INFORMATION SECURITY

POLICY STATEMENT

Introduction

The security of INFRATEC-UK's information, and that which is trusted to us by our customers, partners, suppliers and vendors who may hold information on our behalf, is fundamental to protecting maintaining and operating our business.

The loss, corruption or theft of information and supporting systems could have a serious impact on the company's business activities and reputation.

Our people, information and processing systems are critical to our business and need to be protected appropriately.

Our policy is to create an environment in which our information is secure. We achieve this by:

- Ensuring the availability, confidentiality and integrity of our information, data and business systems are maintained and controlled.
- Providing a well-managed security function that offers a high level of trust and confidence to our internal stakeholders as well as customers and partners.
- Ensuring we have a robust, secure, and monitored IT infrastructure which protects customers' data and commercial interests.
- Ensuring that the use of information systems by employees does not create unnecessary business risk through inappropriate behaviour.
- Managing assets so they are identifiable, traceable, and compliant with legal and business requirements and remain fit for purpose, ensuring that contractual and business conditions are met.
- Having appropriate controls in place to meet regulatory and legislative requirements and to ensure those controls are effective.
- Ensuring the company promotes good security, guidance, and advice where appropriate.

It is the responsibility of every individual in and associated with the business to:

- Handle our own and third-party information appropriately according to its sensitivity and/or classification.
- Take steps to minimise the chance of information being lost.
- Report security incidents or anything suspicious which may give rise to a security incident.
- To prevent or minimise disruption to the business that may lead to financial or operational loss or a negative impact to reputation to the company.
- Exercise vigilance when using computers, removable storage devices and phones or when using email and internet services.
- Use INFRATEC-UK's information and supporting business systems for approved business purposes only and in a manner that does not compromise their confidentiality, integrity, or availability.

Communication and Training

The policy will be communicated at regular intervals, using a range of appropriate media and providing opportunities for questions and concerns to be fully addressed. The policy will also be communicated to other stakeholders, including customers, suppliers and business partners, as opportunity or the need arise.

Implementation

The Managing Director is responsible for the implementation of this policy and other related policies and procedure, including the communication and detailed interpretation, monitoring and any disciplinary action in response to an apparent breach of this policy. The Company Secretary is responsible for maintaining and

reviewing this policy, and for clarifying and resolving general issues. The Company Secretary will oversee any audit of policy compliance on behalf of the Managing Director, which may be considered necessary.

The Managing Director shall update the Senior Management Team (SMT) on at least an annual basis on compliance with this policy.

David Bullock
Managing Director
For and on behalf of the Senior Management Team

Revision Status

Revision	Date	Amendment	Author	Approval
1.0	01/01/2020	New Policy	Lee Payne	David Bullock
1.1	01/01/2024	Updated to reflect new IMS Branding	Lee Payne	David Bullock
1.2	03/01/2025	SMT review – No changes	Lee Payne	David Bullock