

MEMORANDUM CIRCULAR NO. 22-17
Series of 2022

SUBJECT : GUIDELINES ON TECHNOLOGY CONTROL PLAN (TCP)

WHEREAS, pursuant to Section 8 of Republic Act No. 10697, otherwise known as the Strategic Trade Management Act (STMA), the Strategic Trade Management Office (STMO) is created as a bureau under the administrative supervision of the Department of Trade and Industry (DTI) to serve as the executive and technical agency of the national government for the establishment of the management systems for the trade in strategic goods;

WHEREAS, Section 9 (g) of the STMA provides that the STMO has the power and function to ensure and operate end-use/end-user controls and establish compliance checks and exercise authority to enter premises for such purposes.

WHEREAS, under Rule IV, Section 1 of the STMA Implementing Rules and Regulations (STMA-IRR), the STMO may require, among others, the establishment of an Internal Compliance Program (ICP) as a precondition for the issuance of a global authorization.

WHEREAS, under Rule IV, Section 2 of the STMA IRR provides that the STMO may require a Technology Control Plan (TCP) for applicants of export, re-export, transit and/or import authorizations, (a) Technology Control Plan, in case of technology transfer and (b) Network Security Plan, in case of intangible software transmission.

WHEREAS, under Rule I, Section 4(m) of the STMA-IRR defines Internal Compliance Program (ICP) as an effective, appropriate, and proportionate means and procedures, including the development, implementation, and adherence to standardized operational compliance policies, procedures, standards of conduct, and safeguards, developed by exporters to ensure compliance with the provisions and with the terms and conditions of authorizations set out in the STMA.

NOW, THEREFORE, this Circular is hereby issued for the information, guidance, and compliance of STMO and all covered persons.

1. SCOPE

1.1. Covered persons. The following covered persons shall establish a Technology Control Plan (TCP):

- a. Applicants or Holders of Individual or Global Authorization involving Tangible and Intangible Transfers of Technology;
- b. Applicants or Holders of Governmental End-Use Assurance involving Tangible and Intangible Transfers of Technology; and,

STRATEGIC TRADE MANAGEMENT OFFICE

c. Other persons as determined by the STMO.

1.2. Personnel Responsible for Technology Control Plan Compliance. The Chief Strategic Trade Compliance Officer (CSTCO) or equivalent, depending on the covered person's structure and/or set-up, shall implement effective systems and procedures to ensure the security, integrity, and effectivity of this Circular, and shall serve as the focal person in all matters relating thereof.

1.3. Tangible and Intangible Transfers of Technology. Transfer of software or technology may occur through any of the following activities:

- a. Forms of tangible transfers of technology (e.g. USB, hard drives, laptops, and tablets, physical shipment of hard copy materials).
- b. Forms of intangible transfers of technology (e.g. phone, video call, and email, electronic mail and facsimiles, cloud storage or routing, cloud computing, downloads, access to files on network servers or shared drives).
- c. Technology transfers within multinational companies that share common IT systems.
- d. Accessing or downloading controlled technology overseas, employee access to a company intranet when overseas, third party access overseas to intranets or cloud services, third party help desk and administration services, and IT system testing and maintenance.
- e. Procurement, training, maintenance services or direct technical support of R&D, manufacturing and assembly.

2. TECHNOLOGY CONTROL PLAN COMPLIANCE. A Technology Control Plan (TCP) is a system designed to prevent unauthorized access, transmission or sharing of sensitive and controlled items, materials, information, software or technology.

The TCP document shall contain the following elements:

2.1. Physical Security Plan. This refers to security measures taken to prevent unauthorized personnel from observing or having access to the premises/facilities wherein the research, development, production, use, and storage of strategic goods, information, software or technology are being processed and made. The covered person shall comply with the following applicable requirements:

- a. The covered person may have facility control systems in place such as:
 - i. Automatic (electro-mechanical) doors controlled by access badges with corresponding access level permission.
 - ii. Biometric sensors or system to record timestamps of personnel entering and going out in the facility.
 - iii. Secured desks, working bays or workstation where computers are being used and operated.
 - iv. Secured storage rooms, cabinets, etc.
 - v. Security personnel deployed on and within the facility 24/7.

- vi. Mounted cameras such as CCTV to monitor the interior and exterior view of the facility.
 - vii. Other systems than can be utilized by the covered person to ensure physical security against unauthorized access.
- b. The covered person shall have a system, software or technology in place to trail entries and exits in the facility, and the same shall be reviewed regularly;
 - c. The covered person shall have non-disclosure agreements in place in the event that third-party support is required;
 - d. The facility shall be reasonable and appropriate for the conduct of research, development, production, use, and storage of strategic goods, information, software or technology;
 - e. Devices being used in the facility shall be dedicated only for the research, development, production, use, and storage of strategic goods, information, software or technology;
 - f. The facility shall have an schematic plan indicating and describing the perimeter security controls, working bays, entry and exit point/s of the facility, and storage areas;
 - g. The covered person shall provide policies and action plans against noticeable threats, vulnerabilities, hazards on the facility;
 - h. Visitor management policy for persons who will enter in the premises for the purpose of visits, audits, etc.; and,
 - i. Other security controls available and appropriate to comply with the requirement specified in this Section.

2.2. Network Security Plan. This refers to security measures and policies that are taken to prevent unauthorized personnel from observing or having access to electronic data or electronic data carriers containing controlled information/ data/ software and technology. The covered person shall comply with the following applicable requirements:

- a. The covered person shall implement a system, software, or technology to deploy a dedicated and secured channel for the intangible transfer or transmission of controlled information, software or technology and/ or relevant data;
- b. Network protection layers such as firewall to monitor incoming and outgoing network traffic and decide whether to allow or block specific traffic to prevent unauthorized intangible access and cyber-attacks;
- c. The system or software shall have a diagnostic tool for archiving policy, data loss and theft, and identify specific viruses, malware attacks, security gaps and system bugs;

- d. The system or software shall have an audit trail feature to locate all the digital footprints and transactions being done in the system;
- e. To establish continuity, a Network Disaster Recovery Plan should be in place in case of internal and/or external network interruptions; and,
- f. Other security controls available and appropriate to comply with the requirement specified in this Section.

2.3. Information Security Plan. This refers to security measures and policies that are taken to protect the controlled and uncontrolled information, software, or technology. The covered person shall comply with the following applicable requirements:

- a. Procedures for marking, labeling, and classifying of uncontrolled and controlled equipment, devices, information, software or technology;
- b. The system or software shall feature User IDs and levels, password control, encryption and decryption function, firewalls, and registering of IP Addresses to prevent the unauthorized access against rogue devices and unregistered IPs prior, during, and after the transfer of controlled technology or information;
- c. The system or software can be managed by a VPN, VLAN, or the like to allow authorized persons to safely access and transmit data using the internet and local network. Visitors or third-party personnel who need internet access during their visit in the facility shall be connected to a separate or guest network;
- d. Reliable system for securing both hard and soft copies of data containing or associated to the controlled information, software or technology;
- e. Should the controlled information, software or technology will be discussed or shared on an event to any personnel or third party entities, i.e. power point presentations, orientations, seminars personal demonstration, e-mail, telephone, fax, or means that contain the such, security controls shall be made such as pre-checking the personalities, attendees and participants involved, signing of confidentiality agreement to avoid inadvertent and exports/disclosures. The CSTCO shall decide whether to allow, limit or prohibit such presentation or information sharing; and,
- f. Other security controls available and appropriate to comply with the requirement specified in this Section.

2.3.1. Repository of intangible records. A secure records management system for blueprints, design files, schematics and diagrams shall be in place and can only be accessed by the company's authorized personnel.

2.4. Project Personnel Requirement. This refers to security measures and policies that should be followed by personnel involved in the research, development, production, and storage of strategic goods, information, software or technology. The covered person shall comply with the following applicable requirements:

- a. List of all persons who are determined to have authorized access in the research, development, production, and storage of strategic goods, information software or technology;
- b. Proofs of employment (i.e. employment contracts) stating the designation and defining the duties and responsibilities, length of service of the listed personnel;
- c. Personnel involved shall agree with the technology transfer agreement or non-disclosure conditions for strategic goods, information or software or technology;
- d. Programs/ training to regularly update and inform the listed personnel should there be any changes, update, modification made in the security controls or systems;
- e. Procedures on termination and job transfer for the personnel involved (i.e. briefing regarding continued protection of classified and unclassified export controlled information, penalties, and termination certification with regard to obligation to STMA.); and,
- f. Other security controls available and appropriate to comply with the requirement specified in this Section.

2.5. Foreign Person Participation. This refers to security measures that are taken to properly evaluate, screen, and select the foreign personnel who will be involved in the activities on research, development, production, and storage of strategic goods, information, software or technology. The covered person shall comply with the following applicable requirements:


- a. Effective procedures in place to perform pre-employment and regular screening/verification such as background checks, work history, personal, academic and liability background of local and foreign applicants, third-party supports, and can preclude employment in any capacity, and reasonable accommodation to perform an essential function, that conflicts the job requirement;
- b. The above procedures shall use repositories of the Philippine Government and entity lists issued by the International Authorities and Conventions, and shall follow and in compliance with the applicable national and foreign laws; and,
- c. Other controls available and appropriate to comply with the requirement specified in this Section.

3. OTHER PROVISIONS


- 3.1. Assistance for Companies.** The STMO shall guide the covered persons in establishing the measures, conditions, or requirements provided in this Circular, and are hereby advised to contact the STMO Policy and Enterprise Relations Division (PERD) through stmoinfo@dti.gov.ph.

This Circular shall take effect immediately.
20 July 2022, Makati City.

Recommending Approval:


ATTY. ALEXANDER B. SANTOS
Atty. V, Investigation and Compliance Division, STMO

Approved by:


ATTY. JANICE SACEDON DIMAYACYAC
OIC-Director, STMO