Pentacle Ltd Information Security Policy

1. Introduction

This information security policy is a key component of Pentacle's overall information security management. It incorporates Pentacle's handling of personal data, protection of that data, security of the systems and staff procedures.

Pentacle is committed to safeguarding your personal information. Whenever you provide such information, we shall use your information in line with all laws concerning the protection of personal information, including the Data Protection Act 2018.

Some areas of Pentacle's systems may contain hyperlinks to websites owned and operated by third parties. These third party websites have their own privacy policies, including cookies, and we urge you to review them. They will govern the use of personal information you submit or that is collected by cookies while visiting these websites. We do not accept any responsibility or liability for the privacy practices of such third-party websites and your use of such websites is at your own risk.

This policy will be reviewed annually and updated if necessary.

2. Objectives, Aim and Scope

2.1. Objectives

The objectives of Pentacle's Information Security Policy are to preserve:

- **Confidentiality** – Access to Data shall be confined to those with appropriate authority.

- **Integrity** – Information shall be complete and accurate. All systems, assets and networks shall operate correctly, according to specification.

- **Availability** – Information shall be available and delivered to the right person, at the time when it is needed.

2.2. Policy Aim

The aim of this policy is to establish and maintain the security and confidentiality of information, information systems, applications and networks owned or held by Pentacle, by:

- Ensuring that all members of staff are aware of and fully comply with the relevant legislation as described in this policy.

- Describing the principals of security and explaining how they shall be implemented in the organisation.

- Introducing a consistent approach to security, ensuring that all members of staff fully understand their own responsibilities.

- Protecting information assets under the control of the organisation.

2.3. Scope

This policy applies to all information, information systems, networks, applications, locations and employees of Pentacle or supplied under contract to it.

2.4. Responsibilities for Information Security

When using Pentacle QUBE services, customers maintain complete control over their content and are responsible for managing critical content security requirements, including:

- What content they choose to store on QUBE.
- Which Qubicles they place content in.
- The format and structure of that content and whether it is uploaded to QUBE or shared as a window.
- Who they request to have access to that content and how those access rights are granted. The only people allowed to access are people who the client invites directly or who Pentacle is asked to allow access to (with the exception of Pentacle authorised people). At any time the client can ask Pentacle to revoke access.

Because QUBE users retain control over their data, they also retain responsibilities relating to that content as part of the QUBE "shared responsibility" model. This shared responsibility model is fundamental to understanding the respective roles of the customer and QUBE in the context of the Cloud Security Principles.

Ultimate responsibility for information security rests with the Directors of Pentacle, and, as Pentacle is a small company, on a day-to-day basis the Directors shall be responsible for managing and implementing the policy and related procedures.

All staff shall comply with information security procedures including the maintenance of data confidentiality and data integrity.

Each member of staff shall be responsible for the operational security of the information systems they use.

Pentacle only provides data access and information to employees and contractors who have a legitimate business need for such privileges.

3. Legislation

3.1. Pentacle is obliged to abide by all relevant UK and European Union legislation. The requirement to comply with this legislation shall be devolved to employees and agents of Pentacle, who may be held personally accountable for any breaches of information security for which they may be held responsible. Pentacle shall comply with the following legislation and other legislation as appropriate:

- The Data Protection Act (2018)
- The General Data Protection Regulation (EU) 2016/679
- The Data Protection (Processing of Sensitive Personal Data) Order 2000.
- The Copyright, Designs and Patents Act (1988)
- The Computer Misuse Act (1990)
- The Health and Safety at Work Act (1974)
- Human Rights Act (1998)
- Regulation of Investigatory Powers Act 2000
- Freedom of Information Act 2000

4. Policy Framework

4.1. Access Controls
Only authorised personnel who have a justified and approved business need shall be given access to restricted areas containing information systems or stored data.

4.2. Equipment Security
In order to minimise loss of, or damage to, all assets, equipment shall be physically protected from threats and environmental hazards.

4.3. Information security events and weaknesses
All information security events and suspected weaknesses are to be noted. All information security events shall be investigated to establish their cause and impacts with a view to avoiding similar events.

4.4. Protection from Malicious Software
The organisation shall use software countermeasures and management procedures to protect itself against the threat of malicious software. All staff shall be expected to co-operate fully with this policy.

4.5. System Access and Use
The policy is to balance performance and security, therefore appropriate security protocols are selected to ensure security and low latency (minimum 128 bit cryptographic strength). For enhanced security, QUBE is entirely compatible with client VPN solutions and caged server installations.

Access to data servers via username and password is not permitted; SSH access keys are utilised. Access to data servers and web-based administrative systems is restricted by IP address.

An audit trail of system access and data use by staff shall be maintained.

4.6. Business Continuity and Disaster Recovery Plans
The organisation shall ensure that business continuity and disaster recovery plans are produced for all mission critical information, applications, systems and networks.

4.7. Data Retention and Destruction
Data will be retained by Pentacle for the purpose of providing services to the client and where requested will be removed and destroyed, except where legal or regulatory requirements dictate.

5. Physical Hosting

Pentacle only uses reputable hosting providers who are able to offer:

- 24 x 7 x 365 Manned Security & Monitoring
- Smart Card access policies
- Internal and External CCTV systems
- Security breach alarms
- 24 x 7 environmental monitoring systems
- Constant evaluation and testing of all systems
- N+1 redundant Heating Ventilation Air Conditioning (HVAC) system
- Fully redundant air handling units provide constant fresh airflow
- Raychem Fluid Detection
- FM200 fire suppression equipment

6. Privacy

Pentacle will only collect information necessary to provide the service.

Pentacle will not pass any personal information to any third party at any time without prior permission.

Pentacle may contact you for the following reasons:

- in relation to the functioning of any service you have signed up for in order to ensure that Pentacle can deliver the services to you
- where you have opted to receive further correspondence
- for marketing purposes

We will keep your information confidential except where disclosure is required by law (for example to government bodies and law enforcement agencies).