SAND2024-10872O

Export Controls Internal Compliance Program (ICP) Guidance Manual for Research Organizations

Emilya Titanyan
Director and Research Supervisor
Innovation Research Center, Yerevan, Armenia

August 2024

* The views expressed in this paper are those of the author and do not necessarily reflect the position of Sandia National Laboratories. The inclusion of available software and compliance tools does not constitute endorsement.

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

This page left blank

CONTENTS

DEFINITIONS

Term	Definition
Dual-use items	Any type of goods, any information, product of intellectual activity, including software and technical assistance used for civil purposes which, by virtue of their nature can also be used for military purposes, including for production of weapons of mass destruction and means of their delivery, at the exception of information that can be obtained from the public domain or basic scientific research used for civil purposes which by virtue of its nature and properties can also be used for military purposes, including for production of weapons of mass destruction and their means of delivery.
Academia	Universities, research organizations in Republic of Armenia (hereinafter – also RA).
Weapons of mass destruction	Nuclear, radiological, chemical and biological weapons.
Means of delivery	Rockets and remotely piloted air vehicles which can be used for military purposes, including for delivery of weapons of mass destruction.
Transfer of dual-use items, information or products of intellectual activity	Export, transit, transshipment or brokering of dual-use items.
Export of dual-use items, information or products of intellectual activity	Outbound transportation of dual-use items, information and products of intellectual activity from the territory of the Republic of Armenia across its customs border.
Transit of dual-use items	Transportation of dual-use foreign items through the customs territory of the Republic of Armenia from the customs body of their entry into the Republic of Armenia to the customs body of their exit from the Republic of Armenia.
Transshipment of dual-use items	Transportation of dual-use items through the customs territory of the Republic of Armenia from the customs body of their entry into the Republic of Armenia to the customs body of their exit from the Republic of Armenia with the items being unloaded from the mean of transportation of entry and reloaded onto an other mean of transportation.
Brokering of dual-use items	Information or products of intellectual activity: intermediary services consisting in the negotiation or arrangement of transactions for the purchase, sale or supply of dual-use items, information or products of

Term	Definition
	intellectual activity from a foreign country to any other foreign country, or the selling or buying of dual-use items, information or products of intellectual activity that are located in foreign countries for their transfer to another foreign country.
Financial services on transfers of dual-use items	Information or products of intellectual activity: provision of funds in support of a international commercial transaction involving the transfer of dual-use items, information or products of intellectual activity.
Dual-use trade control	A system of measures undertaken in relation to the transfer of dual-use items, information or products of intellectual activity aimed to ensure the fulfillment of international obligations assumed by the Republic of Armenia, as well as the protection of its national security interests.
End-user	A foreign state, legal or physical entity of a foreign state that is the real user of the dual-use commodity, information or products of intellectual activity transferred from or through the Republic of Armenia.
End-use	Use of the dual-use items by the end-user in compliance with its declared purpose of use.
End-user certificate	Document containing information about the state or name, location and place of operations of the person (legal or natural) of such a state which is the recipient of dual-use items, information or products of intellectual activity; the description of the dual-use items, information or products of intellectual activity to be transferred ; the purpose of end-use of these items, information or products of intellectual activity which also certifies that the specified items, information or products of intellectual activity will not be transferred to any third country or person or will not be used for any purposes other than the declared one without the written and duly validated consent of the state governance body of the transferring country. The end-user certificate – if stipulated in the legislation of the importing country - shall be approved by the authorized state governance body of the end-user's country.
Research security	The implementation of measures and practices designed to protect sensitive research information, technologies, and data from unauthorized access, theft, exploitation, or misuse in relation to export control processes.

1. INTRODUCTION

In academic research and innovation, it is essential to balance open scientific exchange with security concerns. Dual-use items and intangible dual-use technologies that can be used for both civilian and military purposes present unique challenges. Effective export controls are necessary to prevent these items and technologies from being used to proliferate weapons of mass destruction or other illicit activities.

The guidance (hereinafter also ICP) highlights the various research areas and situations in which dual-use export controls may be required. It provides a list of red flags and several examples of how an Internal Compliance Program (ICP) might be established in a research organization. Previously, in July 2019, the Commission published similar guidance on ICPs for industry (Recommendation (EU) 2019/1318 of July 30, 2019 on ICPs for dual-use trade controls). Although these recommendations are not legally binding, they are valuable tools to fulfill legal obligations under the EU Dual-Use Regulation 2021/821.

The main purpose of the ICP in an academic context is to raise awareness of the importance of export controls among teachers, researchers and administrative staff. It provides the necessary tools and guidance to identify dual-use goods and intangible technologies, assess potential risks, and implement appropriate controls. By developing a culture of compliance, universities and research institutions can protect their research from misuse and contribute to global security efforts. Implementing ICP is particularly important for Armenia. As a country seeking deeper integration into the global research and technology ecosystem, Armenia must ensure that its academic and research institutions adhere to international export control standards. This is important not only to ensure compliance with global norms, but also to protect the country's scientific achievements and contribute to international security and nonproliferation efforts. Failure to comply with international export control regulations can have serious consequences for universities and research centres. It is important for institutions in Armenia to adhere to these rules to avoid several problems.

First, violating these rules can result in the loss of important funding. Many international funding organisations require institutions to follow EU standards. Otherwise, they may not receive the grants or financial support they need, which can slow down their research and limit their ability to work on international projects.

Secondly, non-compliance with EU rules can damage an institution's reputation. This means that other researchers, partners and the broad academic community may not trust the institution any longer. A negative reputation may also make it more difficult to attract talented students and researchers, which can have a negative impact on the institution's reputation and research progress.

In addition, failure to comply with these regulations can mean loss of access to some of the important technologies and materials needed to conduct research. This may prevent institutions from conducting cutting-edge research and remaining competitive in the global research arena.

Finally, institutions that do not comply with the rules may be left out of international co-operation. Many research projects require participants to comply with these regulations, and non-compliance can mean missed opportunities for collaborative work and knowledge sharing.

On September 23, 2021, the European Commission issued Recommendation (EU) 2021/1700 of September 15, 2021, concerning internal compliance programs (ICPs) for the management of research involving dual-use items and intangible dual-use technologies in accordance with Regulation (EU) 2021/821 of the European Parliament and of the Council. This regulation lays down rules for controlling the export, brokering, technical assistance, transit and transfer of dual-use items and technologies.

As the new EU Dual-Use Regulation 2021/821 enters into force on September 9, the Commission, in accordance with Article 26.1, has issued a guidance document specifically aimed at academia. The guidance is intended to help research organizations develop or review their internal policies and procedures, known as an internal compliance program (ICP), to ensure compliance with export control requirements for dual-use goods and technologies in research activities. The European Commission's Recommendation (EU) 2021/1700[1] and Regulation (EU) 2021/821[2] are significant for Armenian research organizations, even though Armenia is not an EU member state. These regulations set out guidelines for internal compliance programs (ICPs) for managing dual-use items and intangible dual-use technologies. They are relevant to Armenian organizations for several key reasons:

[1]https://op.europa.eu/en/publication-detail/-/publication/a5b08317-1c07-11ec-b4fe-01aa75ed71a1#:~:text=0-,Commission%20Recommendation%20(EU)%202021%2F1700%20of%2015%20September%202021,%2C%20brokering%2C%20technical%20assistance%2C%20transit

[2] https://eur-lex.europa.eu/eli/reg/2021/821/oj

First, Armenian research organizations frequently collaborate with international partners, including those from the EU. Understanding and adhering to EU regulations is essential for facilitating smooth cooperation and ensuring that joint projects comply with international standards.

Second, for organizations aiming to export dual-use items or seek funding and partnerships within the EU, compliance with these regulations is crucial. Non-compliance could result in restricted access to EU markets or sanctions, which would significantly impact the organization's ability to engage in international research and trade.

Third, aligning with EU regulations allows Armenian research organizations to meet global standards. This alignment enhances their reputation and credibility, positioning them as reliable and compliant partners in international collaborations.

Thus, as academia continues to push the boundaries of knowledge and innovation, implementing effective export control programs for dual-use goods and intangible technologies is vital. This guide can ensure that the fruits of scientific progress are used responsibly, preventing misuse and supporting international security and nonproliferation principles.

For universities, implementing robust research security measures is essential for several reasons. It protects sensitive technologies and data, preventing unauthorized access or transfer that could lead to misuse or exploitation. It also mitigates risks from malicious actors by safeguarding against espionage, theft, or sabotage by individuals or entities seeking to exploit academic research for harmful purposes. Furthermore, research security ensures compliance with legal obligations, helping institutions adhere to export control regulations and avoid legal penalties, thus maintaining their reputation. Finally, it supports national and international security efforts, contributing to global nonproliferation and preventing the spread of weapons of mass destruction.

Research security is not merely a compliance issue but a strategic imperative for academic institutions. By prioritizing it, universities can foster a secure and responsible research environment, balancing the pursuit of knowledge with the need to protect sensitive information.

2. LEGISLATION, AUTHORIZED BODIES AND PURPOSE

2.1. European Union (EU) Export Controls

European Union Council Regulation (EC) No 428/2009 initially set the framework for the EU's control over the export, transfer, brokering, and transit of dual-use items. This regulation was updated in September 2021 with Regulation (EU) No. 2021/821, now known as the "Dual-Use Regulation."

The European Commission's Recommendation (EU) 2021/1700 and Regulation (EU) 2021/821 are significant for Armenian research organizations, even though Armenia is not an EU member state. These regulations set out guidelines for internal compliance programs (ICPs) for managing dual-use items and intangible dual-use technologies. They are relevant to Armenian organizations for several key reasons:

First, Armenian research organizations frequently collaborate with international partners, including those from the EU. Understanding and adhering to EU regulations is essential for facilitating smooth cooperation and ensuring that joint projects comply with international standards.

Second, for organizations aiming to export dual-use items or seek funding and partnerships within the EU, compliance with these regulations is crucial. Non-compliance could result in restricted access to EU markets or sanctions, which would significantly impact the organization's ability to engage in international research and trade.

Finally, aligning with EU regulations allows Armenian research organizations to meet global standards. This alignment enhances their reputation and credibility, positioning them as reliable and compliant partners in international collaborations.

2.2. National Legislation

The principles of implementation of the state policy in the field of control over the exportation of dual-purpose items, the transit transportation thereof through the territory of the Republic of Armenia, the transfer of dual-purpose information and products of intellectual activity, the rights and liabilities of exporters of dual-purpose goods, the rights and liabilities of subjects transferring dual-purpose information and products of intellectual activity are regulated by the RA Law “On control over the exportation of dual-purpose items, the transit transportation thereof through the territory of the Republic of Armenia, as well as the transfer of dual-purpose

information and products of intellectual activity", the RA Government Decree No.924-N dated July 1, 2010, the RA Government Decree No.1785-N dated December 15, 2011 and the RA Government Decree No.808-N dated December 15, 2011 and Decision No. 808-N dated May 25, 2023.

2.3. Dual-Use Items and Scope of ICP

The Law on Export Control of the Republic of Armenia sets forth both the meanings of dual-use information and products of intellectual activity and dual-use items. For convenience, we provide a simplified definition here: Dual-use items include any type of goods, information, or products of intellectual activity (such as software and technical assistance or other technology (such as documents, plans, blueprints, sketches, diagrams, etc.)) used for civil purposes that, by their nature, can also be used for military purposes, including the production of weapons of mass destruction and their delivery systems. This excludes information obtainable from the public domain or basic scientific research used for civil purposes, which by their nature and properties can also be used for military purposes, including the production of weapons of mass destruction and their delivery systems.

Below is a non-comprehensive list of possible cases where academia might encounter export control issues:

- **Research Collaborations with Foreign Entities**

Example: A university team collaborates with a foreign university on a project involving dual-use technologies, such as advanced materials that could have military applications.

- **Foreign Nationals Accessing Controlled Technology**

Example: An international student working in a laboratory has access to research involving sensitive technologies, like aerospace engineering components, that are subject to export controls.

- **International Conferences and Publications**

Example: Researchers present findings on encryption technology at an international conference, sharing information that could be considered controlled technical data.

- **Field Research Abroad**

Example: A team conducts geological surveys in a foreign country, using equipment and data analysis tools classified as export-controlled.

- **International Shipments of Research Equipment**

Example: A university sends a high-precision laser system to a partner institution abroad for joint research, which requires an export license.

- **Development of Encryption Software**

Example: Computer science researchers develop software for secure communications, which may fall under export control regulations due to its potential use in national security.

- **Collaborative Research in Sensitive Fields**

Example: A joint project with an international partner involves research on nuclear physics, raising concerns about the transfer of sensitive information.

- **Grants Involving International Collaborations**

Example: A grant-funded project includes collaboration with a foreign university on developing new pharmacological compounds, possibly involving controlled chemicals.

- **Consultancy Services to Foreign Governments or Entities**

Example: Faculty members provide expert advice to a foreign government on cybersecurity measures, potentially involving controlled technical data.

- **Transfer of Proprietary Research Data**

Example: Researchers share proprietary data with international partners, including detailed information on advanced manufacturing techniques.

- **Development of Sensitive Technologies**

Example: A project develops new drone technology that could be used for both civilian and military applications, making it subject to export controls.

- **Student and Faculty Exchange Programs**

Example: Students and faculty from countries with export restrictions participate in exchange programs, involving access to sensitive research labs.

- **Hosting Foreign Visiting Scholars**

Example: A university hosts a visiting scholar from a country under sanctions, who may access controlled research areas or information.

- **Use of Controlled Software and Technology in Teaching**

Example: Courses include the use of specialized software for satellite imagery analysis, which is controlled under export regulations.

- **Participation in International Competitions or Projects**

Example: A team participates in an international competition on artificial intelligence, using algorithms that could have export control implications.

- **Exporting Biological Samples for Research**

Example: Biological samples, such as genetically modified organisms, are sent abroad for collaborative research, potentially requiring export licenses.

- **Cross-border Data Transfers for Joint Research**

Example: Data collected from joint research with foreign institutions is stored on servers located outside the country, raising export control issues.

- **Involvement in Defense-Related Research Projects**

Example: A university works on a project funded by the defense department, involving technology that could be used in weapons systems.

- **Donations of Equipment to Foreign Institutions**

Example: The university donates laboratory equipment to a foreign university, where the equipment could be used for research in controlled areas.

2.4. Research Stakeholders Involved in ICP

This Internal Compliance Program (ICP) is designed for all members of the Academia, including:

- University Administrators: To ensure institutional adherence to export control regulations.
- Researchers and Faculty: To maintain compliance with legal requirements in international research collaborations, and instruction and training provided to foreign students.
- Students: To understand their responsibilities when involved in research, particularly in science and technology fields.

This ICP has been implemented to ensure that the institution complies with all relevant export control regulations. Compliance with these requirements is critical to avoid legal fines and penalties, protect the institution's reputation, and ensure continued access to research funding and cooperative opportunities. The primary goal of this ICP is to establish a comprehensive system for managing export control compliance at the Academia in dual-use related field.

2.5. Authorized Bodies

The authorization body for export control in Armenia is the Ministry of Economy. In several cases, such as those involving biological items that contain viruses, the handling can fall under the jurisdiction of both the Security Council of Armenia and the Ministry of Economy For academic institutions also, it is essential to obtain the necessary permissions from the Ministry of Economy, ensuring that they have the required documentation and are in compliance with the regulations set by the authorized bodies.

3. ROLES AND RESPONSIBILITIES

Certain positions within Academia come with specific duties aimed at ensuring adherence to export compliance regulations. These roles are crucial for maintaining legal and regulatory standards. Below is a detailed outline of these roles and their associated responsibilities.

ROLE	RESPONSIBILITIES
Researcher	Researchers must ensure their work follows export control laws. They should attend relevant training sessions, keep accurate records of projects involving export-controlled items or information, and report any potential issues to the Export Control officer or other relevant administration official.
Administration staff	Administrative staff support the export control compliance program by maintaining necessary documentation and records, and facilitating the monitoring ongoing research and teaching activities on campus. They facilitate communication between researchers, the legal department, and export control officer. They also organize and schedule training sessions on export control for staff and faculty and report any administrative issues related to export control. They will also establish anonymous reporting mechanisms for potential export control violations at their organization.
Legal department	The legal department advises on export control laws and their impact on research activities. They ensure institutional policies and practices comply with these laws, and review contracts and agreement in the matter of export issues.
Deputy director in Scientific field	Deputy director in Scientific field oversees research activities to ensure compliance with export control laws. He/she implements and enforces export control policies in his/her department, supports researchers in understanding and complying with these requirements, acts as a liaison with the Export Control Officer, and allocates resources for compliance activities, including training and documentation.
Director	The Director provides leadership and management of export control compliance at the institution. Director develops and implements export control-related policies and procedures, identifies and manages risks associated with export-controlled research activities, ensures that export control policies are

	clearly communicated throughout the institution, and holds departments and employees responsible for compliance.
Export control specialist	He/she is the primary expert on export control laws and regulations. They monitor compliance across the institution, develop and deliver training programs on export control, review research proposals and contracts for compliance, and provide guidance to researchers and administration on export control issues. They also provide oversight and governance for the institution's export control program, develop and review policies and procedures related to export control, review and approve export control assessments and compliance plans, address incidents of non-compliance, and report to senior management on the status and effectiveness of the export control program.

4. SCREENING PROCEDURE

To determine whether an export is controlled, it is necessary to thoroughly examine the essential elements of export controls, ensuring that each aspect is carefully considered to ensure compliance and prevent unauthorized export transactions. It is important to fully understand all elements and considerations. This section provides a general checklist to assist with this process:

4.1. Items

Items[3]: Identify what the item is (tangible or intangible), its purpose, its military defense use, and whether it is subject to export controls.

Tangible items: For tangible items, exports usually involve the direct physical movement of items across international borders. These goods are usually subject to customs and trade regulations, as well as export control inspections.

Intangible items: For intangible item, export scenarios are less straightforward. Examples of how intangible exports may occur include:

- Transmission of software and technology via email or fax.
- Provision of support, engineering, and other services related to the use, production, or development of controlled items.
- Oral transmission, where the conversation content is equivalent to reading a document, including help-desk support.
- Availability of items on websites, such as software downloads and uploads.
- Technical assistance, including training, data for research and development projects, technical specifications, etc.
- Conference presentations, online lectures, presentations for researchers outside Armenia, and secondments outside Ireland.

[3]Control lists, also known as controlled dual use item lists, are official lists maintained by governments or international organizations that identify specific items, technology, software, or data that are subject to export controls. These items are regulated due to their potential use in weapons of mass destruction, military applications, or other sensitive areas that could pose a risk to national security or international peace if misused. Government of RA set 2 control lists : RA Government Decree No.1785-N dated December 15, 2011 https://www.arlis.am/DocumentView.aspx?DocID=157865 and Decision No. 808-N dated May 25, 2023 https://www.arlis.am/DocumentView.aspx?DocID=190787

- Publishing online research methods.

4.2. Destination

Identify the final destination, check for applicable sanctions or embargoes, assess the risk of diversion

In an academic setting, it is crucial to assess the destination of an export to ensure compliance with relevant regulations and prevent unauthorized distribution of controlled items. This involves considering various aspects of the destination to mitigate risks associated with export activities.

First, the final destination of the export must be determined. It is essential to verify whether the destination country is subject to any international sanctions or embargoes. Additionally, assessing the political and economic stability of the destination country can help evaluate potential risks.

Evaluating the risk of diversion is also important. The likelihood of the exported items being diverted to unauthorized destinations or users should be assessed. Measures such as thorough end-user verification and contractual safeguards can help mitigate these risks.

4.3. End User

Identify who will receive the goods, check for end-user restrictions and verify the identity of the end-user.

4.4. End Use

Determine how the recipient will use the item. Ensuring that exported items are used exclusively for their intended purposes is a crucial responsibility. It is vital to have a comprehensive understanding of the end-users of research and outputs. Many countries have identified specific entities, individuals, and regimes as prohibited or restricted, and these designations can extend to any business or industry partner in the transaction chain, including resellers or intermediaries.

To manage this, countries and organizations maintain lists of prohibited and restricted parties. Exporting to these parties often requires governmental approval or may be entirely prohibited. Consequently, it is essential to rigorously monitor these lists and adhere to export control regulations to ensure compliance and prevent the misuse of research and outputs.

4.5. Finance

Determine who will finance the product, what fees and commissions will be charged, what intermediaries will be involved, and the required statements in the contract documents.

4.6. Other Steps

Determine other important points relevant to the specific case. For example, in exchange programs, this could include checking gaps, social media profiles, and previous projects or jobs. For grants or collaborations, it might involve reviewing contracts, finance, the end user, and other pertinent details. The 'other' category provides the flexibility to conduct additional background checks as deemed necessary by the export control officer.

4.7. Guidance for Researchers

Researchers are encouraged to engage proactively in the export control screening procedure to ensure compliance with regulations and the protection of sensitive information. To proceed effectively:

1. Initial Assessment: Begin by conducting a preliminary evaluation of your project or item to determine if it might fall under export control regulations. This involves considering the nature of the item, its potential applications, and the destination or end-users involved.

2. Consultation: Engage with your institution's export control officer or compliance team early in the process. They can provide expert guidance on whether your project or item requires a more in-depth review and help you navigate the relevant regulations.

3. Use of Tools and Resources: Refer to available tools and resources, such as the decision-making tree and process outlined in Annex 2. These resources are designed to help you systematically assess each element of the export control process, ensuring that no critical aspect is overlooked.

4. Continuous Monitoring: Remain vigilant throughout the lifecycle of your project or export activity. Circumstances can change, and ongoing monitoring is necessary to ensure continued compliance with export control regulations.

For a detailed overview of the decision-making process and additional guidance, please refer to Annex 2. This annex provides a step-by-step guide to assist you in navigating the complexities of export control compliance.

5. PROCESS OF GETTING PERMITS

Universities and research centers frequently engage in cutting-edge research that may involve dual-use technologies. It's crucial for these institutions to understand and comply with the regulations to prevent any misuse of their research and technology. This helps ensure that their work is used only for peaceful purposes and does not inadvertently support military applications.

5.1. Types of Permits

There are three main types of permits required for handling dual-use items:

One-Time Permit: This permit is for individual researchers or scholars who are not private entrepreneurs. It allows them to export a single controlled item or transfer specific information to one recipient. This permit is valid for one year and is suitable for one-time transactions.

Individual Permit: This permit is for legal entities, such as universities or private businesses. It allows them to export or transfer controlled items or information to one end-user. This permit is valid for up to five years or the duration of the contract and is ideal for ongoing projects.

General Permit: This permit is for legal entities and covers the export or transfer of multiple controlled items to several recipients. It is valid for five years or the contract duration. This permit is useful for institutions involved in multiple international projects.

5.2. Applying for a Permit

To obtain a permit, institutions must submit the following documents:

1. **Application Form**: This form includes details about the institution, such as its name, legal status, and address, as well as the type of permit requested.
2. **End-User Certificate**: This certificate ensures that the recipient of the controlled items or information will use them responsibly and in accordance with the law.
3. **Technical Specifications**: Detailed descriptions of the controlled items or information to be exported or transferred.
4. **Contract Copies**: Copies of any contracts related to the export or transfer of controlled items or information.

5. **Declaration or Expert Report**: A statement confirming that the items or information fall under the category of controlled dual-use items according to the law.

5.3. Decision Process

Once the application and documents are submitted, the authorities will review them. A decision on the permit is typically made within 20 working days. If the permit is approved, the application is sent to various government bodies for further review. If there are any concerns or objections, the decision might be escalated to higher authorities, which can take a few additional days.

Fees

There are fees associated with obtaining permits:

- **General Permit**: 30,000 Armenian drams (AMD).
- **Individual Permit**: 30,000 Armenian drams (AMD).

These fees cover the administrative costs of processing the permits.

Reasons for Rejection

An application may be rejected if:

- The submitted documents are incomplete.
- The information provided is false.
- The planned activities do not align with the law's objectives, such as preventing the proliferation of weapons of mass destruction.

If an application is rejected, the institution will be informed of the reasons and may have the opportunity to appeal or correct any issues.

Transit Regulations

If controlled items need to be transported through Armenia, a prior notification must be submitted at least 25 working days before the planned transit. This notification should include details about the items, the means of transportation, and the involved parties.

6. RECORDKEEPING AND DOCUMENTATION

Effective recordkeeping and documentation are essential in academia to ensure compliance with export control regulations. Properly managing both hard copies and electronic information supports transparency, accountability, and operational continuity. The Academia should establish the rules regulating the work with export control information and documents in accordance with the requirements of current legislation. Academia must maintain proper documentation at least five years. Below is a list of key documents that should be retained:

1. **Export Permits:**

- **Copies of all export permits obtained for exporting controlled items, technologies, or information:** These permits are official authorizations granted by regulatory bodies, allowing the export of specific controlled items. Maintaining copies ensures that the institution can demonstrate compliance with legal requirements and quickly provide documentation during audits or inspections.
- **Documentation of the application process and any correspondence with regulatory agencies:** This includes all communications, such as emails and letters, between the institution and regulatory agencies during the permit application process. Keeping these records helps track the progress of applications, understand any conditions or limitations imposed, and provide a complete history of compliance efforts.

2. **Shipping Records:**

- **Commercial invoices, packing lists, and bills of lading for all exported items:** These documents provide a detailed account of the items shipped, including descriptions, quantities, values, and destination details. They are crucial for verifying the nature of exported goods and ensuring that they match the items listed in the export permits.
- **Shipping logs and courier service receipts detailing the movement of controlled goods:** These records track the physical movement of controlled items, providing a chain of custody from the institution to the final recipient. They help verify that shipments reach their intended destinations without unauthorized diversion.

3. **End-User Certificates:**

- **Certificates or statements from recipients verifying the end-use and end-users of exported items:** These certificates confirm that the recipient will use the exported items in accordance with the terms specified in the export permit and will not re-export them without proper authorization.
- **Any related correspondence confirming the recipient's compliance with export control regulations:** This includes communications that verify the recipient's commitment to adhere to relevant export control laws and regulations, ensuring that controlled items are not misused or illegally transferred.

4. **Technology Control Plans (TCPs):**

- **Detailed plans outlining how controlled technologies and information are managed and protected within the institution:** TCPs provide a framework for safeguarding sensitive technologies and information, detailing measures such as access controls, encryption, and secure storage. They help prevent unauthorized access and ensure that controlled items are only accessible to authorized personnel.
- **Records of employee training and acknowledgments of understanding and compliance:** These documents confirm that staff and students have received training on export control regulations and understand their responsibilities. They also include signed acknowledgments, demonstrating that individuals are aware of and agree to comply with institutional policies and legal requirements.

5. **Training Records:**

- **Documentation of export control training sessions attended by staff and students:** This includes attendance logs, training materials, and presentations used during training sessions. These records demonstrate that the institution is actively educating its personnel on export control compliance.
- **Attendance records, training materials, and certifications of completion:** These documents verify who attended the training, what topics were covered, and that participants successfully completed the training. They are essential for proving that the institution is taking steps to ensure compliance through education.

6. **Internal Audit Reports:**

- **Reports from internal audits assessing compliance with export control regulations:** These reports evaluate the institution's adherence to export control policies and identify any areas of non-compliance. They are valuable for identifying weaknesses in the compliance program and implementing corrective actions.
- **Records of findings, corrective actions taken, and follow-up audits:** These records document the outcomes of internal audits, including any issues discovered and the steps taken to address them. They also include follow-up audits to ensure that corrective actions have been effective.

7. **Communication Records:**

- **Emails, letters, and meeting notes related to export control matters:** These records capture all communications regarding export control, including discussions about specific transactions, compliance strategies, and regulatory updates. They provide a comprehensive history of the institution's efforts to stay informed and compliant.
- **Correspondence with regulatory agencies, internal communications about compliance, and discussions with external partners or collaborators:** These documents demonstrate the institution's proactive engagement with regulatory bodies and stakeholders to ensure compliance with export control regulations.

8. **Export Control Compliance Assessments:**

- **Documents related to periodic assessments of the institution’s export control policies and procedures:** These assessments evaluate the effectiveness of the institution's compliance program and identify areas for improvement. They are a critical component of ongoing compliance management.
- **Reports detailing the assessment process, findings, and any implemented improvements:** These reports provide a detailed account of the assessment process, including methodologies used, key findings, and actions taken to address identified issues. They serve as evidence of the institution's commitment to continuous improvement in compliance.

9. **Transaction Records:**

- **Detailed records of all transactions involving controlled items, technologies, or information:** These records include purchase orders, contracts, and invoices related to the acquisition, transfer, or sale of controlled items. They provide a complete history of the institution's dealings with controlled technologies and are essential for audits and investigations.
- **Purchase orders, contracts, and invoices related to the acquisition and transfer of controlled items:** These documents specify the terms of transactions, including the nature of the controlled items, quantities, prices, and conditions of sale or transfer. They are critical for verifying that all transactions comply with export control regulations.

10. **Visitor Logs:**

- **Logs of visitors who have accessed areas where controlled items or information are stored:** These logs record the names, dates, and purposes of visits by individuals who access secure areas. They help monitor and control access to sensitive technologies and information, ensuring that only authorized individuals are granted entry.
- **Records of visitor agreements and non-disclosure statements:** These documents confirm that visitors understand and agree to comply with export control regulations and institutional policies regarding access to controlled items and information.

11. **Scientific Documents:**

- **Research proposals and grant applications involving controlled technologies or information:** These documents outline the scope of research projects and identify any controlled items or information that may be involved. They are important for determining the need for export control reviews and approvals.
- **Lab notebooks and research records documenting experiments and findings related to controlled items:** These records provide detailed documentation of research activities, including methodologies, results, and analyses. They are essential for tracking the use and development of controlled technologies within the institution.

- **Publication drafts and correspondence regarding the dissemination of research involving controlled technologies:** These documents track the preparation and review process for publications, ensuring that any export control issues are identified and addressed before dissemination.
- **Records of collaborations and agreements with international researchers or institutions:** These records document the terms of international collaborations, including the handling of controlled items and information. They are critical for ensuring compliance with export control regulations in cross-border research activities.
- **Documentation of export control reviews and approvals for research projects:** These documents confirm that research projects involving controlled technologies have been reviewed and approved by the institution's export control compliance office, ensuring that all regulatory requirements are met.

6.1. Secure Storage and Organized Filing

Hard copies of documents should be stored in locked cabinets or rooms with controlled access. These storage areas should only be accessible to authorized personnel to prevent unauthorized access and potential data breaches. Documents should be systematically organized and labeled for easy retrieval and auditing. Each document should include a clear title, date, and any relevant reference numbers, ensuring quick and accurate identification when needed.

6.2. Secure Servers, Access Control, and Backup Systems

Electronic documents need to be stored on secure servers with robust encryption and access controls. Regularly updating these servers with the latest security patches helps protect against cyber threats. Implement multi-factor authentication (MFA) to add an extra layer of security for accessing electronic records. Restricting access to authorized personnel and regularly reviewing permissions helps maintain data integrity and confidentiality.

6.3. Backup Systems

Regular backups are crucial to prevent data loss. It is recommended to perform the following:

- Regular Backup Schedule: Implement a regular backup schedule to ensure all data is consistently backed up. This could be daily, weekly, or monthly depending on the data's importance and frequency of updates.
- Encryption: Ensure that all backup data is encrypted to prevent unauthorized access.
- Backup Testing: Regularly test backups to ensure that data can be successfully restored. This helps verify the integrity and reliability of the backup process.

6.4. Passwords

Passwords of staff should be changed each 3 months. Passwords must be a minimum of 12 characters and include a combination of uppercase letters, lowercase letters, numbers, and special characters (e.g., !, @, #, $, etc.). It is not allowed to reuse any of their last five passwords. Passwords should never be shared or written down. If a password is suspected to be compromised, it must be changed immediately.

6.5. Limiting Access to Sensitive Materials

Authorization: To protect sensitive documents, it is important to establish a clear access authorization protocol. The export control officer should provide an updated list of authorized personnel on a monthly basis to ensure that only authorized individuals have access to information. Authorization protocols should be clearly defined and reviewed regularly to adapt to any changes in personnel or roles.

Monitoring: The export control officer regularly monitors and records access to both paper and electronic documents. This involves keeping detailed records of who accessed documents, when, and for what purpose. Regular auditing of these logs will help to quickly detect any unauthorized access or suspicious activity. With thorough access monitoring, organizations can quickly identify and address potential security breaches, thereby better protecting sensitive information.

7. TRAININGS

Each year export control officer's should set regular training in the theory and practice of export control for all academic personnel involved in international research and collaborations and export control related activates The training is integrated into the personnel training and professional development system of the institution. The aim is to raise awareness and discuss possible issues.

Specialists are trained in the following areas:

- Understanding the fundamental purposes and aims of export control measures.
- Familiarity with the regulatory framework, including relevant laws and regulations impacting academic research and international collaborations.
- Insight into the organizational structure and functions of the ICP within the academic setting.
- Procedures for verifying export transactions in compliance with legal requirements.

Forms and Methods of Training:

- Self-training: Individual study and familiarization with export control materials.
- Group thematic studies: Courses and workshops conducted within departments, involving experienced specialists in export control from both within and outside the institution.
- Conferences and seminars: Participation in national and international conferences and seminars focused on export control and non-proliferation.
- Specialized training abroad: Opportunities for the most experienced export control specialists to receive training at foreign specialized centers and laboratories.
- Current information updates: Regular updates and briefings on the latest developments in export control.

The plan for training specialists is developed by export control officer and approved by the head of the Academia. The export control officer maintains records of training sessions, including dates, topics, and participants.

8. ANONYMOUS REPORTING

In an academic environment, it is critical that all relevant staff and students comply with all export control regulations to ensure the security of confidential information and technology. There may be occasions when a staff member or student becomes aware that someone has intentionally or accidentally violated these rules. To address such situations while protecting the identity of the person reporting, anonymous reporting mechanisms must exist. This section explains the process and importance of anonymous reporting.

Anonymous reporting offers several benefits. It encourages people to report abuses without fear of retaliation or negative consequences. It also protects the reporter's identity, ensuring that they do not suffer any harm or career setbacks. Ensuring trust between researchers, students, administration, and compliance officials is of paramount importance to the success of research outcomes and export control compliance. Finally, it helps maintain compliance with export control regulations by allowing agencies to quickly resolve and remediate issues.

Here are important considerations for anonymous reporting:

1. **Acknowledgment of Violation**: Employees and students must be aware of activities that violate export control regulations. These may include the unauthorized exchange of controlled technology, data or information; export of goods without the necessary licenses; or any other actions that violate legal requirements.
2. **Reporting Violations via Online Form:** To report any suspected abuses or violations, employees and students are encouraged to use the secure reporting form available on the institution’s website. This form is designed to protect the identity of the reporter while providing a structured and official method for submitting concerns.
3. **Details to Include in the Report:** When completing the online form, it is important to provide as many details as possible to assist with the investigation. Once submitted, the form will be directed to the Export Control Officer, who is responsible for receiving and investigating these reports. The Export Control Officer will ensure the confidentiality of the reporter’s identity throughout the process. The form will prompt you to include:
    a. A clear description of what happened.
    b. Dates and times of the incident.
    c. Persons involved.
    d. Any evidence or documents supporting the report.

4. **Safeguards for Reporters:** There are strict safeguards in place to protect reporters. The identity of the reporter will be kept confidential, and a strict non-retaliation policy is in place to prevent any adverse actions against those who report violations. This means reporters cannot be fired, demoted, or harassed for coming forward. Additionally, support services such as legal advice and counseling are available to help cope with stress or issues arising from the report.
5. **Importance of Anonymous Reporting:** Anonymous reporting through the online form is a vital tool for ensuring compliance with export control regulations. By providing a safe and secure method to report violations, institutions can protect sensitive information and technology. It is critical that all staff and students are aware of these reporting channels and that institutions maintain the highest standards of confidentiality and protection for those who come forward.

9. PENALTIES

Violations of export laws can have major consequences for Academia. They can include criminal charges, fines, asset seizure, and loss of state privileges. Such violations can also damage a university's overall public image, affect its ability to attract funding and partnerships, and interfere with its research and commercial activities. Penalties and fines for export law violations differ from country to country, so it is critical for academia to understand and comply with the rules in each jurisdiction in which they operate.

10. AUDITS

Regular reviews are crucial to ensure that ICP procedures are implemented correctly and adhered to on a set schedule. These reviews are designed to verify that the established procedures are executed accurately and by competent personnel. Specialists conducting these reviews must have a thorough understanding of the export control system to identify any deficiencies or incorrect implementation of the ICP. Importantly, these specialists should not be involved in the university's ongoing export activities (if it is possible).

Reviews must be conducted regularly across all departments of the university. The initial review should take place six months after ICP implementation, followed by annual reviews. The Export Control Officer should develop a plan to address any deficiencies within 20 business days and maintain records of all ICP reviews and corrective measures.

The Export Control Officer is responsible for monitoring compliance within the academic institution, ensuring a consistent and periodic review of the compliance framework. Academic institutions should be committed to fulfilling all export control obligations at all times, and it is essential for each institution to be aware of any potential violations. All employees are responsible for reporting any suspected non-compliance.

Refer to the section on Anonymous Reporting if you suspect a violation has occurred. Any suspected errors or violations regarding the ICP and procedures established within the university for complying with applicable export control regulations, including issues related to export permissions or other export control approvals, must be reported immediately to the Export Control Officer.

11. SANCTIONS

Nowadays, there are many sanctions in the world. Sanctions are rules or penalties put in place by countries or groups of countries to try to change someone's behavior or punish them. Sanctions are a common tool for seeking to influence foreign governments and individuals to change their behaviour. The United Nations Security Council (UNSC) can impose sanctions in response to a threat to international peace and security[4]. They can include stopping trade, freezing assets, banning travel, or restricting financial transactions. The goal of sanctions is usually to encourage better behavior, protect human rights, or enforce international laws. These measures can have a big impact on the country being targeted, affecting its economy and its relationships with other nations. The most common types of sanctions include arms embargoes, trade restrictions, financial sanctions (e.g., asset freezes), travel bans and visa bans. Sanctions and embargoes take precedence over licensing requirements. In addition, there are government-backed lists of "restricted parties" with whom companies, organizations, or individuals are generally prohibited from doing business.

Sanctions are frequently updated to remain effective in an ever-changing global environment. Countries and international organizations, such as the European Union (EU) and the United Nations (UN), regularly review and adjust their export controls to bring them in line with international standards and respond to emerging threats. These updates are driven by changes in geopolitics, technological advances, and evolving security risks to ensure that sanctions are relevant and able to meet new challenges.

The process varies by jurisdiction, but generally involves stakeholder coordination, expert involvement, and international cooperation. Regular updates also ensure compliance with global treaties such as the Arms Trade Treaty (ATT) and the Treaty on the Non-Proliferation of Nuclear Weapons (NPT), harmonizing national rules with international obligations.

[4] The Security Council can take action to maintain or restore international peace and security under Chapter VII of the United Nations Charter. Sanctions measures, under Article 41, encompass a broad range of enforcement options that do not involve the use of armed force. Since 1966, the Security Council has established 31 sanctions regimes, in Southern Rhodesia, South Africa, the Former Yugoslavia (2), Haiti (2), Angola, Liberia (3), Eritrea/Ethiopia, Rwanda, Sierra Leone, Côte d'Ivoire, Iran, Somalia/Eritrea, ISIL (Da'esh) and Al-Qaida, Iraq (2), Democratic Republic of the Congo, Sudan, Lebanon, Democratic People's Republic of Korea, Libya (2), the Taliban, Guinea-Bissau, Central African Republic, Yemen, South Sudan and Mali.
https://main.un.org/securitycouncil/en/sanctions/information

Thus, frequent updating of sanctions is critical to maintaining their effectiveness in enhancing global security, responding to new risks, and enforcing international laws. Such adaptability is key to ensuring international stability and preventing the escalation of conflicts.

11.1. Resources for Sanctions

These resources are essential for staying compliant with international regulations and for ensuring that your activities do not inadvertently violate any restrictions.

1. EU Sanctions Map - https://www.sanctionsmap.eu/#/main

   The EU Sanctions Map is an interactive tool that allows users to explore the sanctions imposed by the European Union. It provides a comprehensive overview of restrictive measures, including trade restrictions, financial sanctions, and travel bans, applied against countries, entities, and individuals.

2. UK Sanctions Regimes - https://www.gov.uk/government/collections/uk-sanctions-regimes-under-the-sanctions-act

   This resource offers detailed information about the sanctions regimes implemented by the United Kingdom under the Sanctions and Anti-Money Laundering Act 2018. It covers a variety of sanctions, including financial restrictions, trade measures, and immigration-related penalties, targeting specific countries and entities.

3. Russia Sanctions Dashboard (by Castellum) - https://www.castellum.ai/russia-sanctions-dashboard

   The Russia Sanctions Dashboard offers real-time data and insights on sanctions imposed on Russia in response to its military aggression against Ukraine. The dashboard consolidates sanctions from various jurisdictions, providing a comprehensive overview of the global reaction to the conflict.

4. EU Sanctions Following Russia's Aggression Against Ukraine - https://finance.ec.europa.eu/eu-and-world/sanctions-restrictive-measures/sanctions-adopted-following-russias-military-aggression-against-ukraine_en

   The European Commission's website outlines the sanctions implemented by the EU in response to Russia's military aggression against Ukraine. It offers comprehensive information on restrictive measures, including trade embargoes, financial sanctions, and individual listings.

5. Sanctions Explorer by C4ADS - https://sanctionsexplorer.org/

   Sanctions Explorer by C4ADS is a comprehensive database that consolidates all major sanctions imposed by the EU, UN, US, and other global entities. It serves as a vital tool for tracking and understanding the wide array of international sanctions, providing insights into their scope and enforcement.

11.2. Employee Compliance Obligations

If an employee or other research participant learns that the research or scholarly activity involves sanctions zones, he or she should immediately notify the Export Control Officer. The following additional actions should be taken by the appropriate parties:

Researchers:

- Upon discovering a link to sanctioned areas, researchers should immediately report the link to the Export Control Officer.
- Researchers must immediately cease any collaboration, partnership, or activity related to the sanctioned areas until further notice.
- Researchers should secure relevant data, materials, and communications to prevent unauthorized access or dissemination.

Administration:

- The Administration should immediately inform the appropriate departments and individuals of the problem and the steps being taken to address it.
- The Administration should initiate a review of all current and proposed research agreements and partnerships to ensure that they comply with export control regulations and are not associated with sanctions zones.
- The Administration should provide guidance and support to researchers in terminating and managing the situation to ensure compliance with legal and institutional regulations.

Export Control Officer:

- The Export Control Officer should conduct a thorough review of the research or activity to assess the extent of involvement with sanctioned areas and entities.
- The Export Control Officer should gather all necessary information and documentation from the researchers involved to ensure a comprehensive understanding of the situation.
- The Export Control Officer should offer clear guidance to the researchers and administration on the steps that need to be taken to ensure compliance, including the possibility of terminating the research or seeking a license or exemption, if applicable.
- The Export Control Officer should continuously monitor the situation and provide regular updates to university leadership and relevant stakeholders, ensuring all actions align with legal obligations and institutional policies.

- The Export Control Officer should promptly communicate with relevant government agencies to report the situation and seek guidance on necessary actions.

REFERENCES

[1] European Commission Recommendation (EU) 2021/170. https://op.europa.eu/en/publication-detail/-/publication/a5b08317-1c07-11ec-b4fe-01aa75ed71a1#:~:text=0-,Commission%20Recommendation%20(EU)%202021%2F1700%20of%2015%20September%202021,%2C%20brokering%2C%20technical%20assistance%2C%20transit

[2] United Nations (UN) Security Council - Resolution 1540 (2004). https://www.un.org.

[3] Regulation (EU) 2021/821. https://eur-lex.europa.eu/eli/reg/2021/821/oj

[4] Recommendation (EU) 2019/1318 of July 30, 2019. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019H1318

[5] RA Government Decree No.1785-N dated December 15, 2011. https://www.arlis.am/DocumentView.aspx?DocID=157865

[6] Decision No. 808-N dated May 25, 2023. https://www.arlis.am/DocumentView.aspx?DocID=190787

[7] Federal Office for Economic Affairs and Export Control (BAFA) - "Guidelines for Internal Compliance Programs (ICP) for Export Control." Available at: https://www.bafa.de.

[8] U.S. Department of Commerce, Bureau of Industry and Security (BIS) - "Export Compliance Guidelines: The Elements of an Effective Compliance Program." https://www.bis.doc.gov/index.php/documents/pdfs/1641-ecp/file

APPENDIX A. TECHNOLOGY CONTROL PLAN (TCP)

A Technology Control Plan (TCP) is crucial for:

1. **Legal Compliance**: Ensuring adherence to export control laws and avoiding penalties.
2. **Protection**: Safeguarding sensitive technologies and intellectual property from unauthorized access.
3. **International Collaboration**: Managing the secure and legal exchange of controlled information with global partners.
4. **Risk Management**: Mitigating the risks of security breaches and protecting the organization from liability.
5. **Awareness and Training**: Educating employees about compliance responsibilities and protocols.
6. **Ethical Standards**: Upholding the institution's integrity and ethical standards in research and technology handling.

Below you can find the TCP example for the university (not real data)

A.1. Organizational Unit

Responsible Individual:

- **Principal:** Dr. Anahit Manukyan, Department of Physics, Division 3, Ext. 1123, amanukyan@university.am
- **Alternate:** Prof. Vahan Avetisyan, Department of Physics, Division 3, Ext. 1145, vavetisyan@university.am

A.2. Scope of Activities or Locations

A.2.1. Project-Based Activities:

This TCP covers all research projects involving export-controlled technology and technical data within the Department of Physics. These projects include research on advanced materials, nanotechnology, and computational physics.

A.2.2. Location-Based Activities:

The TCP applies to all facilities within the university campus, specifically:

- Physics Building, Rooms 301-305 (Laboratories and Offices)
- Data Center, Room 210 (Data Storage and Management)
- Clean Room Facility, Room 105 (Sensitive Equipment and Materials)

A.3. Effective Date

August 1, 2024

A.4. Source of Funding

Funding sources for activities covered by this TCP include:

- Government research grants from the Armenian National Science and Education Fund (ANSEF)
- International collaborative grants from the European Union's Horizon Europe program
- Private sector partnerships and sponsorships

A.5. Applicable Agreements

Applicable agreements include:

- Memorandum of Understanding with the Armenian Ministry of Science and Education, outlining compliance with national export control laws.
- Collaborative research agreements with international partners, which include specific clauses on the handling and transfer of export-controlled technology.
- Non-disclosure agreements (NDAs) with private sector partners.

A.6. Technical Description

A.6.1. Controlled Items and Technologies:

The export-controlled items include advanced simulation software, specialized laboratory equipment, and detailed technical data on the properties of nanomaterials. These technologies are critical for research in cutting-edge physics fields.

A.6.2. Export Control Jurisdiction and Classification:

The controlled items and technologies fall under the jurisdiction of the Armenian Ministry of Foreign Affairs, classified according to the Republic of Armenia's export control lists. The items are classified under categories related to dual-use goods and advanced technology.

A.6.3. Controls and Licensing Requirements:

All export-controlled items and technologies require an export license from the Armenian Ministry of Economy for any transfer to foreign nationals or entities. Specific exemptions may apply under collaborative research agreements, which are reviewed on a case-by-case basis.

A.7. Physical Security Plan

A.7.1. Location:

- Physics Building, Room 301: High-security lab for sensitive materials.
- Data Center, Room 210: Centralized data storage with controlled access.
- Clean Room Facility, Room 105: Restricted access area for handling sensitive equipment.

A.7.2. Security Measures:

- All labs and facilities are secured with electronic access controls, requiring a key card for entry.
- Access is limited to authorized personnel, and visitor access is strictly monitored and documented.
- Security cameras are installed in key areas to monitor access and activities.

A.7.3. Perimeter Security:

- The campus perimeter is secured with fencing and monitored by security personnel.
- Entry points are controlled and monitored 24/7 by security staff.
- Additional security measures, such as biometric scanners, are in place for high-security areas.

A.8. Information Security Plan

A.8.1. System Setup:

- The university's IT infrastructure includes secure servers and networks for storing and transmitting controlled information.
- The system setup includes firewalls, intrusion detection systems, and encrypted communication channels.

A.8.2. Security Measures:

- Password protection and multi-factor authentication are mandatory for all systems accessing controlled information.
- Data encryption is used for all sensitive information, both in storage and transmission.
- Secure communication protocols, such as VPNs, are employed for remote access.

A.8.3. Access Management:

- Access to controlled information is restricted to authorized personnel only. Authorization is granted based on project involvement and security clearance levels.
- Access rights are reviewed regularly and revoked immediately upon termination of employment or project completion.

A.8.4. Restricted Communications:

- Discussions involving export-controlled information are held in secure areas, and all participants must be authorized.
- Communication with external parties is conducted under strict guidelines, ensuring compliance with NDAs and export control regulations.

A.9. Item Security Plan

A.9.1. Item Marking:

- All tangible items, including equipment and documents, are clearly marked with export control labels indicating their status.

A.9.2. Item Storage:

- Sensitive items are stored in locked cabinets or secure rooms with restricted access.
- Both digital and physical data, including lab notebooks and reports, are securely stored and managed.

A.10. Training Plan

- All personnel involved in projects covered by the TCP undergo mandatory training on export control laws, data protection, and security protocols. Training sessions are conducted annually and as needed based on regulatory updates or project requirements.

A.11. Recordkeeping Requirements

- The university maintains comprehensive records of all export-controlled items and activities, including licensing documentation, training records, and access logs. Records are retained for a minimum of five years or as required by applicable laws and agreements.

APPENDIX B. EXPORT CONTROL COMPLIANCE ASSESSMENT

B.1. Introduction

The Export Control Compliance Assessment is a fundamental component of the Internal Compliance Program (ICP) at academic institutions. This assessment ensures that all research, technological developments, and international collaborations comply with applicable export control laws and regulations. It specifically addresses dual-use items, which are technologies and goods that can be used for both civilian and military purposes. The goal is to prevent unauthorized access, transfer, or use of such items, thereby safeguarding national and international security interests.

B.2. Scope

The scope of this compliance assessment covers all academic departments, research centers, and laboratories. It includes faculty, researchers, administrative staff, and students involved in activities related to dual-use items. The assessment also applies to all collaborative efforts, including partnerships with foreign entities, visiting scholars, and joint research projects.

B.3. Decision making process