Avanco International, Inc.
www.avanco.com
International.Programs@avanco.com

TECHNOLOGY CONTROL PLAN

Background:

A. The requirements for the Technology Control Plan (TCP) are set forth in Sections 10-509 and 2-307 of the National Industrial Security Program Operating Manual (NISPOM) and Part 126.13 of the International Traffic in Arms Regulations (ITAR). The original purpose for the TCP was to require cleared contractor facilities to develop specific access and physical control measures to control access to classified information and programs by foreign national employees and visitors similar to the procedures required for DoD Components in DoD Directive 5230.20. This requirement is described in Section 10-509 of the NISPOM. In an attempt to remind cleared contractors of the requirement and expedite decisions on export license applications related to the hiring of foreign nationals and long-term plant visits by foreign nationals, the requirement specified in the NISPOM was included in Part 126.13 of the ITAR. With respect to this requirement for the TCP, the Defense Security Service (DSS) may grant an exception regarding the preparation of a specific "TCP" if the facility has in place other security documentation (such as a Standard Practices Procedures (SPP) document) that adequately covers the specific components of a TCP.

B. Section 2-307 of the NISPOM requires a TCP in all situations when facilities are cleared under certain Foreign Ownership, Control or Influence (FOCI) arrangements. In such cases, it is presumed that there is a significant risk of unauthorized or inadvertent access by foreign nationals because of the FOCI circumstances. Therefore, a specific TCP is mandatory even though the facility may have in place a SPP or other similar security document that implements the NISPOM. When a SPP or other security document adequately covers controls for classified information and programs, the TCP may be limited to unclassified export controlled information, including that related to dual-use items controlled by the Export Administration Regulation. However, the documents should cross-reference each other.

Preparation Guidance:

A. The purpose of a TCP is to describe specific procedures covering HOW access to classified and controlled unclassified information and other export controlled information will be controlled in circumstances when foreign nationals are located at security cleared contractor facilities as visitors or employees or there is a FOCI situation. The TCP must cover the requirements of export control laws and regulations, the NISPOM, classified contracts and, in the case of a FOCI situation, the provisions of the facility clearance arrangement. Even though foreign

nationals who are "protected individuals" may be given access to unclassified export controlled information pursuant to the ITAR and Export Administration Regulation (EAR), the TCP must still address such persons since they are not eligible for access to classified information (except in limited circumstances pursuant to a Limited Access Authorization (LAA) which has been approved pursuant to DoD 5200.2-R and the NISPOM). In such cases, access under the LAA will be restricted to specified classified information and limited to a specified government program or project; therefore, access to other information must be controlled. Their access to certain controlled unclassified information (e.g., privacy information, another company's proprietary information) also is restricted unless the consent of the person (for privacy information) or originator is obtained.

B. It is not necessary or desirable to repeat the requirements that are stated in the NISPOM or the export control regulations except where necessary to emphasize a particular requirement. The facility security and export control officials must be thoroughly familiar with the specific security and export control requirements, and it is they, in the first instance, who are responsible for monitoring enforcement.

C. It is not necessary to prepare a TCP for each foreign national visitor or employee. Access authorizations and restrictions for individual situations can be prepared and appended to a single, generic TCP (or SPP).

D. Even if a facility's internal security procedures documentation (e.g., SPP)) might fully cover the requirements that are to be addressed in a TCP, and DSS determines that a separate TCP is not necessary, it would be preferable that the TCP requirements be included in a separate annex to the SPP or other document so that the guidance can be removed, merged with guidelines on information access authorizations and restrictions, and provided to the foreign national visitor or employee and co-workers. This also will facilitate compliance with the ITAR provision dealing with the submission of a copy of the TCP with requests for licenses for foreign national visitors and employees by cleared companies.

E. The TCP guidance and the information access authorizations and restrictions must be provided to each foreign national visitor or employee, as well as co-workers, and they must acknowledge their receipt and understanding of the requirements.

TCP Content:

See attached recommended Prototype.

Avanco International, Inc.
www.avanco.com
International.Programs@avanco.com

TECHNOLOGY CONTROL PLAN
(Prototype)

1. PURPOSE. The purpose of this Technology Control Plan (TCP) is to prescribe the access controls and protective security measures necessary to preclude unauthorized access by foreign national visitors and employees to classified information and controlled unclassified information and other unclassified export controlled information that are furnished to or generated by [insert name of company] or its employees. This TCP implements the requirements of Section 10-509 of the National Industrial Security Program Operating Manual (NISPOM) and Part 126.13 of the International Traffic in Arms Regulations (ITAR) (22 CFR 120-130). (**GUIDANCE:** If the company is cleared under a FOCI arrangement, add: "This TCP also satisfies the requirement of Section 2-307 of the NISPOM with regard to companies cleared under a (identify the FOCI arrangement)." The pertinent requirements of the FOCI arrangement may be summarized)

2. APPLICABILITY. This TCP is applicable to all officers, directors and employees of the Company, including part-time and temporary employees. It shall be made binding on subcontractors, consultants, advisors, agents and other such representatives of the Company through contract provisions.

3. DEFINITIONS.

a. Alien. Any person who is not a citizen or national of the United States (8 U.S.C. 1101). (See also "Foreign National", below).

b. Defense Article. Any item or related technical data designated as a defense article in Part 121 of the International Traffic in Arms Regulations (ITAR)

c. Controlled Unclassified Information (CUI). For the purpose of this TCP, unclassified information to which access or distribution controls are applied in accordance with national laws and regulations. For the United States, CUI is unclassified information that is exempt from public disclosure under the provisions of the Freedom of Information Act. When used in connection with government contracts, the contracting agency must mark the information when it is provided to the contractor, and include in the contract instructions to the contractor for identifying and marking such information that may be generated under the contract.

d. Export. For the purpose of this TCP, sending or taking export controlled articles outside the United States or the transfer or disclosure of export controlled articles

or technical data to a foreign person by any means, whether in the United States or abroad (22 CFR 120.17).

e. Export Controlled Information. For the purposes of this TCP, any knowledge that is subject to export controls pursuant to the International Traffic in Arms Regulations or the Export Administration Regulations.

f. Foreign National. Any person who is not a citizen or national of the United States (8 U.S.C. 1101).

g. Foreign Person. For the purpose of this TCP, a foreign person is any natural person who is not a protected individual as defined in 8 U.S.C. 1324b. A Foreign Person also is any corporation, business association, partnership, society, trust, or any other entity, organization, or group that is not incorporated or organized to do business in the United States; and any international organization or a foreign government, and any agency or subdivision of a foreign government, as defined in 22 CFR 120.16.

h. Lawfully Admitted for Permanent Residence. The status of having been lawfully accorded the privilege of residing permanently in the United States as an immigrant, in accordance with the immigration laws, such status not having changed (8 U.S.C. 1101). (**Note:** i.e., "green card holder". Aliens temporarily in the United States with work visas and other foreign nationals who in the United States for temporary purposes, such as students, researchers, military personnel, etc., do not qualify. Pursuant to 8 U.S.C., individuals generally lose their protected individual status, if: (1) after residing in the United States for at least five years, they have not applied for naturalization within six months of their eligibility or (2) they have applied for naturalization, but have not been naturalized within two years of their application. The requirement to declare "intending citizen" status upon entry no longer exists.)

i. Person. A natural person as well as a corporation, business association, partnership, society, trust, or any other entity, organization, or group including governmental entities (22 CFR 120.14).

j. Public Domain. Information which is published and which is generally accessible or available to the public through sales at newsstands, through subscriptions which are available without restriction to any individual who desires to obtain or purchase the published information, through second class mailing privileges granted by the U.S. government, at libraries open to the public or from the public can obtain documents, through patents available at any patent office, through unlimited distribution at a conference, meeting seminar trade show or exhibition, generally accessible to the public in the United States, through public release (i.e., unlimited distribution) in any form after approval by the cognizant

U.S. Government department or agency, and through fundamental research in science and engineering at accredited institutions of higher learning in the United States where the information is ordinarily published and shared broadly in the scientific community. Such research will not be considered fundamental research if the institution or its researchers accept other restrictions on the publication of scientific and technical information resulting from the project or activity, or the research is funded by the U.S. government and specific access and dissemination controls protection information resulting from the research are applicable (22 CFR 120.11).

k. Protected Individual. A citizen or national of the United States; an alien lawfully admitted for permanent residence, an alien lawfully admitted for temporary residence (subject to amnesty provisions of the law), a refugee, or a person admitted for asylum (8 U.S.C. 1324b). (**NOTE:** See NOTE at paragraph h., above.)

l. Security Assurance. For the purpose of this TCP, a written confirmation by a foreign national's government with respect to access to classified and controlled unclassified information by a foreign national who is a visitor, who is designated as a escort or courier for a classified package or consignment, or who is assigned to a facility as a liaison officer, the person possesses a specified level of personnel security clearance, the person is authorized by his or her government to take possession of or acquire knowledge regarding classified information, and the foreign national's government will ensure that the information will be protected in accordance with applicable security agreements or other requirements specified by the U.S. Government.

m. Technical Data. Information required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance, or modification of defense articles. This includes information in the form of blueprints, drawings, photographs, plans, instructions and documentation. It includes classified information related to a defense article, information covered by an invention secrecy order, and software defined in Part 121.8(F) of the ITAR directly related to defense articles. It does not include information concerning general scientific, mathematical or engineering principles commonly taught in schools, colleges, or universities or information in the public domain; or basic marketing information on function or purpose or general system descriptions of defense articles. (In general, knowledge constitutes technical data if it explains "how" or "why" with respect to design, development, production, etc.)

n. U.S. Person. For the purposes of this TCP, a U.S. person is a natural person who is a lawful permanent resident alien or who is a protected individual as defined in 8 U.SC. 1324b. A U.S. person also is any corporation, business association, partnership, society, trust, or any other entity, organization, or group that is

incorporated to do business in the United States; and any U.S. federal, state, or local governmental entity (22 C.F.R. 120.15. (**NOTE:** refer to items f., g., and k., above. A foreign national (alien) who is a "U.S. person", but who is not a U.S. citizen or national shall be treated as any other foreign national with regard to their access to classified information.)

4. RESPONSIBILITIES. (**GUIDANCE:** This section should identify the facility security officer and the individual who is responsible for coordinating export control and licensing matters, any assistants to those officials who are assigned responsibilities for specific matters (e.g., visit coordination and/or approval), and officers and directors who have security and/or export control oversight responsibilities, and describe their responsibilities. If a company is under FOCI and the clearance arrangement requires a Government Security Committee (GSC), add a description of the composition of the GSC and the roles to be performed by individuals on the GSC.

5. EXPORT AUTHORIZATION REQUIREMENTS. (**GUIDANCE:** This paragraph is particularly pertinent to a FOCI situation. Summarize the company's licensing procedures and the applicability of exemptions. Also, identify the responsible office or position within the company (e.g., "empowered official") and describe its responsibilities or duties with respect to ensuring compliance with the NISPOM and export control regulations.)

6. EXPORT VIOLATIONS AND CONSEQUENCES. (**GUIDANCE:** Describe typical export control violations, and Federal and company penalties for violations; emphasize dangers of marketing initiatives, and proposals that may create false impressions that the U.S. Government may be willing to approve a transaction. Include procedures for handling violations. If the TCP is prepared for a FOCI situation, employees should be cautioned regarding potential violations that could occur with respect to visits by individuals representing foreign owners or shareholders, as well as foreign national employees.)

7. VISITS AND OTHER CONTACTS WITH FOREIGN NATIONALS. (**GUIDANCE:** Describe the company's procedures concerning the application of Chapters 6 and 10 of the NISPOM.)

a. PLANT VISITS BY FOREIGN NATIONALS. (**GUIDANCE:** Describe procedures for authorizations, security assurances, oversight responsibility and records. If the company is under a FOCI clearance arrangement, describe any additional internal procedural enhancements required by the arrangement with respect to affiliates of the parent company, records, contact reports, etc; these should appear in the clearance arrangement) (NOTE: A visit authorization that is approved by a U. S. Government agency may constitute an export authorization (to qualify, the authorization must specifically identify the technical data that is authorized for disclosure) if technical data is

divulged; records therefore must be maintained in compliance with the ITAR requirements for export records.)

b. VISITS BY COMPANY REPRESENTATIVES. (**GUIDANCE:** Describe procedures for obtaining authorizations and for maintaining records; how to handle visits to other government or contractor facilities by foreign national employees of the company, including those who are protected individuals. Include procedures for notifying the locations to be visited of foreign national employee access authorizations and restrictions.)

c. OTHER CONTACTS. (**GUIDANCE:** Describe procedures for controlling the use of e-mail, faxes, telephones, etc., that are necessary to avoid inadvertent exports/disclosures. If cleared under a FOCI arrangement, include any additional requirements prescribed by the arrangement with regard to record keeping and/or reports, including assignment of responsibilities for oversight.)

d. AREA ACCESS CONTOL AND OVERSIGHT. (**GUIDANCE:** Describe procedures pertaining to off-limit areas, work segregation, the use of distinctive badges, controls on the use of information systems, such as reproduction machines, e-mail, etc., and the designation of a contact officer/responsible employee to provide oversight and monitor the foreign national's activities within the company.)

e. ACCESS TO INFORMATION. (**GUIDANCE:** Describe procedures for identifying specific information and technology that is authorized for access by each foreign national visitor (or group of visitors if present for the same purpose and access is the same) assigned to the facility, e.g., a separate authorization document which may be appended to a generic TCP. This information should be extracted from the applicable visit authorization or license that approved the presence of the visitor or from contract documents, such as a security classification guide, Program Protection Plan, or Program Security Instruction. The contact officer or other designated employee of the company will ensure compliance with regard to specific access, and justify any additional access requirements to be submitted for government approval. This person must be familiar with the pertinent export control and security laws and regulations and all aspects of the TCP.)

f. ORIENTATION AND CERTIFICATION. (GUIDANCE: Describe procedures to ensure that foreign national visitors assigned to the facility on an extended visit authorization are notified of and attest in writing to their understanding of and intent to comply with the TCP requirements, the information access authorizations, restrictions pertinent to their particular situation, and the consequences of any violations of same.)

8. FOREIGN NATIONAL EMPLOYEES.

a. HIRING FOREIGN NATIONALS. (**GUIDANCE:** Describe company hiring policy, the distinction between access to unclassified export controlled information and classified information by foreign nationals, who are foreign persons and those who are U.S. persons (i.e., protected individuals), and limited access authorization (LAA) considerations and procedures regarding any foreign national that will require access to classified information, etc.)

b. AREA ACCESS CONTROL AND OVERSIGHT (GUIDANCE: Same as for paragraph 7.d., above.)

c. ACCESS TO INFORMATION. (**GUIDANCE:** Same as for paragraph 7.e., above.)

d. ORIENTATION AND CERTIFICATION. (**GUIDANCE:** Same as for paragraph 7.f., above.)

e. TERMINATION OF EMPLOYMENT. (**GUIDANCE:** Describe procedures to be followed upon the termination of employment of a foreign national employee (e.g., termination briefing regarding continued protection of classified and unclassified export controlled information, penalties, and termination certification with regard to obligation for compliance with security and export control laws and regulations.).)

9. SECURITY EDUCATION AND AWARENESS. (**GUIDANCE:** Describe procedures for ensuring all employees, subcontractors, consultants, advisors, and agents of the company are aware of the presence of foreign national visitors or employees; the terms of the TCP and access authorizations and restrictions; and requirements to report any violation of the company's internal security procedures, including the TCP, the NISPOM, or export control laws and regulations, and FOCI arrangement, if applicable.)