fundamental research, industrial research or experimental development or to widely disseminate the results of such activities by way of teaching, publication or knowledge transfer. It includes

universities, university colleges, academies of science applied research centres, and laboratories (EU, 2021/1700).

"Sanctions": Restrictive measures that target states, or entities and individuals. Some are mandated by the United Nations Security Council, whereas others are adopted autonomously by the European Union or nationally by an EU Member State - (EU, 2021/1700). [*The European union maintains restrictive trade measures on exports or imports of specific goods and technologies including arms embargoes, asset freezes, and travel bans against nearly 40 countries to protect international security and human rights. This can be accessed through the EU Sanctions map]*

"Tangible goods": Items, equipment, second-hand lab equipment, lab apparatus, goods, samples, prototypes, materials & components that are export controlled and shared through physical means such as by plane or ship or other transport method.

"Technology": specific information necessary for the development, production or use of goods. This information takes the form of technical data or technical assistance (EU, 2021/1700).

"Technical assistance or support": There are two types of controls of technical assistance, one which is regulated in the dual-use Regulation and one which is regulated according to national law in the EU Member States.

- Technology, according to the EU dual-use Regulation, may take the form of technical assistance such as verbal instruction, training, passing-on of technical knowledge and skills or advisory services, including, by telephone or electronic means. The technical assistance must be specific enough to meet the technology thresholds in Annex I to the dual-use Regulation.
- Other than dual-use listed technology in the form of technical assistance listed in Annex I of the EU dual-use Regulation, it covers all other technical support related to the repair, development, manufacture, assembly, testing, maintenance or any other technical service intended for use in connection with

the development, production, handling, operation, maintenance, storage, detection, identification or dissemination of chemical, biological or nuclear weapons or other nuclear explosive devices or the development, production, maintenance or storage of missiles capable of delivering such weapons or related to military end-uses in destinations subject to an arms embargo (EU Recommendation 2021/1700, pg. 23)

"Third country": A country that is not a member of the European Union as well as a country or territory whose citizens do not enjoy the European Union right to free movement, as defined in Art. 2(5) of the Regulation (EU) 2016/399 (Schengen Borders Code (EU definition).

A comprehensive list of more export control definitions can be found in the EU Commission Recommendation 2021/1700 and the university's Internal Compliance Programme (ICP) for export controls.

4. Scope

4.1 Universities (including scientists and research organisations) are subject to the same laws as consumers or manufacturers. While researchers enjoy the right to academic freedom in the Charter of Fundamental Rights of the European Union, they are still obligated to comply with export control regulations to protect the security interests of the EU and of its Member States (EU, 2021/1700).

4.2 Researchers must also ensure that all research activities are screened and assessed in accordance with the relevant export control provisions, trade sanctions and the respective export control lists before exporting any controlled items within EU Member States and/or to third countries, where necessary.

4.3 The responsibility falls primarily on researchers to determine and make the final decision if their research activity or project is export-controlled (e.g. subject to export control legislation) or would require an export authorisation

as they have more expertise, knowledge and engagement with the research activity or project, its technological details, specifications, or application. It is also their responsibility to keep track of and monitor the validity of their export authorisations and request renewals accordingly.

4.4 This policy applies to:

- All members of the university community, including but not limited to, staff, faculty, researchers, contractors, visiting scholars, and other third parties who access any ATU campuses and facilities.
- All research activities involving and relating to controlled items.
- Researchers, research staff, and management who are regularly involved with and engaged in research activities, projects and controlled items in the research environment.
- Any exporter who provides technical assistance or support or who exports cyber surveillance items (researchers included) within the scope of export control regulations.
- Any supporting or administrative staff, or other personnel, who may be involved with internal procedures, including those related to physical and information security such as: IT, HR, finance, research centres, legal, and academic affairs etc.
- All academic staff including lecturers or faculty.

4.5 This ‘policy’ and ‘controls on technology export’ (i.e. export de-controls) do not apply to any information that is already in the public domain, basic scientific research and the minimum necessary information required for patent applications in the research environment (EU 2021/1700). This paragraph also applies to the university’s Internal Compliance Programme (ICP) for export controls.

5. Policy Statement

5.1 ATU is a technology-focused, research-driven and innovative university committed to advancing scientific knowledge and fostering further research. As a university, we are dedicated to ensuring that controlled items are protected from misuse or security abuse that could threaten international peace and security.

5.2 While the university strongly supports the freedom of knowledge, research, collaboration, and data exchange, it equally recognises the importance of export control compliance. It is committed to effectively communicating this responsibly to the university community.

5.3 This policy reflects requirements under the following legislation which provides for the control of exports:

- Control of Exports Act, 2023
- Regulation (EU) 2021/821
- The above-mentioned legislation is also read together with the requirements under the EU Commission Recommendation 2021/1700 of 15 September 2021 on internal compliance programmes for controls of research involving dual-use items.

5.4 Contravention of the provisions of the export control regulations and legislation by any university member, constitutes an offence and may be subject to a fine, imprisonment or both. An example of this can be seen in the university's Internal Compliance Programme (ICP) for export controls.

5.5 Furthermore, ATU risks facing significant reputational damage which could hinder its ability to achieve research objectives, and/or engage in collaborations with researchers or organisations from other countries. Additionally, this will result in jeopardising its ability to secure research funding which is vital for research organisations.

5.6 Non-compliance with export controls may also result in a loss of export privileges, and breaches of legal agreements, which could risk future research collaboration opportunities for the university and give rise to additional damages, respectively.

6. Roles and Responsibilities

a) Organisational and Governance Chart: Refer to Appendix A

6.1 Each member of the university community including, but not limited to, staff, faculty, researchers, contractors, visiting scholars, and other third parties who access any ATU campuses and facilities have the responsibility to fully comply with this policy.

6.2 All areas within the university that are exposed to controlled items have a responsibility to ensure that they have correct and reasonable mitigating measures and safeguards in place to prevent them from getting lost, stolen or shared without a valid export authorisation.

6.3 An exporter engaged in the export of controlled items, whether for research activities or other purposes, bears primary responsibility for adherence to export control requirements. This also includes an exporter who provides technical assistance or support or who export cyber-surveillance items (researchers included) within the scope of export control regulations.

6.4 Researchers must take appropriate steps to ensure compliance with all relevant obligations in relation to export control and trade sanctions laws within the research environment. They are required to undertake the prescribed mitigation measures and obtain necessary approvals while performing research activities.

6.5 While every member of the university is responsible for complying with the policy, processes and procedures, the following roles and responsibilities are assigned to meet the export control obligations as noted below:

President: committed to ensuring compliance with export control and trade sanctions regulations.

Chief Officer, Research, Innovation and Engagement or nominee: responsible for ensuring overall compliance with export control and trade sanctions regulations.

Governing Body: review and approve the policy, as necessary.

University Planning Team: review and approve the policy, as necessary.

Research Office: responsible for administrative and other duties relating to export control as follows:

- Provide support and assist the Research Compliance Coordinator where necessary or required (i.e. to assist in managing and maintaining export control records and documentation if required, integrate export controls within the research environment).
- Seek export control-related legal or compliance advice and report any concerns relating to export control within research where necessary.

Research Compliance Coordinator: respond to export control enquiries and breaches, review and provide recommendations for the export control screening procedures and other related procedures, provide guidance and support to relevant areas within the university on matters relating to export control compliance as required, prepare export authorisation applications with support of researchers, help staff understand any export authorisation conditions, conduct training and awareness sessions where required, conduct due diligence and identify mitigating measures necessary for specific activities.

Principal Investigators (PIs): overall responsibility of oversight to ensure compliance with export control and trade sanctions legislation for relevant research projects as required, determine if the project, including any associated items and goods, technology, software or knowledge are subject to export controls, export authorisations and trade sanctions legislation throughout its lifecycle (i.e. from beginning to end), conduct relevant end-user and consignee due diligence checks and partner vetting as required, and

ensure that all team members understand and adhere to export control requirements.

All Researchers: support compliance and monitor their own research project or activities in accordance with export control and trade sanctions legislation as required, review and evaluate if their own research activities, including associated items and goods, technology, software or knowledge are subject to export controls, export authorisations, or trade sanctions legislation throughout its lifecycle (i.e. from beginning to end), conduct relevant end-user and consignee due diligence checks and partner vetting as required, and follow the guidance provided by the principal investigator(s).

Faculties and Research Centres: to assess and identify controlled items and export control requirements within their area with the support of the Research Compliance Coordinator and implement any reasonable mitigating measures where required, to safeguard controlled items and reduce the risk of their loss, theft, or unauthorised export.

Research Legal Solicitor: ensure that all relevant formal legal agreements abide by the applicable export control laws and record-keeping requirements, where necessary.

Estates/Building and personnel: to assess, determine and implement any reasonable measures within ATU buildings and campuses, where required, to mitigate and reduce the risk of loss, or theft of controlled items.

Human Resources: to ensure that an identification verification process is in place for staff who are recruited at the university at the time of application (e.g. nationality).

IT Department: to support compliance with information security requirements relating to controlled items and implement any reasonable mitigating measures, where necessary, to safeguard such items.

All Staff: to become familiar with, understand and apply export control requirements as follows:

- Report any export control concerns, suspicions or related activities to the Research Office or Research Compliance Coordinator, where necessary.
- Seek guidance on export control matters by reviewing relevant export control resources, guidance materials, and applicable legislation, and by consulting with the Research Compliance Coordinator where appropriate.
- Ensure compliance with export control regulations in their work, where necessary.

b) Training and Awareness

6.6 Training and awareness-raising sessions will be implemented to educate and familiarise staff with export control regulations and related requirements, and to ensure that they can take appropriate action when confronted with any breaches or concerns.

6.7 The goal of training is to infuse a culture of compliance and responsibility in relation to export controls throughout the university.

6.8 General export control training will be conducted by the Research Compliance Coordinator, once upon policy implementation/as part of onboarding, and will then be subsequently updated and provided every three years.

6.9 The Research Compliance Coordinator is responsible for providing general export control training to:

- Any supporting or administrative staff, or other personnel, who may be involved in internal procedures, including those related to physical and information security such as: IT, HR, finance, research centres, legal, and academic affairs etc.
- Academic staff including lecturers and faculty.

- Researchers, research staff, and management who are regularly involved and engaged with research activities (especially high risk sensitive research areas likely to trigger dual-use export control), projects and controlled items in the research environment.

6.10 Additional targeted training sessions will be developed and delivered by the Research Compliance Coordinator as required. Such training may be provided to address:

- Regulatory updates and new legislative requirements.
- Amendments to export control policies and procedures.
- Specific requests, as deemed necessary.

6.11 The above-mentioned training sessions will be updated, as necessary, in line with best practice.

6.12 The Research Compliance Coordinator will maintain a training register to ensure accurate recordkeeping and to support compliance monitoring and audit requirements.

6.13 All researchers (including PIs and others engaged in the project) must attend mandatory export control training sessions provided by the university as required, to understand how export controls may impact or apply to their research work.

c) Record-Keeping

6.14 The Research Compliance Coordinator and Research Office (only where necessary or required) will be responsible for establishing, maintaining, and securing a safe and encrypted system for all export control documentation, records and information.

6.15 It is their duty to ensure that the above-mentioned documentation, records and information are accurate, up-to-date, and properly maintained. They must also be clearly marked, labelled and easily understood.

6.16 Additionally, they should ensure that all necessary university members are informed and educated about their record-keeping requirements associated with export controls.

6.17 These documents will include (non-exhaustive list):

- Records of export control training sessions and training participants' registers.
- Records of any communications and correspondences relating to exports or export authorisation applications as required for audit purposes (i.e. with DETE, third parties and researchers etc).
- All relevant export control screening procedure documents, forms and/or export control, end-user and consignee due diligence and partner vetting assessments.
- All transactional documentation relating to final exports.
- All export authorisation applications with supporting documents.
- Activity logs of any queries, breaches, suspected breaches and corrective actions taken.
- Ancillary documentation (e.g. compliance notices from the DETE etc).

6.18 The university will ensure that these records are kept for a period of 6 years from the end of the year in which the export took place or longer if required by the export authorisation (i.e. licence) or any applicable legislative requirement.

d) Audits, Reporting and Corrective Actions

6.19 Export authorisation applications and other export-related documents may be subject to audits by the Department of Enterprise, Tourism and Employment (DETE).

6.20 There will be more detail regarding participation and process of the audits held by the Department of Enterprise, Tourism and Employment (DETE) in the university's Internal Compliance Programme (ICP) for export controls.

6.21 The Research Compliance Coordinator should conduct internal audits on a cyclical basis and risk-based basis on a sample number of existing export authorisations, research projects and related-activities ensuring that all key areas are assessed over time according to risk and available resources. The internal audit results shall be reported to the Chief Officer, Research, Innovation and Engagement or nominee.

6.22 The Research Compliance Coordinator shall assess the audit results, maintain an audit log as well as report with corrective actions, lessons learned and address any necessary updates required as part of continuous improvement of export control compliance.

6.23 All members of the university must fully cooperate, assist, and provide support in connection with any export control audits and audit requests made by the Department of Enterprise, Tourism and Employment (DETE), and where necessary ATU internal.

6.24 The university commits to continuously review its export control policies and processes to identify potential risks and implement remedial actions to mitigate those risks, as necessary.

e) Physical and Information Security

6.25 The university is committed to ensuring that the appropriate safeguards are in place for the protection of controlled items, including dual-use or military items, in compliance with applicable export control legislation.

6.26 ATU (with the support of all relevant staff members) will ensure that all or any tangible controlled items are correctly packaged, labelled and securely maintained, both on ATU campuses and during travel.

6.27 ATU will implement reasonable information security controls and measures to ensure secured storage and controlled access of all or any intangible controlled items, particularly dual-use and military software or technology,

tech-know-how, or any other controlled electronic data outputs. These measures will be supported where necessary, by appropriate safeguards, including but not limited to antivirus checks, file encryptions, audit trails and logs, user access controls to identify, detect and mitigate security risks.

6.28 The university further commits to complying with the Ireland National Guidelines for Research Security in relation to export controls once they do come in effect.

f) Travel Security

6.29 All exporters (researchers included) must consider necessary security and travel protocols when carrying or transporting tangible or intangible controlled items, particularly dual-use or military, to other destination countries, institutions, within all the ATU campuses, research centres and rooms etc. Failure to do so may result in loss, theft or unauthorised access of controlled items. For a more detailed pre-travel checklist, refer to Appendix H.

g) Customs Declarations

6.30 All exporters (researchers included) must ensure that customs declarations are made for all relevant exports, where necessary.

6.31 When transporting controlled items to airports and other transit points, exporters must ensure that all relevant documentation is completed as required by applicable customs laws and regulatory requirements.

6.32 In cases where controlled items are being returned, exporters must ensure that it is handled in accordance with applicable customs laws and regulatory requirements.

6.33 The university will implement and develop necessary procedures and processes to support customs handling processes within export controls in due course.

7. Internal Compliance Programme (ICP) for Export Controls

7.1 The university has developed the Internal Compliance Programme (ICP) for export controls which systematically addresses and seeks to mitigate risks associated with the control of exports, particularly with focus on research organisations involved with dual-use controlled items. It should be read together with this policy for reference.

7.2 The ICP for export controls contains supporting export control procedures and processes (internal) comprising a comprehensive associated set of export control screening procedures and processes (including supporting forms) along with other related export control processes. These will be developed, implemented and enforced in due course for researchers, research organisations and the university in terms of the EU Commission Recommendation 2021/1700, and the Control of Exports Act 2023.

7.3 It covers the following:

- Chief Officer, of Research, Innovation and Engagement or nominee statement of commitment to export controls compliance.
- Associated set of export control screening procedures and processes (including supporting forms) that will be developed, implemented, and enforced in due course, to assist research organisations and researchers in meeting their export control and trade sanctions requirements, with focus on dual-use items and goods, technology, software and knowledge which research organisations are more likely to work with or have access to in the research environment. This is intended to guide and assist all researchers to comply with export control requirements. They provide a practical way to comply and serve as a helpful tool to guide them through the project assessment, relevant due diligence checks, and proper evaluation while also maintaining a record of compliance to support audits and reviews.
- Procedure for export control audits with the Department of Enterprise, Tourism and Employment (DETE).
- Procedure for export authorisation applications.

- Due diligence measures and obligations for staff members who are directly and indirectly affected by export controls.
- Procedure for breaches, suspected breaches and query handling.

8. Development and Review of Related Policies and Procedures

8.1 The Research Compliance Coordinator with support of research management, will develop and review policy, frameworks and procedures, as required, relating to the implementation of the export control policy, in due course, considering trade sanctions legislation, research security and export control legislation.

8.2 These may include but are not limited to:

- Security policy for and around export-controlled items throughout the lifetime of a research activity/project.
- Destruction policy for export-controlled items, including laboratory equipment, project components, materials, samples that may need to be disposed.
- Whistleblowing policy for export control breaches.
- Travel policy which will address security protocols in relation to travelling with laptops or other electric devices that have controlled technology or software etc, and/or travelling with any sensitive controlled items, samples, prototypes etc.
- Research collaboration policy.
- Any other export control related policies as necessary (e.g. patenting and licensing research results, publishing, electronic transmission etc).

9. Policy Compliance, Monitoring and Review

9.1 The Research Compliance Coordinator will continuously monitor the effectiveness of the policy, identify issues, and conduct a formal annual review of the policy.

10. Export Control Breaches and Non-Compliance

10.1 The university will take responsibility for reporting any suspected or confirmed instances of non-compliance with export control regulations. This will be addressed with the Research Compliance Coordinator with support of research management where required and necessary.

10.2 If there are any suspected breaches or confirmed breaches of this policy and the export control regulations and legislation, it should be documented in writing with the respective corrective actions taken to remedy the breaches.

10.3 Additionally, the Research Compliance Coordinator will maintain a log noting any/all incidents or breaches and remedial actions to ensure accountability.

10.4 The university will investigate such incidents and put in place appropriate procedures, taking appropriate corrective actions, which may include but not limited to:

- Implementing additional safeguards.
- Conducting additional export control training.
- Notifying relevant government authorities such as the Department of Enterprise, Tourism and Employment (DETE) or An Garda Síochána if required.

10.5 All university members who breach this policy will be subject to the ATU-wide disciplinary procedure.

10.6 ATU reserves the right to report incidents or violations to the Department of Enterprise, Tourism and Employment (DETE) or An Garda Síochána, where necessary.

11.Contact

11.1 Export control queries or related issues regarding export controls should be directed to:

Email: exportcontrols@atu.ie

Title: Research Compliance Coordinator

11.2 All export control queries will be addressed within 7-14 working days, or longer in the event of unforeseen delays. The Research Compliance Coordinator may request additional information or documents if required, either via email or by arranging meetings.

11.3 Any export control breaches and/or non-compliance of export controls should be sent to:

Email: exportcontrols@atu.ie

Title: Research Compliance Coordinator

11.4 The outcome of the export control breach investigation could take between 14-21 working days, or longer in the event of unforeseen delays. However, the Research Compliance Coordinator will provide relevant updates and progress on the investigation.

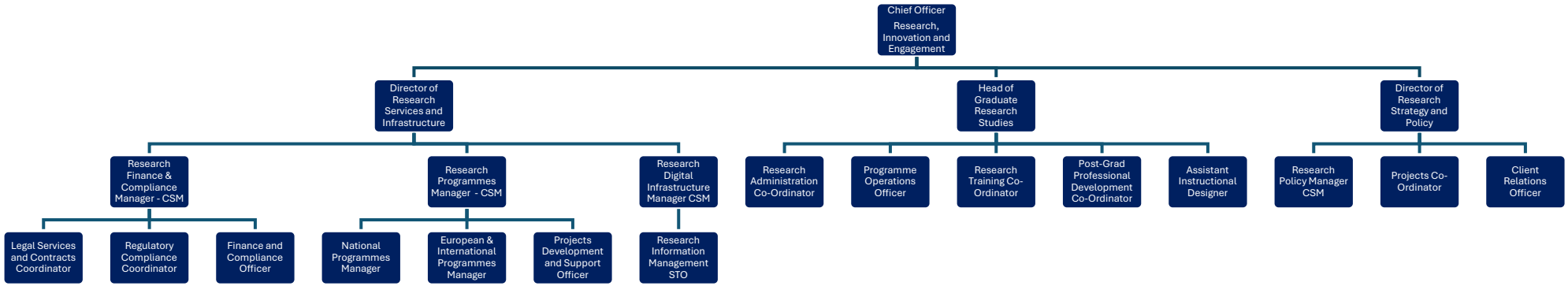
12. Appendices A-H: Supporting Documents and Helpful Resources

12.1 The following appendices contain supporting documents and helpful resources to assist with export controls, governance, and related matters.

- **Appendix A:** Organisational and governance chart.
- **Appendix B:** Useful resources.
- **Appendix C:** Appendix 1 of the EU Commission Recommendation 2021/1700 (Possible research areas that are more likely to be impacted by dual-use export controls).
- **Appendix D:** Appendix 2 of the EU Commission Recommendation 2021/1700 of 15 September (Research scenarios that may trigger dual-use export controls and where researchers may be regarded as exporters).
- **Appendix E:** Common export control pitfalls for research organisations and researchers.
- **Appendix F:** Due diligence and partner vetting guidance.
- **Appendix G:** Understanding export control obligations for research organisations and researchers.
- **Appendix H:** Pre-travel checklist for controlled items.

Appendix A: Organisational and Governance Chart

This is the current proposed ATU structure for Research as of July 2025.



Appendix B: Useful Resources

- Control of Exports Act, 2023
- Regulation (EU) 2021/821 of the European Parliament of 20 May 2021 - EU Regulation - 2021/821
- Department of Enterprise, Tourism and Employment Export Control Page
- EU Commission Recommendation 2021/1700 of 15 September 2021
- EU Dual-Use List (this list is updated every year, review the most recent version using https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202402547).
- EU Common Military List (this list is updated every year, review the most recent version using https://eur-lex.europa.eu/homepage.html)
- Eu Sanctions Map
- EU Guidance on Enhanced Due Diligence
- EU Information on the "No Re-Export to Russia" Clause

Appendix C: Appendix 1 of the EU Commission Recommendation 2021/1700

Appendix 1

Research areas that are more likely to be impacted by dual-use export controls

The following research areas are more likely to be impacted by dual-use export controls than other research disciplines. Please note that this list is non-exhaustive and may serve as (non-binding) tool to more easily identify relevant research. In this Appendix, the dual-use descriptors (right column) are rather general in nature. Specific export controls comprising sharp technical parameters are summarized in the Annex I to the EU dual-use Regulation, which should be consulted primarily.

Research area	Dual-use descriptors
Biology and (nano)biotechnology	Human, plant and animal pathogens Toxins Biological protection, containment and handling equipment
Chemistry Advanced material science	Chemicals, polymers, lubricants and fuel additives Chemical manufacturing facilities, equipment and components such as pumps, heat exchangers, valves and distillation columns Chemical protection, containment and handling equipment
Nuclear physics and engineering	Nuclear reactors and specially designed or prepared equipment and components Nuclear material
Energy and environmental technology	Optical and acoustic sensors Cameras
Computer science and engineering Information and communications technology	Source code for some listed acoustic data processing Digital ruggedized computers Intrusion software related items Telecommunications systems, equipment, components and accessories (including interception and jamming) Information security hardware, software and technology (including encryption and cryptanalysis)

Avionics and aerospace engineering and design	Accelerometers Gyroscopes Navigation (receiving) systems Drones Launch platforms Satellites Aero gas turbine engines Ramjet, scramjet or combined cycle engines
Semiconducto	Integrated circuits Semiconductor manufacturing, testing or inspection equipment Wafer substrates (Computer-aided-design) software for semiconductors
Optical engineering	Lasers Optical sensors Imaging cameras

Robotics and process automation	Machine tools Robots, end-effectors and remotely controlled articulated manipulators Dimensional inspection systems
Additive manufacturing (3D printing)	Feedstock materials Manufacturing equipment
Quantum technologies	Quantum cryptography
Artificial intelligence and machine learning	Neural network integrated circuits Neural computers Electronic components
Naval technologies	Surface vessels Underwater vessels Underwater vision systems Power transmission and generation systems

Cyber-surveillance items	Mobile telecommunications interception equipment Internet surveillance systems Tools for the generation, command and control, or delivery of intrusion software Law enforcement monitoring software Digital forensic/investigative tools

Appendix D: Appendix 2 of the EU Commission Recommendation 2021/1700

Appendix 2

Research scenarios of where export controls may come into place

The following are scenarios where dual-use export controls may come into place. The list is non-exhaustive.

Scenario	What does the EU dual-use Regulation say?	To be considered as well
Teaching, consulting, collaborating or working on research involving dual-use items inside customs territory of the Union with visiting third country researchers	— The EU dual-use Regulation does not foresee controls for non-EU persons accessing dual-use items inside the customs territory of the Union. Hence, no licence is needed as long as the controlled dual-use items remain inside the customs territory of the Union. When the visiting third country researcher returns home with access to (or in possession of) the controlled dual-use item, then a licence is needed.	— In some cases, based on national provisions, a technical assistance licence is required or the supply of technical assistance is prohibited. — A licence may be required in case a sanctioned entity or a natural/legal person of a sanctioned country seeks cooperation inside the EU. In some cases such cooperation is prohibited according to EU sanctions.
Teaching, consulting, collaborating or working on research involving dual-use items outside customs territory of the Union	— The EU dual-use Regulation does not foresee controls for EU persons engaged outside the customs territory of the Union in research involving dual-use items. Hence, no licence is needed in principle *if there is no access to controlled dual-use items from within the customs territory of the Union.*	— In some cases, based on national provisions, a technical assistance licence is required or the supply of technical assistance is prohibited. — A licence may be required in case a sanctioned entity or natural/legal person of a sanctioned country seeks cooperation inside the EU. In some cases such cooperation is prohibited according to EU sanctions.
Organising inside customs territory of the Union a (virtual) conference/meeting/seminar/… or presenting at a (virtual) conference/meeting/seminar/… on research involving dual-use items	— The EU dual-use Regulation does not foresee controls for non-EU persons accessing dual-use items inside the customs territory of the Union. Hence, no licence is needed *if the controlled dual-use items remain inside the customs territory of the Union.* When the visiting third country researcher returns home with access to (or in possession of) the controlled dual-use item, then a licence is needed. — If the conference/meeting/seminar is virtual and transmitted to a destination outside of the EU, then a license is needed for that part of the research that involves controlled dual-use items.	— In some national cases, a technical assistance licence is required — It is a good compliance practice to warn participants of licence requirements when exiting the customs territory of the Union with the controlled item(s). — A licence may be required in case a sanctioned entity or natural/legal person of a sanctioned destination seeks cooperation inside the customs territory of the Union. In some cases such cooperation is prohibited according to EU sanctions.
Organising outside customs territory of the Union a (virtual) conference/meeting/seminar/… or presenting at a (virtual) conference/meeting/seminar/… on research involving dual-use items	— The EU dual-use regulation does not foresee controls for EU persons engaged outside the customs territory of the Union in research involving dual-use items. Hence, no licence is needed in principle — *if orally presented, even when recorded on the spot, as long as there is no access to controlled dual-use items from within the customs territory of the Union.*	— In some cases, based on national provisions, a technical assistance licence is required or the supply of technical assistance is prohibited. — A licence may be required in case a sanctioned entity or a natural/legal person of a sanctioned country seeks cooperation inside the EU. In some cases such cooperation is prohibited according to EU sanctions

	— *if accompanied by presentation or other conference material where the information is not meeting the controlled technology threshold(s).* — The EU dual-use regulation requires a licence, — *if there is access to controlled dual-use items from within the customs territory of the Union.* — *if accompanied by presentation or other conference material (carried in paper, on laptop or other physical carrier such as USB stick) that contains controlled dual-use technology.*	
Publishing listed dual-use technology	— A publication including technology that meets the thresholds for dual-use control needs an export authorisation. The intention to publish (and thus the act of publishing) is not enough to be considered to be in the public domain and is therefore not exempted from control. The export control authorities rely on the due diligence of research organisation to screen prepublications in sensitive research areas. — In case a (draft) publication (or raw data) meets the thresholds for containing export controlled dual-use technology it is subject to export controls. This applies to both the pre-publication phase and to the actual publication phase. In principle, this can also apply to Master or PhD thesis that meet the controlled technology threshold(s).	The researcher or research organisation could consider to amend or omit the specific parts that contain the controlled technology or restrict the access to these specific parts. If mitigation is not feasible the researcher or research organisation should contact the competent authority how to fulfil the licence requirement (e.g. individual licence application).
Patented information and information for patent application	— No licence is needed in principle, as the export of patented information that is fully disclosed on the public record is considered to be "in the public domain" and hence exempted from export controls. — No licence is needed for the export of the minimum necessary information for patent applications.	
Export of tangible dual-use items (goods), including prototype design and second-hand lab equipment	— Research organisations may (re)sell, donate or lend dual-use items or temporarily export them for their own research projects. Regardless whether the items are new, a prototype or second-hand, they require a licence for export if listed in Annex I and for intra-EU transfers if listed in Annex IV of the EU dual-use Regulation.	

Appendix E: Common Export Control Pitfalls for Research Organisations and Researchers

Export control pitfalls	Risks	Mitigation
Improper sharing of controlled information or data during presentations, conferences or research visits etc.	Accidental disclosure of controlled technical information or data in presentation slides, posters, speeches or lecture content without prior clearance and a valid export authorisation.	• Review all presentation slides, posters, speeches, lecture content, and other related material before sharing at conferences, or research visits etc.
Unrestricted access to controlled datasets or software.	Providing third parties, entities, other research organisations, institutions, or students access to controlled datasets or software.	• Access to controlled datasets and software must be restricted and adequately protected. • Confirm, verify or validate the permissions of all end-users to ensure that only authorised individuals have access.
Improper sharing of controlled information or data through informal channels. This includes casual conversations (e.g. over coffee), informal online or in-person meetings, personal emails or exchanges, and unregulated electronic screen sharing.	Informal sharing of controlled technical information or data without prior clearance and a valid export authorisation.	• Only discuss and share controlled information with authorised individuals who have valid clearance. • Use university approved secure communication channels (i.e. not personal or unverified accounts) for any exchanges. • When in doubt, avoid discussing the topic and consult the Research Compliance Coordinator first. • Review all materials in advance before sharing electronic screens or sending any emails to ensure that all recipients or attendees are authorised.
Improper sharing of controlled information or data via third-party cloud storage or virtual platforms.	Uploading controlled technical information or data to cloud services, devices, virtual or software platforms hosted in other countries, institutions or by third-party service providers.	• Use only university approved secure servers, cloud, devices, virtual or software platforms and storage systems. • If uncertain, seek guidance and support from the Research Compliance Coordinator.

Returning with controlled technical know-how or data from conferences, research visits and other events without clearance and a valid export authorisation.	Transferring controlled technical knowledge without prior clearance or a valid export authorisation.	• Verify if any information or data is controlled before bringing it back. • Store securely, if needed, and consult the Research Compliance Coordinator before sharing or disseminating such data.
Providing technical assistance or advice within the scope of export control regulations during conferences and presentations etc.	Accidental disclosure of controlled technology or technical assistance without prior clearance or a valid authorisation.	• Review presentation material and discussions in advance. • Remove controlled information or data and only share content that is approved and authorised.
Lack of training or awareness of export control and trade sanctions requirements.	Non-compliance of export control and trade sanctions legislation.	• Attend or complete export control training and stay up to date with any export control regulatory changes. • Review relevant resources, guidance materials, and applicable legislation, and consult with the Research Compliance Coordinator as appropriate.
Inadequate partner screening and due diligence.	Non-compliance of export control and trade sanctions legislation. There could also be possible diversion risks where controlled goods and items, technology, software or information ends up somewhere other than the authorised end-users and consignees, or dual-use controlled items may be diverted for the development or manufacture of weapons. Additionally, there is risk of possible re-export without valid export authorisation.	• Conduct thorough due diligence on the destination country, end-users and consignees before any export. • Seek guidance and support from the Research Compliance Coordinator as required.
Incorrect classifications of research products, goods and items, technology, software or data for the research project or activity at hand.	Misclassification may lead to exporting dual-use or military technology, software, information or data without prior clearance or a valid export authorisation.	• Seek guidance and support from the Research Compliance Coordinator or DETE on classification matters. • Reassess classifications and research work whenever the scope of the project changes, or when new elements, collaborations or technologies are introduced.

		• Review the latest export control lists regularly.
Transiting controlled items through certain countries without prior clearance or valid authorisation.	Violating embargoes or transit restrictions on route even if the end destination (e.g. end-users and consignees) is permitted.	• Verify transit routes and intermediary countries for trade sanctions and restrictions. • Obtain the necessary prior clearance and valid authorisation, if required.
Assuming that if an item or technology is not contained in the Dual-Use List, then export controls does not apply.	Accidental disclosure of non-listed dual-use items or technical data or knowledge (while even if not listed) that may be used for weapons of mass destruction, military or sanctioned end users.	• Review Articles 4,5,9 and 10 of the EU Regulation 2021/821 for guidance.
Assuming all research projects or activities qualify as 'basic scientific research' or are 'in the public domain' and are therefore exempt from export controls.	This could lead to the uncontrolled sharing and accidental disclosure of dual-use or military controlled items.	• Confirm the applicability of exemptions with the Research Compliance Coordinator prior to sharing or publication of results.
Intra-Transfers between EU Member States are not subject to export controls.	Non-compliance of export control legislation.	• Refer to Annexure IV of the Dual-Use List which contains specific sensitive items that do require valid prior clearance and an export authorisation even for EU Member State transfers.
Assuming that due diligence and partner vetting are unnecessary simply because the destination country of the partner or entity (e.g. end-user and consignee) is not under any trade restrictions or sanctions.	Non-compliance of export control and trade sanctions obligations and legislation. There may be other concerns related to the destination country partner or end-users and consignees (e.g. indirect linking to countries or partners that are restricted or have trade sanctions, past violations, or diversion risks etc).	• Seek guidance and support from the Research Compliance Coordinator. • Conduct due diligence and partner vetting before all exports even if the destination country of the partner or entity (e.g. end-users and consignees) is not under any trade restrictions or sanctions.
Assuming that low-risk research areas or activities (research outside traditionally high-risk dual-use areas) are always safe and pose no compliance risk for export control.	Non-compliance of export control legislation. New collaborations, technology or project developments may introduce controlled items and may still pose export control and ethical risks.	• Seek guidance and support from the Research Compliance Coordinator. • While there are some research areas that are at greater risk, it remains vital that all researchers are aware of how export controls may impact their research work in certain circumstances.

Appendix F: Due Diligence and Partner Vetting Guidance

Outlined below are guiding points to assist in understanding due diligence and partner vetting obligations (i.e. end destination country, end-user, and consignee checks), in relation to trade sanctions and export control requirements.

	Clearly establish the end destination country of the partner or entity (e.g. end-users and consignees) and refer to the EU sanctions map for up-to-date information about current trade sanctions and embargoes by country.
	Obtain an 'End-Use Certificate' from the destination country before applying for an export authorisation (templates are available on the DETE website).This certificate should clearly state the intended use of the controlled goods or technologies and identify the parties involved.
	Conduct and record thorough due diligence on the destination country, end-users and consignees before any export. This involves actively researching, verifying, and assessing any potential risks associated with exporting to a particular destination.
	Examples of due diligence activities include: conducting sanction screening using the EU sanctions map , identifying diversion risks, investigating backgrounds, confirming physical addresses or locations, checking for past export violations or fines, spotting any red flags ot suspicious activities including unusual travel route or packaging requests, reviewing public reports, evaluating ethical risks or other concerns.
	Evaluate the risk level of exporting to the intended destination country, outline and document the reasons for proceeding with the final export.
	If there is uncertainty or doubt, consult the Research Compliance Coordinator for guidance before exporting any controlled items to a particular destination, especially if it is restricted or has sanctions.

Appendix G: Understanding Export Control Obligations for Research Organisations and Researchers

Know the research work and products involved	Get familiar with the export control lists,understand your research work and identify if it involves controlled items (particularly dual-use or military). Consider emerging technologies and sensitive research areas (eg. AI, engineering, cyber security, nuclear, robotics etc).
Classify the research work and products involved	Assess if the research goods and items, technology, software or knowledge (tech-know-how) appears on any of the export-controlled lists and if uncertain, consult with the Research Compliance Coordinator or the DETE for guidance and support.
Know the destination country	Verify the relevant destination country,end-users and consignees for all exports of controlled items. Conduct thorough due diligence and partner vetting to avoid unintentionally supporting illegal exports, involvement in WMD proliferation, or military end-use in restricted or embargoed countries.
Document assessments	Maintain records of all export control, end-user and consignee due diligence and partner vetting assessments, relevant supporting forms, decision-trees and considerations for the research work involved (whether it is or is not export controlled). Ensure records are available for DETE or internal audits.
Apply for export authorisations	Contact the Research Compliance Coordinator to apply for an export authorisation, as and where required .
Monitor export authorisations	Maintain oversight of export authorisations and track their expiry dates to ensure timely renewals.
Training and awareness	Attend or complete export control training, review relevant resources, guidance materials and applicable legislation and stay updated on regulatory changes.
Report issues	Immediately report any breaches, red flags or suspicious activity to the Research Compliance Coordinator.

Appendix H: Pre-Travel Checklist for Controlled Items

Consult the Research Compliance Coordinator	☐ Consult the the Research Compliance Coordinator before travelling with controlled items.
Complete export control training and ensure all neccessary documentations are in place	☐ Complete or attend export control training and be aware of your export obligations. ☐ Ensure that all relevant legal agreements are in place. ☐ Carry important travel documentation (eg.valid export authorisation and customs declaration as required and where neccessary). ☐ Keep key emergency and insitutional contacts while travelling.
Secure and manage tangible controlled items	☐ Clearly mark, package and label items (without attracting any undue attention). ☐ Securely pack items (eg. lockable laptop, cable locks etc). ☐ Prepare an inventory with serial numbers, size, shape and quantity. ☐ Avoid transporting or carrying items if it is not required. ☐ Use protective baggage or carriers to protect items. ☐ Track and trace items at all times while travelling. ☐ Arrange secure, access controlled storage at research centres, airports, rooms, entities or other insitutions where neccessary. ☐ Carry any required protective equipment for carrying controlled samples, chemicals or other items.
Secure and manage intangible controlled items	☐ Store controlled technical data (tech-know-how), software or technology on ATU insitutional devices only. ☐ Use encryption , access control and strong authentication measures. ☐ Classify and clearly mark all sensitive data. ☐ Enable backup features to prevent lost or stolen data. ☐ Keep track of and trace all electronic devices carrying controlled data while travelling. ☐ Do not use unsecured USBs, flashdrives, networks or untrusted devices for sharing or uploading any controlled data. ☐ Use only university approved software platforms for uploading or storing any controlled data or projects involving controlled data and consult the Research Compliance Coordinator for further guidance.
Report any lost, stolen or unauthorised access of controlled items immediately	☐ Report any lost, stolen or unauthorised access of controlled goods and items, technology, software or data to the Research Compliance Coordinator immediately.