PiSYS
Since 1988

BUSINESS CONTINUITY

PLAN

REV	DATE	REVISION	PREPARED	CHECKED	APPROVED
1	20/Oct/2015	First Issue	PIH	RAG	
1.3	04/Mar/2020	Update data-centre references from IFB to AWS	KRC/RAG	MAK	PIH
1.4	09/Jun/2020	Replaced Pisys.net references	KRC/RAG	MAK	PIH
	17/Aug/2021	Reviewed	KRC/RAG	MAK	PIH
	14-Jun-2022	Reviewed	KRC/RAG	MAK	PIH
1.5	12/Jun/2024	Updated for 27001:2022	KRC/RAG	MAK	PIH

TABLE OF CONTENTS

TABLE OF CONTENTS 2

LIST OF FIGURES 4

LIST OF TABLES 5

ASSOCIATED DOCUMENTS 6

DOCUMENT REVISION NOTES 6

SECTION A. STATEMENT 7

SECTION B. SCOPE 7

SECTION C. ROLES AND RESPONSIBILITIES 8

Section C.1. Information Security Manager (ISM) 8

Section C.2. Employees 8

Section C.3. Contractors and Vendors 8

Section C.4. Overall and Day to Day Responsibilities 8

Section C.5. Prevention 8

C.5.1. Risk assessment 9

C.5.2. Security awareness training 9

C.5.3. Access control 9

C.5.4. Regular backup 9

C.5.5. Physical security 9

Section C.6. Detection 9

C.6.1. Monitoring systems 9

C.6.2. Incident response team (IRT) 9

C.6.3. Reporting procedures 9

Section C.7. Response 9

C.7.1. Activation of the IRT 9

C.7.2. Containment 9

C.7.3. Eradication 9

C.7.4. Recovery 9

C.7.5. Post-incident review 9

Section C.8. Recovery 10

C.8.1. Business continuity planning 10

C.8.2. Disaster recovery planning 10

C.8.3. Testing and exercises 10

C.8.4. Vendor management 10

C.8.5. Insurance 10

SECTION D. ANNEX A: ESSENTIAL ACTIVITIES (BCP) 11

Section D.1. If an incident occurs 11

Section D.2. What to do after the first hour after the incident 11

Section D.3. Structure of the Incident Response Team (IRT) for Business Continuity 11

Section D.4. Critical Systems 11

Section D.5. Work Area Recovery 12

SECTION D.6. BACKED UP DATA 12
SECTION D.7. ALTERNATIVE COMMUNICATIONS 12

LIST OF FIGURES

No table of figures entries found.

LIST OF TABLES

Table 1 - Responsibilities Table **8**

Table 2 – Incident Response Team **11**

Table 3 - Critical Systems **11**

Table 4 - Areas of Work **12**

ASSOCIATED DOCUMENTS

Pisys Ref. Number	Title / Description

DOCUMENT REVISION NOTES

REV	Title / Description

SECTION A. STATEMENT

Our statement of Business Continuity is:

- To ensure all employees are competent to do their tasks and to give them adequate training.
- To review and revise this plan regularly.
- To provide a general plan on what to do in an emergency.
- To provide details of emergency contacts – staff/suppliers/customers.
- To ensure that the Business continues.
- To ensure that the security of our information assets is maintained and that our information security management system continues to operate as required.

Signed:

Position in Company: Director

Date Signed: 20-Oct-2015

SECTION B. SCOPE

The purpose of this business continuity plan (BCP) is to ensure that ISO 27001 certification is maintained in the event of any disruptions or disasters. The plan outlines the procedures, processes, and resources necessary to protect and restore critical information assets and minimise the impact on Pisys operations. It covers four key areas: prevention, detection, response, and recovery.

This BCP applies to all departments, employees, contractors, and stakeholders involved in the management and protection of information assets within Pisys. It covers all potential disruptions or disasters that could affect operations, including but not limited to:

- Natural disasters: earthquakes, fires, floods, hurricanes, etc.
- Technological failures: hardware or software failures, cyber-attacks, data breaches, etc.
- Human errors: accidental deletion, loss or theft of data, unauthorized access, etc.
- Pandemics or epidemics: outbreaks of infectious diseases that affect employees or their ability to work.

SECTION C. ROLES AND RESPONSIBILITIES

Section C.1. Information Security Manager (ISM)

The ISM is responsible for developing, implementing, and maintaining the BCP. They also act as the primary contact for external agencies and stakeholders during a disaster.

Section C.2. Employees

All employees are responsible for reporting any security incidents or potential disruptions to the ISM. They must adhere to Pisys security policies and procedures.

Section C.3. Contractors and Vendors

All external parties involved in the management or protection of information assets must comply with the BCP and maintain the confidentiality, integrity, and availability of data.

Section C.4. Overall and Day to Day Responsibilities

The following individuals are responsible for checking regularly and maintaining where applicable:

Role	Name
Overall responsibility in accident or incident:	Admin Team / Senior Management
Fire Warden:	N/A
Fire alarms:	Admin Team / Senior Management
Security alarms:	Admin Team / Senior Management
IT systems security:	IT
Health & Safety:	Admin Team
Power supplies:	N/A
Flooding:	N/A
Information Security:	ISMS Team / Senior Management
Insurance cover is up to date:	Admin Team
Customer contact numbers:	Admin Team
Supplier contact numbers:	Admin Team
Power/generators:	N/A
IT infrastructure:	IT
Staff contact numbers: (including next of kin details)	Admin Team

Table 1 - Responsibilities Table

Section C.5. Prevention

To prevent disruptions or disasters, Pisys has implemented the following measures:

C.5.1. Risk assessment

Regularly evaluate Pisys information security posture to identify potential risks and vulnerabilities.
Pisys has an established risk assessment and risk treatment process.

C.5.2. Security awareness training

Provide ongoing training to employees, contractors, and vendors on information security best practices and procedures.

C.5.3. Access control

Pisys has implemented strict access controls to limit access to sensitive information and systems.

C.5.4. Regular backup

Pisys maintains regular backups of critical information assets to ensure their recovery in the event of a disaster.

C.5.5. Physical security

Pisys has implemented physical security measures to protect against natural disasters and unauthorized access to facilities and equipment.

Section C.6. DETECTION

Pisys has established mechanisms for detecting security incidents and disasters, including:

C.6.1. Monitoring systems

Pisys continuously monitors critical systems and infrastructure for anomalies or signs of compromise.

C.6.2. Incident response team (IRT)

Pisys has established an IRT composed of individuals with the necessary skills and expertise to respond to security incidents.

C.6.3. Reporting procedures

Pisys has established clear procedures for reporting security incidents and disasters.

Section C.7. RESPONSE

Pisys has established procedures for data breaches, and dealing with security incidents.
Upon detection of a breach or security incident, the following steps will be taken:

C.7.1. Activation of the IRT

The IRT will be notified and immediately activated to begin responding to the incident.

C.7.2. Containment

The IRT will work to contain the incident and prevent further damage or loss of data.

C.7.3. Eradication

The IRT will work to identify and eliminate the root cause of the incident.

C.7.4. Recovery

Once the incident has been contained and eradicated, Pisys will initiate its recovery procedures, including restoring critical systems and information assets.

C.7.5. Post-incident review

A post-incident review will be conducted to identify lessons learned and areas for improvement in the BCP.

Section C.8. RECOVERY

The recovery process will focus on restoring Pisys information assets and systems to their pre-incident state. This will include:

C.8.1. Business continuity planning

Pisys has developed and maintains a business continuity plan (Annex A) that outlines procedures for recovering critical business functions in the event of a disaster.

C.8.2. Disaster recovery planning

Pisys has developed and maintains a disaster recovery plan that outlines procedures for recovering IT systems and infrastructure.

C.8.3. Testing and exercises

Pisys regularly tests and exercises the BCP and DRP to ensure their effectiveness and identify areas for improvement.

C.8.4. Vendor management

Pisys maintains relationships with reliable vendors and service providers who can assist with the recovery process if needed.

C.8.5. Insurance

Pisys maintains appropriate insurance coverage to mitigate financial risks associated with disasters or disruptions.

SECTION D. ANNEX A: ESSENTIAL ACTIVITIES (BCP)

Section D.1. If an incident occurs

If an incident occurs, call the emergency services, then inform senior management if they don't already know about the situation.

Section D.2. What to do after the first hour after the incident

If a move to an alternative site is taking place, remote working is well established so phones and server access etc. are already in place. Divert the main reception number to the remote phone and continue to operate as normal.

Take whatever steps are necessary to maintain the security of any information, but do not put yourself at risk while doing this.

Directors will convene a meeting with the IRT (see below) and take appropriate action to ensure that normal operation is resumed as soon as possible, meantime staff can continue to work remotely.

All customer and asset data are stored on the cloud and will be accessible remotely.

Section D.3. Structure of the Incident Response Team (IRT) for Business Continuity

Role	Name
Director	Pisys Directors
Admin/Commercial	Admin Team
Systems	IT Manager

Table 2 – Incident Response Team

The team will meet in person if available. Microsoft Teams and/or mobile phones may be used to meet remotely.

Section D.4. Critical Systems

The following systems are essential to our business:

System	Status
Phones:	Remotely-hosted
Email:	Remotely-hosted
Helpdesk:	Remotely-hosted
Client-facing servers:	AWS
Invoicing:	Remotely-hosted
Bookkeeping:	Installed locally and remotely.
A backup of the latest data is available on the remote backup site.	

Table 3 - Critical Systems

Section D.5. Work Area Recovery

Areas of work in priority order:

System	Status
Internet:	AWS: provide internet for customer-facing/hosted services. (Individual staff internet provided by their own ISP.)
Email:	Pisys tenant Microsoft 365 – office admin portal
Phones:	NSoft for remote support

Table 4 - Areas of Work

Section D.6. Backed up Data

All backups are held off-site: The IT Manager can assist with any required recovery.

Section D.7. Alternative communications

If the phone system is unusable, mobiles or email will be used to communicate with staff and customers.