ITAR Electronic Data Storage & Transmission Procedure

1.0 Objective

The purpose of this Procedure is to establish minimum guidelines for the protection of International Traffic in Arms Regulations (ITAR) information during Electronic Data Storage & Transmission processes. This procedure is intended to instruct the Southern Research Institute (SR) staff as to how this information can be accessed, transmitted and stored.

2.0 Scope

This procedure applies to all electronic communications of ITAR data. Communications include but are not limited to email, instant messaging, chat and all variations of transfer processes. This document applies to information stored on mobile and cellular devices, e.g. cell phones, tablets, smart phones, etc. This procedure also applies to all Computer Systems and peripherals, including USB Ports, CD burners, tape or flash memory, etc. at or owned by Southern Research regardless of location or any piece of equipment that has ITAR data on it.

3.0 Responsibilities

The Export Compliance Specialist (ECS) has overall responsibility and may delegate responsibility for review to appropriate individuals.

Each SR Division/Department is responsible for implementing, reviewing and monitoring compliance with this standard.

Each employee is responsible for the protection and dissemination of the data in their possession in a manner that complies with all export control laws and regulations and adheres to the principles and intent of this document and those enumerated in the project contract.

4.0 Definitions and Abbreviations

Term/Acronym	Definition
ECS	Export Control Specialist
IT	Information Technology
ITAR	International Traffic in Arms Regulations (22 CFR parts 120-130)

ITAR Data	Information other than software which is required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of defense articles. This includes blueprints, drawings, photographs, plans, instructions or documentation.
CONUS	Inside the Continental United States
OCONUS	Outside of the Continental United States
U.S. Person	A citizen of the United States of America, permanent resident of the United States of America (green card holder) or a protected individual as defined by 8 U.S.C. 1324b(a)(3)2. Also includes any corporation, business association, partnership, society, trust, or any other entity that is incorporated to do business in the U.S.A.

5.0 Procedure

5.1 The following definitions describe how ITAR data is to be handled:

Strict control must also be maintained over ITAR information that is stored on personal computers (SR owned), personal computers (employee owned) when accessing SR ITAR data, external media (such as CDs, tapes, or memory sticks) or centrally on servers, as well as transmitted across SR's network. The following guidelines have been developed for the storage and transmission of SR ITAR data:

- **Storage**
  - Electronic ITAR information must be stored on any device as described in Section 2.0 Scope. Exceptions must be reviewed and approved by IT Security.
  - All portable devices must be maintained under the control of Institute employees. All devices must require a unique logon with a strong password for each individual authorized to use it (i.e. shared accounts and passwords are not permitted).
  - Whether the SR ITAR information is housed on a server or workstation, the machine must meet current operating system, hardware and software support levels. Legacy systems (Win95, XP, NT, etc.) required for the work but not connected to the network are exempt from this requirement. Current standards are found in IT Annex (Appendix A).

- **Transmission**

    - ITAR information should never be transmitted over the Internet unless it is encrypted or password protected. It should always be transmitted using an IT Security-approved encryption mechanism. Applications with built-in encryption capabilities, e.g., Microsoft Excel, Word, are acceptable.

    - ITAR information must not be transmitted via unprotected email.

    - Electronically transmitted ITAR information will be protected by encryption or password when transmitted over any wired or wireless network.

    - IT will prevent computers with unapproved electronic communications and data transmission solutions from accessing SR information resources including the SR network.

    - Failure to comply with ITAR restrictions is a violation of Federal Law and may result in prosecution. Additionally, see Section 7.0.

6.0 Protection

See the table below for minimum standard protection requirements for each category of data when being used or handled in a specific context (e.g. ITAR Data sent in an email message). Please note that the below protection standards are not intended to supersede any regulatory or contractual requirements for handling data. Some specific data may have stricter requirements in addition to the minimum standard requirements listed below.

	ITAR Data
Granting Access or Sharing	ITAR data shall only be transmitted or communicated to U.S. persons with a legitimate right to the data unless authorized by a license or specific exception.
Disclosure, Public Posting, etc.	Not permitted unless required by law. If however, it is desirable to disclose the non-ITAR portion of the data, the document may be able to be released in an open forum. Seek the council of the ECS and project manager in this situation.
Electronic Display	ITAR data shall be displayed only in authorized forums where it is verified that access is restricted to U.S. Persons, e.g., a representative of the host company/agency has vouched for the citizenship of the people in the room.

Open Records Requests	ITAR data is typically not subject to open records disclosure.
Exchanging with Third Parties, Service Providers	When data are provided to a third party service provider, notice of ITAR contents must be made by appropriate markings, with a cover sheet.
Storing or Processing: Server Environment	Servers shall comply with security requirements as outlined in the Network Security Policy. List of servers that meet these requirements are listed in the IT System Annex, Appendix A.
Storing or Processing: Endpoint Environment (e.g. laptop, phone, desktop, tablet, etc.)	Systems shall comply with security requirements as outlined in the Network Security Policy.
Storing on Removable Media (e.g. thumb drives, CDs, tape, etc.)	ITAR data stored on removable media and removed from SR facilities shall be encrypted and the media shall be under the control of an appropriate U.S. Person.
Domestic Electronic Transmissions, Email and other electronic messaging*	Secure, authenticated connections or secure protocols shall be used for CONUS transmission of ITAR data. Only those services designated for ITAR data will be used. Examples include but are not limited to; secure file sharing programs such as Center Stage, client secure file sharing programs, or authenticated-key encrypted transmissions. Data shall be included in an encrypted file that is attached to the message. The encryption key/password will be transmitted in a different manner, e.g. separate email or telephonically. *All email is external
Foreign Electronic Transmissions, Email and other electronic messaging*	Taking or sending ITAR data OCONUS is prohibited without proper authorization in the form of a license or specific exemption. *All email is external
Printed materials, mailing, fax, etc.	Printed materials sent out of house that include ITAR data shall only be distributed or available to authorized individuals or individuals with a legitimate need to know and should be marked as ITAR data. Access to any area where printed records with ITAR data are stored shall be limited by the use of controls (e.g. locks, doors, monitoring, etc.) sufficient to prevent unauthorized entry. All faxes should include a coversheet with an ITAR destination control statement on the cover.

Disposal	Any data or copies of data that needs to be discarded should be done so in a way to prevent recovery of the data, consistent with our SR Records Retention Policy.

7.0 Consequences and Sanctions

Non-compliance with these standards may incur the same types of disciplinary measures and consequences as violations of other SR policies, including progressive discipline up to and including termination of employment. Violation of ITAR regulations could lead to prosecution under the law.

Any device that does not meet the minimum security requirements outlined in this standard may be removed from the SR network, disabled, etc. as appropriate until the device can comply with this standard.

Appendix A

IT System Annex

General Software Status	
Supported	**Unsupported**
Windows 7	Windows 2000
Red Hat Enterprise Linux 5.0 +	Win 95
Windows Server 2003	Windows XP
Windows Server 2008	Windows Vista
Windows Server 2012	Windows NT
Microsoft Office 2010 +	

ITAR Approved Electronic Storage:
\\SRIERCFS1\
\\SROERCMT4\