Infosec for the use of Cloud Services Policy

Objective and Scope

The objective of this policy is to manage the use of cloud services to ensure they are a technology asset and not an impediment to information security business operations. A risk assessment shall be undertaken in all circumstances where cloud services are intended to be established or outsourced as SaaS.

The scope of this policy includes:

- in house development of information platforms working with a cloud provider for data collection, processing, transfer and storage
- outsourced SaaS cloud provided hosting of applications enabling access by the organisation
- specific contracted cloud services for shared responsibility of information security alerts, analysis and IS incident management

Roles, Responsibilities and Authorities

The Operations Director with other advisory competent IT Team delegates determine what and who will provide SaaS to the organisation and monitor their performance throughout the contract lifecycle.

The Operations Director takes ownership for managing internal compliance to SaaS tools and assets ensuring individuals are following due process.

Individuals are accountable for general use of SaaS tools and assets and compliance to this policy.

Where an exception or deviation from an expectation or plan occurs, the senior assigned role shall make the determination in terms of what is an acceptable change. The change management process may need to be enacted.

Legal and Regulatory

Title	Reference
Data Protection Act 2018	https://www.legislation.gov.uk/ukpga/2018/12/contents
General Data Protection Regulation (GDPR)	https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/
The Telecommunications (Lawful Business practice)(Interception of Communications) Regulations 2000	www.hmso.gov.uk/si/si2000/20002699.htm
Computer Misuse Act1990	www.hmso.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm
The Privacy and Electronic Communications (EC Directive) Regulations 2003	www.hmso.gov.uk/si/si2003/20032426.htm
The Freedom of Information Act 2000	https://www.legislation.gov.uk/ukpga/2018/12/contents
National Assistance Act 1948	https://www.legislation.gov.uk/ukpga/Geo6/11-12/29/enacted
Criminal Law Act 1967	https://www.legislation.gov.uk/ukpga/1967/58/introduction

ISO 27001/2 REFERENCES	ISO 27001: 2013 Clause ID	ISO 27002: 2013 Annex A ID	**ISO 27001: 2022 Clause ID**	**ISO 27002: 2022 Control ID**
IS use of cloud services				5.23

Infosec for the use of Cloud Services Policy

Infosec for the use of Cloud Services Policy

Related Information

- SaaS Service Level Agreements

Policy

Prevision Research believes that outsourced cloud services, when carefully selected and used under controlled conditions, are an asset to business operations and can enhance security of information and information systems. This however, is dependent on who, what and how SaaS is managed both in the selection of partners/providers and the in-house management of the provided services and technology assets.

Prevision Research takes a risk based approach to the selection, monitoring and management of SaaS activities including:.

- Due diligence of cloud service providers reputation, integrity and evidence of IS standards being met.
- Specific cloud-service SLAs meeting the scope and needs of Prevision Research confidentiality, integrity, availability, information handling and storage standards.
- The need for an Escrow agreement considered and arrangements for contract termination.
- Jurisdictional capabilities and capacity meeting the scope and needs of Prevision Research.
- Complaints and incident management systems in place that affords timely response and transparency of process and outcomes.

SaaS providers shall be listed on the Supplier Register, which is managed and monitored by the Operations Director. SaaS provider SLAs and online performance records shall be maintained and tabled at management and technical review meetings.

Use of cloud services - scope of services

The Operations Director with other advisory competent IT Team delegates shall determine the need for and scope of cloud services based on:

- Executive management strategies for the business.
- Primary needs that are better serviced by a professional provider such as data storage, transfer, web services.
- Information security capabilities not able to be delivered in-house due to resource limitations.
- Provision and nature of threat intelligence information provided in a timely manner

Taking into account business and practical needs, the Operations Director shall make the final determination of the scope of works to be outsourced to cloud service providers.

Infosec for the use of Cloud Services Policy

Selection of cloud services providers

Selection of cloud service providers is based on the provider's ability to meet the following standard selection criteria:

1. Scope of service required as determined by the Operations Director.
2. Proven standards of information security and industry standards based on certifications and accreditations to ISO 27001 Information security l ISO 17788 Cloud computing l ISO 19086 SLA l ISO 19770 IT assets l ISO 22301 Business continuity l ISO 27007 Cyber security & privacy l GDPR l HIPAA l PCl compliance.
3. Service level agreement acceptable to Prevision Research requirements.
4. Appropriate and acceptable jurisdictional scope.
5. Workable complaints and incident management process acceptable to Prevision Research needs.
6. Acceptable termination and exit strategy.
7. Clear roles and responsibilities between parties on how to interact and communicate.

Jurisdictional legal implications

Prevision Research information security standards require the storage of personally identifiable information and business sensitive information to be retained within the jurisdiction of its original source. This is a key criteria of provider selection.

The need for and use of cryptography by SaaS providers shall be considered to ensure regulations for cryptography across the Prevision Research business jurisdiction is not compromised, including legal obligations relating to access and information of encrypted data.

Cloud service agreements including SaaS providers

Depending on the nature and scope of service provision, cloud service agreement requirements include:

- Defined identity and access controls and application security protocols including malware monitoring.
- Defined logging, monitoring, threat detection and analytics standards.
- Defined scope of processing, data storage availability, security, and performance measures.
- Defined archive, backup and restoration processes.
- Acceptable cookie policy.
- Acceptable privacy policy.
- Formal change notice and revision process.

Prevision Research has a preference that the organisation's information security requirements for cloud services are not subcontracted to an external supplier by the prime provider. The Operations Director shall make final decisions on this matter.

Infosec for the use of Cloud Services Policy

Complaints and Incident management

Complaints and incident management processes must be effective for the business and provide:

- Key contacts and multiple contact methods
- Simple method for investigations and undertaking a root cause analysis
- Rapid response times and effective notifications and reporting

Performance monitoring

The Operations Director shall monitor SaaS performance to:

- Ensure it meets the service level agreements
- Maintain effective communications

Performance monitoring shall be maintained and tabled at management and technical review meetings.

Terminating an agreement including SaaS agreements

Termination agreements in place shall cover the need to terminate a SaaS agreement including:

- Archiving and/or transferring arrangements for information security confidentiality, integrity and availability of information.
- Erasure, destruction, and/or rendering unidentifiable 'at risk' data according to agreed standards within (xx) days of the termination of agreement.

Policy review

This policy shall be reviewed by the policy owner no less than every annually or immediately after a process change or a policy breach is known to have occurred.

Periodic reviews shall take into account feedback from the IT team monitoring processes, penetration testing as applicable, regulatory changes and audits. Changes to the policy must be approved by a senior executive then communicated to all previous persons or organisations with access to the policy.

Refer below for the most recent review.

History table

Date	Rev No	Changes	Reviewed By	Approved By	Training Y/N