Business Information Security

Restricted data is often stored in electronic format, which can make it more vulnerable to exposure. Because of this the need to protect identifiable information has never been greater.

Glenair UK Ltd is certified to and complies with the requirements of the Cyber Essentials scheme. We are improving our system to comply with the Information Security Management System standard - ISO 27001 requirements, with certification to the same expected in the near future.

Business Information Security Objectives include:

- Understand the organisations critical information assets and protect them in terms of CIA triad (Confidentiality, Integrity, Availability).
- Compliance with customer expectations, contractual obligations and with relevant legal/regulatory requirements.
- Effective Information Security risk management is in place to recognise and respond to threats.
- Effective management of security incidents.
- Ensure that staff support the Information Security programme and are aware of information security related risks.
- Minimise disruption on business and operational impact. Assurance that all systems are protected from Malware, Viruses, and cyber-attacks.

European IT Manager, in cooperation with Departmental Managers, ensures that only employees with limited access are able to use/access restricted information with both parties being responsible and accountable for ensuring that data is handled in a secure manner.

Glenair does not produce restricted or sensitive data; however, some customers have the need to transfer such information in either electronic or paper format to Glenair for manufacturing purposes.

Commercial products originally designed for military uses are also managed in a controlled manner with appropriate and proportionate controls.

Glenair is not a List X facility.

Data handling involves creating, viewing, using, storing or destroying data. It also relates to how we transfer the data from one location to another. Data is not always stored electronically. Occasionally it could be paper stored in a secure lockable filing cabinet.

Despite not being a List X facility, we use best practices in identifying, transmitting, redistributing, storing or disposing of restricted data.

Incident reporting

Information security and cybersecurity incidents and concerns to be reported to European IT Manager - pdraycott@glenair.co.uk

Supply Chain Security incidents (inc. physical security aspects) and concerns to be reported to Purchasing Manager - sharrison@glenair.co.uk

This statement is periodically reviewed to ensure that it remains as accurate as it can be.