**Technology Control Plan (TCP)** [[1]](#endnote-1)

If your enterprise deals in controlled technology and either employs foreign nationals or has frequent meetings with foreign nationals, it is recommended that your enterprise develop a Technology Control Plan (TCP).

Many enterprises fail to recognize the threat posed by insiders and employees who can potentially abuse or exceed their authorized access to controlled information/data to steal sensitive technology or information for financial gains and other malicious goals (e.g. theft of intellectual property for foreign enterprises or governments). Indeed, insider threats have become a common and popular trend targeting private sector enterprises as well as government agencies for reasons that range from financial gains and IT sabotage to business advantage and industrial espionage. As a result, many enterprises choose to rely on technology control plans that institute physical and IT security policies and mechanisms to combat these threats.

A TCP establishes internal procedures that are designed to prevent unauthorized access to controlled technology and ensure compliance with any national STC requirements. A TCP should be incorporated into an enterprise’s ICP and include the additional features of a **physical security plan, an information security plan, and personnel-screening procedures**.

**Elements of a Technology Control Plan (TCP)**

**A comprehensive TCP** **should address the following areas to help ensure proper management of strategic technology and information:**

* Develop an overarching enterprise policy statement identifying the relevant regulations and legislation and mandating compliance with the requirements of strategic trade controls;
* Document domestic and foreign STC requirements related to technology transfers;
* Clearly specify what constitutes “controlled technology” and define other relevant terminology;
* Designate the empowered compliance official(s) responsible for managing and overseeing the TCP, including contact details;
* Define the roles and responsibilities of the official(s) responsible for managing the TCP (e.g. Technology Control Officer);
* Articulate technology control requirements, processes and procedures;
* Recognize the enterprise personnel to whom the requirements apply;
* Specify employee responsibilities as well as the obligations of contractors and suppliers;
* Identify the location of controlled “technical data” and the facilities and premises where restrictions apply;
* Provide guidance related to **information security and IT systems access** in order to prevent unauthorized transfers of controlled technology;
* Password protection, logins, session lock
* Use of file encryption, firewalls
* Anti-virus and cybersecurity checks
* Use of Virtual Private Networks (VPNs) and non-networked servers
* Destruction/deletion of controlled technology
* Institute **physical security measures** to prevent unauthorized access. Practices should be described related to:
* Access controls
* Visitor identification and control
* Document and data storage
* Disposal of controlled information
* All export and import processes, including intangible transfers, should include review and documentation procedures to prevent unauthorized transfer at each key stage;
* A classification system should be described and in place to appropriately distinguish and classify all controlled information. The system should seek to firewall controlled technology from non-controlled technology;
* Procedures for document control, storage, handling, and disposal should be adequately described
* Develop personnel screening procedures to ensure employees do not have a criminal background or links to designated entities or individuals that are involved in proliferation activities. Note: *The RPST that is part of the ICP Guide can be used to screen personnel against the various, designated entity lists*.

Note: *Appendix 1 of this section contains a “TCP Template” that can be customized and used by your enterprise. Additionally, this section provides information that can enable your enterprise to develop a “Foreign National Access Control Plan.”*

1. Adapted and modified from “Australian Best Practice Guide for the Management of Controlled Exports and Technology,” Australian Industry Group, May 2014, < http://pdf.aigroup.asn.au/13266\_ecf\_best\_practice\_guide\_cover\_web.pdf>. [↑](#endnote-ref-1)