

INFORMATION SECURITY POLICY STATEMENT

Document control

Prepared by	Darren Russell
Department	Information Technology
Reviewed by	Scott Buchanan
Document Status	Draft
First issue	24 th September 2024
Next Review Date	September 2025

Revision History

Revision	Date	Status	Description	Author
R01	22/09/24	Draft	Initial draft for review	DRU
R02	24/09/24	Published	Published version	SBU

INFORMATION SECURITY POLICY STATEMENT

ES Global has implemented, maintains and continuously improves a formal **Information Security Management System (ISMS)**, in accordance with the requirements of ISO/IEC 27001:2022, to protect the confidentiality, integrity and availability of information processed and stored on behalf of employees, contractors, 3rd parties, customers, business partners and other interested parties associated with delivering **ES Global** products and services.

ES Global handles information assets in various forms including but not limited to spoken, printed, handwritten and electronic data throughout the entire lifecycle of creation, storage, transmission and destruction. These information assets may include confidential, personal and sensitive data, each treated according to specific policies and procedures.

ES Global actively looks for potential security risks and has implemented adequate safeguards to mitigate and potentially eliminate these risks that may cause material damage to the company reputation, financial performance or ability to deliver our products and services to our employees, business partners and customers, ensuring that we maintain their trust in protecting the confidentiality, integrity and availability of their information, subject to any legal disclosure requirements.

ES Global is further committed to continuously improve our policies, standards and procedures as new technology emerges, the business environment evolves and the needs of our staff and customers change.

This Policy Statement has been communicated to our internal and external staff and partners and is available on our website for any other interested party to view.

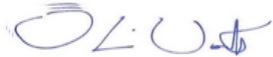
The Chief Operating Officer has overall responsibility for maintaining this policy and providing guidance on its implementation whilst all departmental managers and directors are responsible for ensuring the policies and procedures are implemented and followed within their respective department. It is the responsibility of each affected user of company information assets to adhere to all **Information Security Management System** policies and procedures.

Joint CEO Signatures:

Name: Olly Watts

Date: 24/09/2024

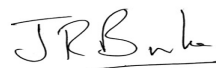
Signed:



Name: Jeff Burke

Date: 24/09/2024

Signed:



COO Signature:

Name: Scott Buchanan

Date: 24/09/2024

Signed:

