Export Control Network Computer Policy

Where a project requires a computer to process or store export controlled data (ITAR/EAR/nuclear), and the computer also requires access to the Internet or the UF intranet, the computer is referred to as an Export Control Network Computer (ECNC).

This policy establishes security requirements for Export Control Network Computers in order to be granted an exemption from the 2008 UF policy [1] that prohibits computers that store and process Export Controlled data from connecting to any network.

In addition to compliance with UF information security policies, standards and procedures [2], the following are required of an Export Control Network Computer.

1. Records must be provided to DSR and Information Security and Compliance that document the following for each Export Control Network Computer:
    a. Location
    b. IP address
    c. Name and GatorLink ID of all individuals with physical and electronic access to the computer
    d. Quantification of export controlled data record volume
    e. Name and Signature of IT staff responsible for ensuring compliance
    f. Name and Signature of Principal Investigator

2. The following must be submitted to the UF Information Security Manager (ISM)for approval.
    a. Firewall configuration
    b. Physical security procedures
    c. Patch management procedures
    d. Account management procedures
    e. Data access management procedures
    f. Backup procedures
    g. Incident management procedures
    h. Media disposal and reuse procedures
    i. Employee exit procedure

3. The Export Control Network Computer will be audited for compliance by UF Information Security and Compliance before receiving or storing any export controlled data and on an annual basis.

4. UF Information Security and Compliance must be provided full administrative privileged access to the Export Control Network Computer in order to verify its compliance.

5. The Export Control Network Computer must comply with controls specified in the DISA – STIGS (http://iase.disa.mil/stigs/index.html) respective to its operating system.
    a. Linux
    b. Windows
    c. Mac
    d. Other

6. Access to Export Control Network Computers must be restricted to and from the fewest Internet and Intranet sites possible. (server vs workstation)

7. Transmission of export controlled data across the network must be encrypted using secure protocols such as SSL, SSH or VPN.

8. All web browsers and email mail clients on the Export Control Network Computer must be run under a user account with minimal privileges and they must run in a sandbox with limited access.

9. Backup and print media must be marked with the warning, “This media (or document) contains data whose export is restricted by the Arms Export Control Act (Title 22, U.S.C., Sec 2751, et seq.) or the Export Administration Regulations (under the Export Administration Act of 1979 and the International Emergency Economic Powers Act). Violations of these export laws are subject to severe criminal penalties. Do not distribute without authorization. Render unreadable prior to disposal or reuse.”

10. Backups that might be transported must be encrypted. Otherwise, access to backups must be protected by a password.

11. Backup and print media must be stored in a secure location such as a safe or locked cabinet that can be accessed only by those who are authorized.

12. Electronic and printed media must be tracked and rendered unreadable prior to reuse or disposal [3].

13. Any incident involving a security breach of the Export Control Network Computer and/or the controlled data contained on the Export Control Network Computer shall be reported to DSR as soon as possible, but in any event within 36 hours of identification of said incident.

14. IT staff in the department conducting the research will audit the Export Control Network Computer on a quarterly basis to ensure compliance with these requirements.

[1] Fundamentals of Export Controls and Trade Sanctions and Embargoes for Research Universities:
http://www.admin.ufl.edu/DDD/attach07-08/19May08_1.doc
[2] UF Information Security Policies:
http://www.it.ufl.edu/policies/security/
[3] UF Media Reuse and Data Destruction Standards for IT Workers:
http://www.it.ufl.edu/policies/security/documents/it-worker-reuse-and-disposal-standards.pdf