Information Security Policy

IMS003
Revision 2

Information Security Policy

January 2023

REVISION HISTORY

Issue No.	Date	Revision Description	Approved by
Initial Issue	July 2022		J Hartley
Revision 1	November 2022	Inclusion of information security business objective within policy.	J Hartley
Revision 2	January 2023	Change of business scope to include consultancy, and removal of individual business objectives listed within the policy as per recommendation from Stage 2 ISO27001 audit in December 2022. Explicit documented commitment to continuous improvement now included.	J Hartley

Information Security Policy

Purpose

The purpose of the Airframe Designs Limited (AFD) Information Security Policy and Information Security Management System, forming part of our overall Integrated Management System (IMS), is to protect and safeguard all information assets either owned by AFD or handled internally or externally with 3rd parties, from all threats, whether internal or external, deliberate or accidental.

Information exists in many forms such as data stored electronically, data in transit, paper records, and verbal information, and this policy and the IMS exists to protect all such information.

The needs and expectations of all interested parties have been considered in the development of this policy.

Policy Objectives

The objective of this policy is to ensure business continuity and minimise the potential for reputational or other commercial damage by preventing and reducing the impact of security incidents relating to information. The implementation of this policy is mandatory.

Please refer to the Enterprise Risk Register to view our business objectives.

Business Scope

The scope of certification is the supply of engineering design services, consultancy, and outsourced manufacturing of mechanical structure.

The policy is designed to ensure:

- Information is protected against unauthorised access
- Confidentiality & integrity of information is maintained
- Information is not disclosed to unauthorised persons through deliberate or careless actions
- Appropriate access to information to authorised users
- The necessary regulatory and legislative requirements are met
- Business continuity plans are produced, maintained and regularly tested
- Training in information security is provided to all staff
- All information security breaches (actual and suspected) are recorded, reported and investigated
- Certification to ISO 27001 is accomplished and maintained.

All staff are provided with training and awareness relating to information security. Records of this training are maintained.

Standards, policies and security operating procedures have been produced to support this policy, covering virus control, access control, personnel security, the use of email and the internet. A formal disciplinary process is documented and implemented to address any issues arising with employees who choose not to comply with these standards, policies and procedures.

The effectiveness of controls are monitored and measured and the results are analysed so that improvements to the IMS can be implemented appropriately.

The CEO takes overall responsibility for all aspects of the IMS and for maintaining this policy and providing guidance on its implementation. It is the responsibility of each employee to adhere to the policies and procedures at all times.

All external consultants are mandated to implement this policy and work within the stipulations of the IMS when undertaking work for AFD. Appropriate access to this policy and IMS is provided to external consultants.

This policy and the IMS are to be regularly reviewed to ensure the policy and system remain appropriate for the business and customer requirements.

We are committed to continuous improvement and this forms a core part of how we conduct business.

Authorised by

Jerrod Hartley

CEO Date 29th July 2022