TECHNOLOGY CONTROL PLAN

1.0 SCOPE OF APPLICABILITY

1.1 All [implementing company name] business units and their associated facilities and operating locations (sites) are required to comply with and implement this Technology Control Plan (TCP).

1.2 All [implementing company name] employees, as well as long-term visitors (on site for 3 weeks or longer), temporary employees, agency employees, subcontractors, consultants, and vendors operating within [insert implementing company] sites are responsible for reading this TCP and ensuring it is understood and implemented in accordance with the procedures and requirements set forth below.

1.3 Failure to comply with this TCP and the procedures prescribed herein may result in severe disciplinary measures, up to and including termination of employment.

2.0 PURPOSE

2.1 The purpose of this TCP is as follows:

2.1.1 To define the administrative controls and procedures that will be implemented at [implementing company name] and its sites located worldwide, and to ensure proper control of classified material and Controlled Unclassified Information (CUI), pursuant to the existing export authorizations under and U.S. laws and regulations.

2.1.2 To prescribe security measures to prevent access by non-authorized personnel.

2.1.3 To establish measures to ensure that any access to classified material by non-Italian citizens or Controlled Unclassified Information by Foreign Persons is authorized under U.S. law, including by licenses or other approvals, as applicable.

2.1.4 To ensure compliance with the International Traffic in Arms Regulations (ITAR), the Export Administration Regulations (EAR) or, as necessary, the U.S. National Industrial Security Program (NISP).

3.0 POLICY

3.1 It is the policy of [implementing company name] to comply with all statutory and regulatory requirements relating to the control and safeguarding of classified materials and CUI.

i

3.2 Neither classified materials nor CUI will be transferred to any individual except as authorized by U.S. law, the NISP, and this TCP.

4.0 BACKGROUND

4.1 [implementing company name] is a supplier of products, technology, services and support to military forces, government agencies and prime contractors worldwide.

4.2 [implementing company name] manufactures and supports a broad range of systems for mission-critical and military sustainment requirements, such as (identify products/systems and services, as applicable)

4.3 [implementing company name] customers include U.S. government agencies, such as the Department of Defense, as well as Italian and other European Ministry of Defense customers.

5.0 REFERENCES

5.1 Export Administration Regulations (EAR), 15 C.F.R. §§730-774

5.2 International Traffic in Arms Regulations (ITAR), 22 C.F.R. §§120-130

5.3 National Industrial Security Program Operating Manual (NISPOM), DoD 5220.22-M

6.0 DEFINITIONS

6.1 "Classified Material" (NISPOM, Appendix C)

6.1.1 Official information or materials that have been determined, pursuant to Executive Order 12958, "Classified National Security Information" (April 17, 1995), or any predecessor or subsequent order, to require protection against unauthorized disclosure in the interest of national security and which has been so designated.

6.1.2 The term includes National Security Information (NSI), Restricted Data (RD) and Formerly Restricted Data (FRD).

6.2 "Controlled Unclassified Information" (CUI)

6.2.1 CUI includes unclassified yet sensitive information to which access or distribution limitations have been applied in accordance with national laws, policies, regulations, or U.S. government customer requirements.

6.2.2 Examples of CUI include any information marked as such from U.S. government customers, information determined to be exempt from public disclosure and Export-Controlled Information.

6.3 "Defense Articles" (ITAR, 22 C.F.R. §120.7)

6.3.1 All items identified on the U.S. Munitions List (USML), 22 C.F.R. §121.1.

6.4 "Defense Services" (ITAR, 22, C.F.R. §120.9)

6.4.1 The furnishing of assistance (including training) to Foreign Persons, whether in the U.S. or abroad, in the design, development, engineering, manufacture, production, assembly, testing, repair, maintenance, modification, operation, demilitarization, destruction, processing, or use of Defense Articles.

6.4.2 The furnishing to Foreign Persons of any Technical Data, whether in the United States or abroad.

6.5 "Export-Controlled Information"

6.5.1 "Technical Data" (ITAR, 22 C.F.R. §120.10)

6.5.1.1 Information, which is required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance, or modification of defense articles to include information in the form of blueprints, drawings, photographs, plans, instructions, and documentation;

6.5.1.2 Classified information relating to Defense Articles and Defense Services;

6.5.1.3 Information covered by an invention secrecy order; and

6.5.1.4 Software directly related to Defense Articles.

6.5.2 "Technology" (EAR, 15 C.F.R. §772)

6.5.2.1 Specific information necessary for the development, production or use of a product;

6.5.2.2 "Technical assistance," such as instruction, skills training, working knowledge, and consulting services;

6.5.2.3 Includes blueprints, plans, diagrams, models, formulae, tables, engineering designs and specifications, manuals, and instructions.

6.6 "Foreign Person"

6.6.1 Insert definition under Italian law

6.6.2 As defined in the ITAR (22 CFR 120.16) and for export matters, a Foreign Person is any natural person who is not a lawful permanent resident of the U.S. or who is not a protected individual (via refugee status or asylum). It also means any corporation, business association, partnership, trust, society or any other entity or group that is not incorporated or organized to do business in the United States, as well as international organizations, foreign governments and any agency or subdivision of foreign governments (e.g., diplomatic missions).

6.6.3 U.S. persons employed by a foreign entity are representatives of a foreign interest (RFI) and, for export control and security purposes, must be treated as a "Foreign Person." NOTE: The term "Foreign Person" does not include, for export control purposes, any U.S. citizen or lawful permanent resident who is employed by an entity, organization or group that is organized to do business in the United States. In particular, U.S. citizens and lawful permanent residents employed by the U.S. subsidiaries and U.S. affiliates of Finmeccanica S.p.A. are not "Foreign Persons" for export control purposes.

6.7 "U.S. Government Disclosure Authorization"

6.7.1 Licenses or written approval from the U.S. Department of State, Directorate of Defense Trade Controls granted pursuant to the ITAR;

6.7.2 Applicable ITAR exemptions;

6.7.3 Licenses or written approval from the U.S. Department of Commerce, Bureau of Industry and Security granted pursuant to the EAR;

6.7.4 Applicable EAR exemptions; and

6.7.5 To authorized persons in accordance with the NISPOM.

6.8 "U.S. Person"

6.8.1 As defined in the ITAR (22 CFR 120.15), a U.S. person is any natural person who is a lawful permanent resident of the U.S. or who is a protected individual (via refugee status or asylum). It also includes any corporation, business association, partnership, trust, society or any other entity or group that is incorporated or organized to do business in the United States.

7.0 RESPONSIBILITIES

7.1 Vice President/General Managers or Site Managers (Site Executives)

7.1.1 Appoint and retain a Security Officer and Technology Control Officer (TCO) responsible for the operational oversight of [implementing company name] compliance with this TCP and the requirements of the ITAR, EAR, and NISP.

7.1.2 Throughout [insert implementing company], demonstrate and communicate a commitment to fully comply with the requirements of this TCP and all U.S. laws and regulations.

7.1.3 Provide the resources required to support the TCP throughout [implementing company name].

7.1.4 Appoint and retain appropriate Trade Management personnel responsible for the operational oversight of each [implementing company name] site's compliance with this TCP and the requirements of the ITAR and EAR.

7.1.5 Oversee the implementation, execution, and monitoring of this TCP, including administering an electronic communication awareness program for personnel within each Site Executive's facility, fostering an environment of support and overseeing strict compliance with the requirements of this TCP.

7.1.6 Provide the resources required to support the site's execution of this TCP.

7.4 Security Officer

7.4.1 Educate and train all new employees as part of their new-hire orientation and all current employees at least annually on the TCP requirements, as applicable.

7.4.2 Maintain all executed statements, acknowledgements, certifications, agreements, visitor logs, and other records associated with the TCP, as applicable, for a period of 5 years past the expiration of any related authorization.

7.4.3 Monitor and conduct periodic reviews of compliance with the TCP, as applicable, as part of daily oversight activities and document the results.

7.4.4 Conduct a complete and thorough investigation into any alleged misuse, unauthorized disclosure, improper handling, safeguarding, or destruction of classified material or CUI

7.5 Site Managers and Supervisors

7.5.1 Ensure neither classified material nor CUI is disclosed, provided or transferred (including, without limitation, shipped, mailed, hand carried, or otherwise transmitted), unless authorization already has been obtained by [implementing company name] from the U.S. government and/or the disclosure, provision or transfer is otherwise in accordance with U.S. government laws and regulations, and the required records are created and maintained.

7.5.2 Ensure classified material and CUI are handled properly, safeguarded, and destroyed in accordance with [implementing company name] policies and procedures, the EAR, the ITAR, the NISPOM, and any other applicable U.S. laws and regulations.

7.5.3 Ensure [implementing company name] employees under their direct supervision execute and return to the Security Officer a signed TCP briefing acknowledgment form indicating they have received a copy of the TCP and were briefed on its contents (Attachment A).

7.5.4 Ensure [implementing company name] employees are aware of what information can and cannot be disclosed to or accessed by Foreign Persons and non-U.S. citizens.

7.5.5 Ensure facility map is included which identifies areas of access (Attachment C).

7.6 Employees

7.6.1 All [implementing company name] employees will receive a copy of the TCP and a briefing from the Security Officer that addresses their responsibilities, as follows:

7.6.1.1 Documents under their control or in their possession containing classified material or CUI will not be released to or accessed by any employee or visitor who is a Foreign Person (or in the case of classified information, a non-U.S. citizen) unless authorization already has been obtained by [implementing company name] from the U.S. government and/or the release or access is otherwise in accordance with U.S. government laws and regulations, and the required records are created and maintained.

7.6.1.2 Foreign Persons (or in the case of classified information non-U.S. citizens) will not be exposed to hardware or activities that reveal classified material or CUI unless

authorization already has been obtained by [implementing company name] from the U.S. government and/or the exposure is otherwise in accordance with U.S. government laws and regulations, and the required records are created and maintained.

7.6.1.3 Defense Services and technical assistance must not be provided to Foreign Persons unless authorization already has been obtained by [implementing company name] from the U.S. government and/or the provision of such Defense Services or technical assistance is otherwise in accordance with U.S. government laws and regulations, and the required records are created and maintained.

7.6.1.4 All classified material and CUI must be marked properly and safeguarded in accordance with U.S. government laws and regulations and [implementing company name] policies and procedures.

7.6.2 All classified material must be disposed of in accordance with U.S. government laws and regulations and [implementing company name] policies and procedures.

7.6.3 All CUI will be destroyed in such a manner as to prevent disclosure of such information to Foreign Persons. At a minimum, cross-cut shredders producing a particulate size no larger than 1/2-inch diameter will be used to destroy CUI prior to discarding through public waste disposal systems. If a third-party vendor is used to destroy technical data, the vendor will be under contractual obligations to ensure only U.S. persons are exposed to the material during the destruction process and that the destruction waste meets the standards of being 1/2-inch or smaller particulate.

7.6.4 While hosting Foreign Persons and/or non-U.S. citizens, [implementing company name] employees will comply fully and take reasonable steps to ensure compliance by others with the requirements of this TCP and Corporate Security Policy SEC-004, "Visitor Control Policy."

8.0 CONTROLS

8.1 The disclosure of classified material to non-U.S. citizens or CUI to Foreign Persons, regardless of whether such disclosure is made within the United States, is considered an export and is subject to authorization, as applicable, by the U.S. government.

8.2 Foreign Persons (or in the case of classified information, non-U.S. citizens) will not be given access to classified material or CUI unless appropriate U.S. Government Disclosure Authorization, as necessary, has been obtained.

8.3 [implementing company name] employees utilizing a U.S. Government Disclosure Authorization to permit the transfer of classified material or CUI to a Foreign Person (or in the case of classified information to a non-U.S. citizen) must receive in advance a security briefing from the cognizant Security Officer for all disclosures authorized pursuant to the NISP and an Export Authority Compliance Plan (EACP) briefing from the Trade Compliance Coordinator for all disclosures of CUI, as appropriate.

8.4 Foreign Persons and non-U.S. citizens employed by, assigned to (extended visit), or visiting [implementing company name] will receive a briefing from the cognizant Security Officer that addresses the following items:

8.4.1 Prior to the release of classified material to a non-U.S. citizen or CUI to a Foreign Person, U.S. government authorization must be obtained by [implementing company name], or the [implementing company name] Trade Compliance Coordinator must validate that no affirmative U.S. government authorization is required.

8.4.2 [implementing company name] security rules, policies and procedures and site personnel regulations.

8.4.3 [implementing company name] policies and procedures for the use of facsimile, automated information systems or reproduction machines. Refer to [implementing company name] Policy #####, "Electronic Communications Plan" for information related to electronic correspondence between [implementing company name] and other companies.

8.4.4 EACP outlining any specific information that has been authorized for release.

8.4.5 Areas in the site where Foreign Person and/or non-U.S. citizen employees or visitors are permitted and restricted.

8.4.6 Classified material to which they are authorized to have access and need to forward to a third party must be submitted to [implementing company name] Security for transmission through government-to-government channels.

8.4.7 Information received at [implementing company name] for a Foreign Person or non-U.S. citizen and information that a Foreign Person or non-U.S. citizen intends to export to a Foreign Person or non-U.S. citizen must be prepared in English.

8.5 The provision of access to and the disclosure of classified material to a non-U.S. citizen or CUI to a Foreign Person employee or visitor must be in compliance with the relevant U.S. Government Disclosure Authorization, as applicable, and the corresponding approved [identify internal visitor control forms and procedure names and numbers].

8.6 Foreign Persons and non-U.S. citizens must enter and exit [[implementing company name] via pre-designated exterior doors, wear their assigned badges at all times and only access areas for which they have been authorized.

8.7 All hand-carried items will be subject at all times to inspection to detect any unauthorized material that may be brought into or attempted to be removed from the [[implementing company name] facility. Unauthorized material may include, but is not limited to, the following: weapons, classified information, CUI, hardware, software or other material as determined by the Security Officer or Trade Compliance Coordinator.

8.8 Foreign Persons and non-U.S. citizens are not permitted to have any recording or photographic equipment (including, but not limited to, such equipment embedded in cell phones) within any [[implementing company name] facility.

8.9 Foreign Person and non-U.S. citizen employees will be accompanied at all times by a U.S. person employee of [[implementing company name], unless the cognizant Security Officer has identified areas of the facility that do not and are not permitted to contain classified material or CUI. Foreign Person and/or non-U.S. citizen employees may be permitted unescorted access in these unrestricted areas during weekday normal business hours after completion of the TCP briefing and execution of the corresponding acknowledgements.

8.10 A detailed record will be created and provided promptly to the cognizant Security Officer for each instance in which a Foreign Person (or in the case of classified information, a non-U.S. citizen) employee or visitor is given access to or otherwise provided with classified material or CUI. Such record will include the following:

8.10.1 The date access or disclosure was provided.

8.10.2 A detailed description of articles or information to which access was granted or disclosure was made.

8.10.3 The export jurisdiction and classification of the article or information.

8.10.4 The Foreign Person (or in the case of classified information, non-U.S. citizen) to whom the access or disclosure was provided, his/her country(ies) of citizenship and birth.

8.10.5 The entity represented by the Foreign Person (or in the case of classified information, non-U.S. citizen) and the entity's country of incorporation.

8.10.6 The authorization (license number/exemption/exception) that permitted the access or disclosure.

8.10.7 A copy of all transferred information and related written communication.

8.11 Foreign Person/Non-U.S. Citizen Visitors

8.11.1 [implementing company name] employees hosting a Foreign Person or non-U.S. citizen must adhere to and complete the requirements as outlined within [implementing company name] "Visitor Control Policy."

8.12 Badging

8.12.1 All [implementing company name] employees and visitors must wear a badge in a prominent location at all times while at any [implementing company name] location. Refer to [implementing company name] Policy, "Visitor Control Policy," or contact your local Security Officer for additional information.

8.12.2 A distinct badge that indicates their status as Foreign Persons or non-U.S. citizens must be worn at all times by all Foreign Person and non-U.S. citizen employees and visitors.

8.13 When necessary, [implementing company name] will establish segregated work areas for Foreign Person and non-U.S. citizen employees or visitors to prevent the inadvertent access to classified material and CUI.

9.0 TCP Non-Disclosure Agreement

9.1 All Foreign Person and non-U.S. citizen employees will be required to sign a TCP Non-Disclosure Agreement (TCP NDA) (Attachment B) prior to the commencement of their employment duties that acknowledges their obligation to control and prevent unauthorized access to classified material and CUI provided to them in the course of their employment with [implementing company name]. TCP NDA's require annual review.

9.2 Any time a Foreign Person visitor will receive access to Technical Data, Technology, Defense Services, technical assistance, or [implementing company name] Proprietary Information, a standard non-disclosure agreement (NDA) is required to be in place. Where an NDA covering the purpose of the visit already has been executed between [implementing company name] and the Foreign Person visitor or their employer, a copy must be provided to the cognizant [implementing company name] Security Officer prior to the date of the visit. When this condition has not been met, the Foreign Person visitor will be required to execute an appropriately completed NDA prior to the commencement of the visit.

9.3 At a minimum, NDAs will be maintained locally throughout the duration of the agreement.

9.4 The original NDA must be retained by the cognizant Contracts Department. The Security Officer will retain their copy of the NDA for a period of 5 years past the date of the visit or the expiration of the authorization that permitted exports to the visitor, whichever date is later.

10.0 OBLIGATION TO STAY CURRENT WITH LAWS AND REGULATIONS

10.1 Laws, regulations, and contractual requirements are subject to change, which may require revision to this policy. In the event of any conflict between this policy and any law, regulation or contractual requirement, the law, regulation or contractual requirement shall prevail. All personnel shall keep themselves current with any such changes and shall comply with such changes, regardless of whether or not the changes have been incorporated into any given version of the policy. Any questions regarding conflicts with this policy shall be addressed to [implementing company name] Security Officer.

10.2 Recommendations for revisions to this policy shall be made to the [implementing company name] Security Officer and Trade Compliance Coordinator.

11.0 OBLIGATION TO REPORT SECURITY VIOLATIONS

11.1 [implementing company name] employee (including any executive or officer of [implementing company name] who witnesses an act involving a potential security violation of either U.S. government security requirements or [implementing company name] security policies shall take reasonable and appropriate measures to stop such activities.

11.2 Any [implementing company name] employee who witnesses an act involving a potential security violation or becomes aware of any violation or potential violation of either U.S. government security requirements or [implementing company name] security policies immediately must report this information to one or more of the following:

11.2.1 Security Officer;

11.2.2 Local management;

11.3 [implementing company name] will take appropriate action against any [implementing company name] employees whose actions are found to violate this policy. Also, disciplinary action may be taken against [implementing company name] employees who knowingly fail to report such violations, or who retaliate against others who lawfully and in good faith report such violations. Discipline may include actions up to and including the termination of employment or of any business agreement or relationship with [implementing company name].

Attachment A

TECHNOLOGY CONTROL PLAN BRIEFING ACKNOWLEDGEMENT

I, _____ (insert individual's name) acknowledge that I have received a copy of the Technology Control Plan (TCP) for _____ (insert name of business) and a briefing outlining the contents of this TCP. I understand the procedures as contained in this TCP and agree to comply with all [implementing company name]. and U.S. government regulations, as those regulations pertain to classified material and Export-Controlled Information.

I certify that I understand my individual responsibility for safeguarding classified material and Export-Controlled Information. I am aware that failure to comply with the terms of this agreement may result in disciplinary action, including termination of my employment or contractual support with [implementing company name] and/or possible prosecution by the U. S. government.

_____	_____
Print Name of Individual	Print Name of Company Briefing Official
_____	_____
Signature of Individual	Signature of Company Briefing Official
_____	_____
Date	Date

Attachment B

TCP NON-DISCLOSURE AGREEMENT

I, [**name of foreign person**], acknowledge and understand that any export controlled information related to a Defense Article covered by the U.S. Munitions List to which I have access per authorization by the U.S. Department of State [**state relevant export license number/exemption**] and disclosed to me during [**my employment by or visit to**] [**name of company**] is subject to the export controls of the International Traffic in Arms Regulations (ITAR) (22 C.F.R. §§120-130).

I, [name of foreign person], also acknowledge and understand that any Export Controlled Information covered by the Commerce Control List to which I have access per authorization by the U.S. Department of Commerce [state relevant export license number/exception] and disclosed to me during [my employment by or visit to] [name of U.S. company] is subject to the export controls of the Export Administration Regulations (EAR) (15 C.F.R. §§730-774).

I also acknowledge and agree that, should I receive classified material or export-controlled information or articles for which I have not been granted access authorization, I immediately will report the incident in writing to the [implementing company name] Security Officer.

In furtherance of the above, I hereby certify that all articles, including export controlled information, to which I have access will not be used for any purpose other than that authorized by the U.S. government and will not be further exported, transferred, disclosed via any means (e.g., oral disclosure, visual access, facsimile message, telephone), whether in their original form, modified or incorporated in any other form, to any other Foreign Person or any foreign country, except as authorized by the prior written approval of the [implementing company name] export compliance official and the U.S. government and applicable law.

_____
Print name

_____
Signature

_____
Date

Attachment C

TCP FACILITY OUTLINE & MAP – AREAS OF ACCESS

Note: The areas of access should be identified by embedding a map of facility to which a Foreign Person will have access and then identifying the sensitive areas to which the same Foreign Person will not have access.

Include a map key to identify:
1) Common areas (i.e. hallways, cafeterias, break facilities, toilets, etc);
2) Foreign Person access area;
3) Areas containing classified or controlled technology, etc.

The following is an example of the key.