3. Policy Statement

It is Xperience's policy to develop, implement and maintain an Information Security Management System that:

- Provides assurance within the company and to our clients and partners that the confidentiality, integrity and availability of their information will be maintained appropriately.
- Manages information security risks to all company and customer assets by basing information security decisions and investments on risk assessment of relevant assets considering; Confidentiality, Integrity and Availability.
- Identifies information security objectives and manages achievement of those objectives.
- Applies appropriate control to maintain the security of information security assets.
- Takes into account business and legal or regulatory requirements and contractual security obligations.
- Protects the company's ongoing ability to meet contracted commitments through appropriate business continuity planning.
- Maintains awareness of all employees so they can identify and fulfil contractual, legislative and company specific security management responsibilities.
- Deals effectively with security incidents to minimise the business impact.
- Ensures commitment to continual improvement.

This Policy is supported by the following:

- A company wide Information Security Management System that is fully compliant and independently certified to the ISO/IEC 27001:2013 Standard for Information Security Management Systems.
- An information security risk assessment process that assesses the business harm likely to result from a security failure and the realistic likelihood of such a failure occurring in the light of prevailing threats and vulnerabilities, and controls currently implemented.
- Setting and regular review of achievement of Information Security Objectives
- Defined security-controlled perimeters and access to controlled offices and facilities to prevent unauthorised access, damage and interference to business premises and information.
- An Information Classification and Exchange Policy including compliance with regulations under the UK Data Protection Act 2018 (DPA 2018) to protect client, partner, supplier, our own and personal employee information which is not in the public domain.
- Development and maintenance of an appropriate business continuity plan to counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters.
- Information security awareness guidance for all company employees.
- Implementation of incident management and escalation procedures for reporting and investigation of security incidents for ISMS management review and action.
- A Senior Leadership Team that supports the continuous review and improvement of the company ISMS.

This Information Security Policy is reviewed by the Senior Leadership Team who recommend amendments and updates to the policy as part of the management review and continuous improvement activities.

Date of Issue: 29 February 2024	Signed:
Date of next review: February 2025	Name: Rod Jackson Chief Operating Officer