I. Purpose

To ensure that SAO-affiliated persons, who work on export-controlled projects and travel with their laptops and mobile devices, take additional export compliance security precautions in advance and bring proper documentation for equipment when traveling overseas. This is to prevent the loss of export-controlled data, violation of export control regulations, and problematic issues of customs duties when entering or exiting foreign borders.

II. Responsibilities

Export Compliance Officer (ECO) export@cfa.harvard.edu 617-496-7557

Accountable Property Officer (APO) shipping@cfa.harvard.edu 617 495-7318

Manager of Computation Facility (CF) vmcglasson@cfa.harvard.edu 617 496-7508

Traveler

III. Questions, Definitions, and References

QUESTIONS:

Address all questions related to this procedure to:
Natascha Finnerty at 617-496-7557 or export@cfa.harvard.edu.

DEFINITIONS:

Electronic Export Information (EEI) – required filing made of export to Bureau of Census by the exporter or shipping company.

Export Administration Regulations (EAR) – 15 CFR Parts 7.30 – 774 Regulations over the export of sensitive items that are commercially available.

International Traffic in Arms Regulations (ITAR) – 22 CFR Parts 120 – 130. Regulations over the export of sensitive items that are related to defense or space applications.

REFERENCES:

SD 931 Use of Computers, Telecommunication Devices and Networks

SI Office of Inspector General (OIG) Management Advisory Regarding Portable Computer Encryption (M-13-01)

SAO 7. Export License Procedure (EC #7)

SAO 8. Export Clearance Procedure (EC #8)

IV. Policy

Travelers who work on export-controlled projects shall use disk encryption on computers and remove all export –controlled information and technical data off laptops and mobile devices. Travelers should activate enhanced security features on smart phones prior to travel. This document supplements SAO's policies related to mobile device security, as communicated by the **CF Manager**, for projects that are export controlled.

V. Procedure

CF works with the **ECO** to offer solutions to better secure export-controlled data on mobile devices. Devices can be compromised. The ITAR regulations permit **overseas Travelers** to access a secure network remotely for restricted files, but the **Traveler** must leave the files on a secure server.

1. If the **Traveler's** device contains export-controlled information, it must be encrypted. (**Travelers** can be stopped by enforcement officials at an airport. **Traveler**s found to have unencrypted export-controlled data can be fined $10,000 and/or the device could be confiscated.)
2. If the **Traveler's** trip involves sharing export-controlled research data with non-U.S. Persons, the **Traveler** should contact the **ECO** to determine if the activity requires an export license or is approvable by license exception under the Export Administration Regulations (EAR), or license exemption under the International Traffic in Arms Regulations (ITAR). Follow Export License Procedure.
3. The following security actions are recommended to protect export-controlled research:
    a. Google Chromebooks are available from the **CF** for travel to ensure no data is stored on the device.
    b. Google mail accounts can be further protected by activating enhanced security features which require 2-step verification when an attempt is made to log into your account from a different device. (For instructions - https://support.google.com/accounts/answer/180744?hl=en)
    c. **Travelers** are encouraged to request the **CF Manager** for a secure a flash drive called an "Iron Key" to store and transport export-controlled data for travel in US or abroad.
    d. Files that need to be accessed during travel should be stored and accessed on SAO's Google Apps for Government domain.
    e. **Travelers** who plan to work on export-controlled projects in public areas such as airplanes should use privacy screens, which can be purchased at office supply stores.
    f. Smart phones with SAO email accounts should have enhanced PIN features that require more than 4-digit PINs. The assigned security PIN should start with high numbers such as 8 or 9.
    g. Mobile devices should be physically secured at all times, even in a hotel room.
    h. Accepting flash drives from vendors or conference organizers is discouraged, as these devices may contain malware.
4. If the **Traveler** is concerned that their device may have been compromised during their travel, they should bring it to the **CF** for scanning. If their device was lost or stolen, they should also report it to the **CF** and to the **APO**.
5. When the **Traveler** brings other research equipment or supplies with them on their trip, they must contact the **APO** in advance, follow the Export Clearance Procedures, and complete the Export of Hardware Checklist (Form ECO-1). The export may need to be filed with the Bureau of Census prior to export, and the equipment may be flagged by U.S. Customs when exiting or entering the U.S. border.

6. The **Traveler** should be cognizant of foreign laws relating to explicit materials on laptops if they are traveling to countries with strict religious codes.
7. **Travelers** need to ensure any items being brought along do not violate Transportation Security Administration (TSA) regulations regarding hazardous material, magnetic items, liquids, flammable items or weapons. For latest update of items that cannot be brought on board an aircraft, click on link above.
8. If the **Traveler** will process items through U.S. Customs temporarily to a foreign country on a carnet or temporary import bond, refer to the Export Clearance Procedure. Contact export@cfa.harvard.edu if there are any questions.

VI. Records to Maintain

Email communications between **Traveler/Administrator** and **ECO/APO** relating to export
Completed Export of Hardware Checklist
Commercial Invoice for research equipment
Electronic Export Information report (EEI) for Bureau of Census, if required
Records are maintained for five years by the **ECO** and/or **APO**