



## **ITAR Export Compliance Procedures**

Even though the Company does not sell to anyone outside of the U.S., we do sell some products that the government controls to ensure that highly sensitive defense technology and associated information do not fall into the hands of other governments, non-US businesses and/or non-US Citizens. The International Traffic in Arms Regulations or ITAR, dictate the conditions and requirements under which controlled information and technology must be protected and/or restricted. This information can also be given to us by Department of Defense (DOD) contractors under strict operating conditions, in order to secure bids or proposals for these activities.

In order to ensure that we comply with the ITAR regulations, instructions must be carefully followed. If you have any questions about the correct procedure to use, speak with your manager and/or Carole Gavalyas, our compliance officer.

Sales Admin staff must take active notice each time you handle information from Customers and Principals. If a document is a Request for Quote, quotation, specifications page, design, drawing, purchase order, password access or any other document that indicates "ITAR", take immediate action to ensure that:

- the information is carefully protected from unauthorized access
- the information is only faxed or sent FedEx with signature required. Do not email, even if the information is first received via email.
- the appropriate "ITAR" labeling is used for each occurrence
- the electronic information is carefully stored on our internal servers behind the fire walls and nowhere else.
- paper documents are stored in locked cabinets
- the information does not pass to anyone born outside of the US. If you have any question about the proposed recipient of information that you are handling, speak with your manager and/or compliance officer.

Sales Engineers, in addition to the points above:

- when you become aware that staff will be handling ITAR-covered documents, be sure to make the staff aware so they can take appropriate precautions
- export-controlled information must not be accessed from shared, public computers, or posted on public websites or websites that rely solely on IP addresses for access control

Remember, it is imperative that each of us actively ensure that this information is protected from unauthorized access.