IM02D Information Security Privacy Policy

1. Introduction

This document establishes the information security and Privacy policy of Advanced Manufacturing Services. As a modern, forward-looking business, AMS recognizes at senior levels the need to ensure that its business operates smoothly and without interruption for the benefit of its customers, shareholders, and other stakeholders.

Information security is critical to the business success and has the full support and backing from the senior leadership team who will ensure that all personnel within the AMS team are equally as committed.

To achieve a continuous operation, AMS has implemented an Information Security and Privacy Management System in accordance with the internationally recognized standard for information security ISO/IEC 27001:2022, and Privacy ISO/IEC 27701:2019. These standards outline the requirements for an ISMS and PIMS based on globally accepted best practices.

Advanced Manufacturing Services (AMS) is dedicated to safeguarding personal data and ensuring compliance with GDPR. We will adhere to data protection principles, implement robust security measures, respect individual rights, provide ongoing employee training, manage third-party relationships carefully, and continuously improve our data protection practices. By maintaining these commitments, AMS aims to uphold the highest standards of data protection and build trust with our customers, partners, and stakeholders.

AMS has made the decision to maintain full certification to ISO/IEC 27001:2022 and is working in compliance with ISO/IEC 27701:2019 although not certificated.

2. Purpose

The purpose of the information security and privacy policy is to provide a framework for establishing suitable levels of information security and privacy for all AMS information assets and to mitigate the information security and data privacy risks associated with the theft, loss, misuse, damage or abuse of these information assets.

3. Scope

This policy applies to all systems, people, and processes that constitute the organization's information systems, including board members, directors, employees, suppliers, and other third parties who have access to these systems.

It governs all information that is created, transmitted, processed, stored or disposed during the course of AMS business, including the information assets and the systems used to create and maintain this information.

4. Policy Statements

4.1 Information Security and Privacy Requirements

AMS relies on its information assets to support its operations and achieve its business objectives. The unauthorized use or risk occurrence involving these assets can lead to reputational damage, business disruptions, and potential legal consequences for AMS. Therefore, it is crucial that we prioritize the protection of the information we are entrusted with, adhering to the principles of confidentiality, integrity, and availability, while meeting our business needs and complying with legal, regulatory, and contractual requirements.

It is therefore AMS's policy to ensure that:

i. The confidentiality of corporate and customer information is assured.
ii. Sensitive information is protected against unauthorized access, and the integrity of information is maintained.
iii. Information is made available to authorized business processes, employees, suppliers, and other interested parties as and when required.
iv. The requirements of interested parties (including regulatory, contractual, and legal requirements) are met.
v. Specific requirements with regard to the information security and privacy of new or changed systems or services is captured as part of the design stage of each project.
vi. The Company's IMS controls implemented are driven by business needs and regularly communicated to all staff through team meetings and briefing documents.

It is the responsibility of **ALL staff members** to adhere to the requirements laid out in this policy, more specifically:

It is responsibility of **ALL staff members** to:

i. Understand and comply with information security and privacy policies, procedures, and controls relevant to their roles.
ii. Protect the Confidentiality, Integrity and Availability of all AMS information assets.
iii. Report any information security and privacy incident or breach for investigation in accordance with the existing incident management process.
iv. Participate in security awareness training programs and adhere to best practices.
v. Safeguard personal and sensitive data from unauthorized access or disclosure.
vi. Respect individuals' data rights and promptly address their requests.
vii. Collect and use only necessary personal data for valid business purposes.
viii. Obtain consent when required and process data only for specified purposes.
ix. Secure approvals before sharing data with third parties.
x. Report any information security and privacy incidents for investigation in accordance with the existing incident response process.
xi. Participate in security and privacy awareness training programs and adhere to best practices.

It is responsibility of **ALL managers** to:

i. Implement this policy within their business areas, and make sure it is adhered to by their members of staff.
ii. Make sure that all staff within their business area undergoes appropriate security awareness and/or training in support of the goals of this policy.
iii. Ensure the building of an information security culture at AMS via effective application of information security controls and efficient process handling; and
iv. Ensure continual improvement of the IMS through process refinement, risk mitigation controls enhancement, effective non-conformity handling, and compliance to all associated regulatory requirements.

4.2 Framework for Setting Objectives

A regular cycle will be used for the setting of objectives for information security and privacy, to coincide with the budget planning cycle. This will ensure that adequate funding is obtained for the

improvement activities identified. The Information security and privacy objectives will be based upon a clear understanding of the business requirements, informed by the annual management review with stakeholders.
The objectives will be documented for the relevant financial year, together with details of how they will be achieved. These will be reviewed on an annual basis to ensure that they remain valid. If amendments are required, these will be managed through the change management process.

4.3 Continual Improvement of the ISMS

AMS is committed to upholding the highest standards of information security and privacy, ensuring the lawful and responsible handling of personal and sensitive information in accordance with applicable regulations and ethical principles. Therefore, AMS has made the decision to maintain full certification to ISO/IEC 27001:2022 and working in compliance with ISO/IEC 27701:2019 although not certificated.

- Achieve ISO/IEC 27001 certification and maintain it on an on-going basis.
- Continually improve the effectiveness of the IMS
- Enhance current processes in alignment with good practices as defined within ISO/IEC 27001, ISO/IEC 27701, and related standards.
- Increase the level of proactivity (and the stakeholder perception of proactivity) with regard to information security and data privacy.
- Make information security and data privacy processes and controls more measurable in order to provide a sound basis for informed decisions.
- Review relevant metrics on an annual basis to assess whether it is appropriate to change them, based on collected historical data.
- Obtain ideas for improvement via regular meetings and other forms of communication with interested parties.
- Review ideas for improvement at regular management meetings to prioritize and assess timescales and benefits.
- Ideas for improvements may be obtained from any source including employees, customers, suppliers, IT staff, risk assessments and service reports. Once identified they will be recorded and evaluated as part of management reviews.

5. Policy Review

This Information Security and Privacy Policy shall be **annually** reviewed and updated to reflect changes in technology, legal requirements, business needs, and best practices.

The ISMS Manager shall ensure that all employees are informed of policy updates and changes.

We have produced information security privacy objectives which relate to this policy and they can be found in document RO3 Quality, Environmental, Health, Safety and Information Security Privacy Objectives.

This policy is available to all parties through publication on our Company Noticeboard and Share Point.

Authorised by: Richard Jones Position: Managing Director



Date Approved: 01.10.2025 Review Date: 01.09.2027