**Physical Security Best Practices**

* **Clearly-Identify Controlled Technology** **→** All controlled items should be clearly marked “controlled” and should be clearly-distinguished and physically segregated from non-controlled technology and information. It might be appropriate to classify information into data categories such as: 1) Public Use, 2) Internal Use Only, and 3) Confidential/Controlled.
* Next, your enterprise may seek to “tag” or appropriately classify any technology or information that is deemed to be sensitive or subject to control. A Commodity Classification Number (CCN) should be assigned to any strategic data that is found on the national control list and this information should be catalogued in databases/document files for future reference.
* **Create Secure Physical Storage →** Controlled technology should be locked in a secure container (cabinet, safe, drawer) when not in use or possession of authorized enterprise personnel.
* Utilize the “One lock Principle”. The “One Lock” principle of securing controlled items requires using at least one mechanism (keys, key cards, access codes, etc.) to prevent disclosures to unauthorized persons. Note: *This is the minimum requirement for safeguarding controlled technology and information*.[[1]](#endnote-1)
* Paper or hard-copy files containing controlled information or technology should be stored under lock in key (e.g. in a secured locked file cabinet in an office that is locked when unoccupied).[[2]](#endnote-2)
* Controlled technology that cannot be stored in a secure a container when not in use may require additional security precautions. This type of “open” storage tends to be less secure and presents greater risk of inadvertent transfers of controlled technology and information.[[3]](#endnote-3)
* It is recommended that controlled information not be removed from storage without approval from the appropriate empowered compliance official within your enterprise.
* Establish procedures for the proper destruction and disposal of controlled information (e.g. papers, schematics, blueprints).
* **Establish Restricted Areas** **→** Restricted areas are used to regulate access to controlled technology that is located in an open area during operating hours. Restricted work areas often employ physical barriers to protect against the oral or visual transfer of controlled information to unauthorized individuals.
* The restricted area should have a clearly defined perimeter, but physical barriers are not always required.
* A restricted area is prudent when it is impractical or impossible to protect access to the controlled technology due to its format, size, quantity, or other unusual characteristic.
* Personnel within the restricted areas are responsible for challenging all persons who may lack appropriate authority to enter the restricted area.
* **Institute Access Controls →** Many enterprises employ access controls to ensure that controlled technology is only accessible to authorized personnel.
* Utilize key controls to manage access to controlled technology. Key controls can be manual but preferably, they should be electronic (e.g. key cards or key control pads with individual employee access codes).
* Employ video surveillance and CCTV around the clock to monitor access to controlled technology
* Establish a single entry policy, whereby every employee must individually access restricted areas or controlled technology using their own key, badge, access code, or credentials (seek to prohibit two people from entering at once).
* Require sign-in to obtain access to controlled technology or equipment. When possible, controlled information should be stored in locked containers with established sign-out procedures so that a log of chain of custody is maintained. When this is not possible, your enterprise should consider utilizing restricted areas in order to track who has entered and exited.[[4]](#endnote-4)
* Create an access log detailing all individuals that have entered restricted areas or accessed controlled information or technology.
* **Develop Visitor Identification and Control Measures** **→** It is your enterprise’s responsibility to ensure that visitors are not afforded access (by visual or oral means) to controlled technology unless it is permitted under a license from the relevant national authorities. **Your enterprise can take the following actions to help prevent visitor access to controlled technology and information and maintain compliance with STC requirements:**
* *Screening*  → It is recommended that your enterprise screen visitors in advance to ensure that they are not designated on any restricted party or entity lists (Note: *Your enterprise can use the RPST to screen visitors against relevant lists*). In addition, it may be important to ascertain the nationality of the visitor in advance as **some countries maintain restrictions on transfers of controlled technology to certain foreign nationals**. Your enterprise may also consider a resume/Visa review to ensure that the visitor does not present undue risks or have any ties to designated parties, individuals, or destinations.
* *Visitor registry* → It is recommended that your enterprise require all visitors to sign a visitor register prior to entry into your enterprise’s facilities. It is your enterprise’s responsibility to establish whether the visitor is authorized to access controlled information, and to provide an appropriate badge and/or escort.
* *Visitor escorts and identification badges* → All visitors should be required to wear an identification badge. The visitor’s ID badge should be easily identifiable and displayed at all times within your enterprise’s facilities. Visitors that do not have access to controlled information should be escorted at all times by employees and should be made to wear visitor identification cards/badges at all times.[[5]](#endnote-5) Some enterprises enable the badges with Radio Frequency Identification (RFID) tags to monitor the physical proximity of visitors to controlled technology.
* *Non-Disclosure Agreements (NDA)* → Your enterprise might consider requiring visitors to acknowledge the existence of the ICP (and/or TCP) and require visitors to sign an NDA that prevents the visitor from disclosing any information related to the visit. Note: *Appendix 2 of this section contains a “Controlled Information Non-Disclosure Agreement Template” that can be customized by your enterprise*.
* *Physical inspections* → Your enterprise might consider conducting physical inspections of bags, parcels, and electronic storage media upon entry. Visitors may be asked to deposit cell phones or other electronic devices prior to entering facilities that contain controlled strategic technology.
* *Third party access controls* → Your enterprise might consider establishing controls to limit custodians, maintenance, building management from accessing controlled information.[[6]](#endnote-6)
1. Beran, Mary and David Brady, "Using Technology Control Plans in Export Compliance," University of Pennsylvania, 2013, <http://www.upenn.edu/researchservices/Export%20Controls%20Conference/Mary%20Beran%20&%20David%20Brady%20-%20Using%20Technology%20Control%20Plans%20in%20Export%20Compliance.pdf>. [↑](#endnote-ref-1)
2. “University of Pennsylvania Office of Research Services TCP Template,” University of Pennsylvania, available at, <http://www.upenn.edu/researchservices/exportcontrols/documents/annotated%20TCP%20Template%20v3.docx>. [↑](#endnote-ref-2)
3. Beran, Mary and David Brady, "Using Technology Control Plans in Export Compliance," University of Pennsylvania, 2013. [↑](#endnote-ref-3)
4. “University of Pennsylvania Office of Research Services TCP Template,” University of Pennsylvania. [↑](#endnote-ref-4)
5. “Australian Best Practice Guide for the Management of Controlled Exports and Technology,” Australian Industry Group, May 2014. [↑](#endnote-ref-5)
6. Beran, Mary and David Brady, "Using Technology Control Plans in Export Compliance," University of Pennsylvania, 2013. [↑](#endnote-ref-6)