Information Security Policy Statement

Information Security at PTFS Europe is the responsibility of all members of staff. We have in place an effective **Information Security Management System** (ISMS) which has resulted in ISO27001:2017 and **CyberEssentials Plus** accreditation.

The **Scope of our ISO27001 registration** is the provision of implementation, hosting and support services for a range of products in the library sector within the UK and European markets.

Our ISMS encompasses all systems used by PTFS Europe in our work of software installation, configuration, data conversion, software development, training, data and systems hosting and customer support for a wide range of customers in the library sector.

Our security policy has the following **objectives** which we track using a set of appropriate key performance indicators:

- Objective 1: PTFS Europe will continuously monitor for and identify emerging security threats, implementing preventative measures on an ongoing basis.
- Objective 2: PTFS Europe will deliver its service in a secure environment such that it minimises the risk of major security incidents and service down time.
- Objective 3: PTFS Europe will regularly analyse risks to information in its care and enhance protective measures as new risks arise.

In pursuit of these objectives we have analysed all parties with an interest in information security at PTFS Europe to identify their security needs and expectations. We continuously scan the **legal and regulatory** environment for changes that affect our security policy and our processes and procedures fully meet the requirements of GDPR legislation.

Physical security at PTFS Europe, a virtual company, is supported by our policy on home working. Although information security is the responsibility of all staff, our Information Security Manager has primary responsibility for ensuring that the large number of servers we deploy and maintain are correctly configured, supported, patched and protected.

Physical data security is enhanced by the infrastructure around our data hosting arrangements with all data being held on remote servers located within an outsourced data centre which has ISO27001:2017 level security in place.

To ensure **business continuity resilience**, daily backups of all customer and internal systems are taken. All servers are backed up to two third party data centre locations with high-capacity power supplies and Uninterruptible Power Supply (UPS) systems. Backups are encrypted using industry standard encryption with decryption only possible by interaction with systems unrelated to the backed up servers to ensure that they are secure and unusable in the event of hardware theft or disk cloning.

Access to our data is closely controlled and is detailed in our Access Control Policy and no third party access is given to any of our internal systems or documentation.

We have carried out a full **risk assessment** of the potential for a breach of security as documented within our separate Risk Assessment Document. Any and all **security incidents** are logged on the helpdesk ticketing system (RT). In the event of a security breach, our Disaster Recovery Plan outlines the procedures to be followed in the case of disasters. In the instance where parts of the Disaster

Recovery Plan can be tested outside of the scope of a disaster recovery incident, and these are recorded.

This policy and the ISMS is **monitored and reviewed** by the Management Team to ensure we meet our security objectives, analyse and respond to risks, train and support our staff appropriately and continuously improve our policies and procedures.

Jonathan Field, Managing Director