PiSYS
Since 1988

DATA PROTECTION POLICY FOR HOSTED SERVICES

ISO 27001

REV	DATE	REVISION	PREPARED	CHECKED	APPROVED
1.0	09-Jul-2024	Draft for Review	KRC	MAK	PIH
2.0	10-Jul-2024	First Issue	KRC, RAG	MAK	PIH

TABLE OF CONTENTS

LIST OF FIGURES

No table of figures entries found.

LIST OF TABLES

ASSOCIATED DOCUMENTS

Pisys Ref. Number	Title / Description

DOCUMENT REVISION NOTES

REV	Title / Description

SECTION A. INTRODUCTION

The Pisys **Data Protection Policy for Hosted Services** is a testament to our unwavering commitment to safeguarding the confidentiality, integrity, and availability of your data. Inspired by the rigorous standards of ISO 27001, this policy combines security measures, ethical practices, and operational excellence to envelop our entire hosting environment. This document is not just a set of rules; it's a pledge to our clients that their digital assets are in the best possible hands.

SECTION B. PURPOSE

The purpose of this policy is to establish the framework for the protection of all data processed, transmitted, and stored within our hosted services, ensuring that the trust you've placed in us is rewarded with an unparalleled level of data security and privacy. By adhering to the principles of ISO 27001, we aim to provide a robust shield against ever-evolving cyber threats and maintain a culture of vigilance and proactive defence in the realm of data protection.

SECTION C. SCOPE

This policy applies to all employees, contractors, third parties, and clients who interact with or have access to our hosted services. It encompasses all forms of data, both digital and physical, across our infrastructure, platforms, and applications. The policy extends to the entire data lifecycle, from inception to archival, ensuring that every bit is treated with the respect and protection it deserves.

SECTION D. POLICY STATEMENT

At the core of our operations is the belief that data protection is a shared responsibility. Therefore, we commit to:

- **Confidentiality**: Protecting the privacy of data by ensuring that it's accessible only to authorized individuals.
- **Integrity**: Safeguarding the accuracy and completeness of data to maintain its authenticity and reliability.
- **Availability**: Ensuring that data is readily accessible to authorized users when needed.

We expect the client to commit to safeguarding access to, and fair use of, Pisys supplied systems and services.

SECTION E. KEY PRINCIPLES

Section E.1. Security Awareness

We foster a culture where every member of our team is a data guardian, committed to understanding and adhering to the best practices in data protection.

Section E.2. Risk Management

We assess, evaluate, and mitigate risks to your data with the same dedication we would for our own, ensuring that our security posture is always one step ahead of potential threats.

Section E.3. Asset Management

Our hosted services are meticulously inventoried, classified, and controlled to prevent unauthorized access or misuse.

Section E.4. Access Control

Only those with a legitimate business need are granted access to your data, and even then, it's on a strict need-to-know basis.

Section E.5. Incident Management

Should the unthinkable happen, we have a battle-tested incident response plan to minimize the impact and restore normalcy swiftly.

Section E.6. Business Continuity

We ensure that your data remains accessible and secure, even in the face of unforeseen disruptions, because we understand that your operations can't afford downtime.

Section E.7. Compliance

We embrace the spirit of relevant laws, regulations, and contractual obligations, ensuring that our hosted services are a bastion of trust and legal adherence.

Section E.8. Regular Audits

Our data protection measures are subject to regular, thorough audits to ensure they remain as robust as the day they were implemented.

Section E.9. Continuous Improvement

Our data protection policy grows stronger with time by adapting to new challenges and incorporating cutting-edge security technologies.

SECTION F. CONTROL MEASURES

Section F.1. Secure Authentication

We implement multi-factor authentication protocols to ensure that only the right people can access your data.

Section F.2. Encryption

Data in transit and at rest are encrypted using industry-leading algorithms.

Section F.3. Segmentation

Our networks are divided into secure zones, reducing the risk of unauthorized access and lateral movement.

Section F.4. Regular Backups

Your data is backed up regularly, stored securely, and can be restored in a timely fashion to minimize the impact of data loss.

Section F.5. Security Updates

Our systems are updated with the latest security patches to keep them impervious to known vulnerabilities.

Section F.6. Incident Response

We have a team ready to respond to security incidents with speed and precision.

Section F.7. Contractual Obligations

We enter into agreements with clients and partners that clearly define data protection responsibilities and expectations.

Section F.8. Staff Training

Our team undergoes regular training to stay sharp and aware of the latest data protection strategies and emerging threats.

Section F.9. Vendor Management

We carefully select and monitor our third-party service providers to ensure they uphold the same stringent data protection standards we do.

Section F.10. Security Assessments

We conduct regular assessments to identify and address any potential weaknesses in our defences.

SECTION G. CONCLUSION

By implementing the ISO 27001-compliant Data Protection Policy for Hosted Services, we aim to create an environment where your data is not just stored but thrives under the watchful eye of a dedicated security team.

This policy is a living document, evolving alongside the digital landscape to provide you with the assurance that your data is always in safe hands.