Data Security and Compliance Policy for ITAR Compliance Data

Corelis complies with the transfer and protection of technical data and documents that require ITAR governance and which no non-US citizen can access. It is essential for Corelis that we safeguard restricted, confidential, or sensitive data from unauthorized users. Corelis' Data Security and Compliance Policy is designed to reflect the company's commitment to managing all data transferred to us from customers or stakeholders, according to strict standards of confidentiality and care. The policy's goal is to ensure that data is gathered, stored, and handled in a manner that protects all parties from any harm caused by the misuse of data or IT systems.

Corelis directs all customers to use our secure LiquidFiles file transfer system when sending files to us; LiquidFiles is hosted on a server at our facility in Cerritos, California, and allows secure direct connections over the internet. All files received on the LiquidFiles server will expire after 14 days and be deleted from the server within seven days of expiration. Before files expire on the LiquidFiles server, they are copied to a dedicated internal file server for storage with permissions limited to only those employees that must access those files in support of our customers. Corelis "periodically" copies the file server to a secondary server at our Cerritos, California facility for redundancy.

This policy ensures the following:

- All employees that have access to our internal server to access any engineering files have US citizenship.
- Secure Access - each individual with access is assigned an account requiring username/password, or other user-specific authentication methods.
- Physical Security- Our facility is protected from the outside, and only the authorized employees can access our building.
- IT Security- Only those employees that must access ITAR-controlled files in support of our customers are authorized to access those files. Our computers are protected from Cyber-attacks and backed up regularly.
- Shared system -managed solely by U.S. Persons.
- Shared system - Audit logs are generated by LiquidFiles, which is our file transfer system.
- The internal file server shall be managed solely by U.S. Persons, as defined in the export regulations. All users with root or sudo privileges must be U.S. Persons.

Corelis, Inc.,
13100 Alondra Blvd. Suite 102, Cerritos, CA 90703
Phone: +1 (562) 926-6727 • Fax: +1 (562) 404-6196
www.corelis.com

Once any customer transfers their data to one of our internal file servers at our Cerritos location, our **Server Security and File Storage Policy** governs the management of these servers and all files and data stored on servers at this location.

Additionally, we train all of our employees annually on the following:

Training and Awareness

- Scope and purpose of a compliance program
- Responsibility to uphold the provisions of this policy
- Penalty awareness
- Definitions, terms, and acronyms
- Agency regulations as they apply to the handling ITAR data
- Types of imports/exports controlled data
- The purpose of compliance
- Electronic data storage

Procedures

- Identification, receipt, and tracking of controlled goods
- Procedure for reporting privacy breaches of data misuse
- Restricted exports
- Licensing policies
- Sample control statements
- Record keeping
- Operations/Shipping and Receiving

Server Security and File Storage Policy

1. Overview

Unsecured and vulnerable servers continue to be a significant entry point for malicious threat actors. Consistent Server installation policies, ownership, and configuration management are all about doing the basics well.

2. Purpose

The purpose of this Server Security and File Storage policy is to establish standards for the base configuration of internal server equipment owned and/or operated by Corelis. The policy also provides documentation of the applicable regulations and measures taken for file storage. Corelis is responsible for managing storage, which includes backups (if applicable), as well as securing access, monitoring department use, and reporting usage patterns.

Effective implementation of this policy will minimize unauthorized access to Corelis proprietary information and technology. It also serves as evidence to third parties that the legal terms of required availability control are carried out correctly.

3. Scope

All employees, contractors, consultants, temporary and other workers at Corelis must adhere to this policy. This policy applies to server equipment that Corelis owns, operates

or leases that is registered under a Corelis-owned internal network domain. This policy specifies requirements for equipment on the internal Corelis network. The secure configuration of equipment that is external to Corelis on the DMZ must also follow the procedures outlined in this policy.

4. Server Security

4.1 General Requirements

4.1.1 All internal servers deployed at Corelis must be authorized by our IT personnel responsible for system administration. Approved server documentation and /or configuration guidelines must be established and maintained by authorized IT personnel, based on business needs and also approved by Management. IT personnel monitor configuration compliance and implement security policies, which include Management review and approval. All internal servers must meet the following requirements:

- Servers must be registered within the corporate enterprise management system. At a minimum, the following information is also required to positively identify the point of contact:
  - Server contact(s) and location, and a backup contact
  - Hardware and Operating System/Version
  - Main functions and applications, if applicable
- Information in the corporate enterprise management system must be kept up-to-date.
- Configuration changes for production servers must follow the appropriate change-management procedures.

4.1.2 For security, compliance, and maintenance purposes, authorized personnel may monitor and audit equipment, systems, processes, and network traffic per the *Audit Policy*.

4.2 Configuration Requirements

4.2.1 Operating System configuration should be in accordance with approved Management guidelines.
4.2.2 Services and applications that will not be used must be disabled where practical.
4.2.3 Access to services should be logged and/or protected through access-control methods such as a web application firewall, if possible.

Corelis, Inc.,
13100 Alondra Blvd. Suite 102, Cerritos, CA 90703
Phone: +1 (562) 926-6727 • Fax: +1 (562) 404-6196
www.corelis.com

5. File Storage

5.1 Responsibilities in the company

- Provide for IT security, file storage, and data backup.
- Corporate management is directly responsible for this and is personally liable where applicable.

5.2 General legal conditions

- Under no circumstances, unless approved by upper management, should backups be kept offsite or on a cloud service.
- Storing work data on physical devices, including but not limited to USB drives, memory cards, CD, or external hard drives, must be pre-approved by authorized IT personnel.
- Employees of Corelis must only use devices provided by the company unless otherwise given permission.
- Lost or stolen devices must be reported to IT staff and/or a manager immediately to help ensure their safe return and prevent a data leak.
- The law requires specific controls via technical and organizational measures, both with processing data for one's own purposes and with commissioned data processing; in this context, availability control applies in particular.
- Verification of the controls or technical and organizational measures, among other things, must be provided to customers within the scope of commissioned data processing.

5.3 Risks

- Human error: incorrect operation/accident, sabotage, attack;
- Technical disruptions: technical malfunction, hardware failure, line disturbance;
- Force major, accidents, catastrophes: water, fire, etc., and
- Significant to existentially threatening effects on companies possible.

5.4 General regulations

5.41 Minimum technical and organizational regulations

- Data backup must be performed responsibly and competently.
- No accidental bypassing of authorization models by data backup measures is permitted.
- Must provide confidentiality and obligate to data protection.
- Must nominate people responsible for each task area.
- Must determine the need for confidentiality, integrity, and availability.

For additional information or questions, please contact Bill Pakray at Bill.Pakray@corelis.com.