Monitor IS

Software Solutions - Service Definition Document

We are technical specialists in cloud software solutions. We provide a full range of cloud services relating to numerous technologies. These include Microsoft, Oracle, Java and more.

Big or small, we can help with your Cloud Software project in whatever capacity you require.

Features

- Tailored solutions
- Best practice
- Enterprise architecture
- Agile methodology and Scrum
- Microservices
- Microsoft
- Full software development lifecycle
- Rapid Application Development
- Continuous Integration and Delivery (DevOps)
- Secure services

Benefits

- Improved efficiencies
- Drive down costs
- Integrate multiple systems and data sets
- Increased productivity
- Customer and requirement-specific solutions
- Harness industry best practice
- Surface the value of your data

Contact

Monitor IS
Jody Reynolds
01793 441414
jody.reynolds@monitoris.co.uk

Service scope

Software add-on or extension

No

Cloud deployment model

- Public cloud
- Private cloud
- Hybrid cloud

Service constraints

NA

System requirements

Appropriate software licenses as required

User support

Email or online ticketing support

Email or online ticketing

Support response times

Variety of support options available.

User can manage status and priority of support tickets

Yes

Online ticketing support accessibility

None or don’t know

Phone support

Yes

Phone support availability

9 to 5 (UK time), Monday to Friday

Web chat support

No

Onsite support

Onsite support

Support levels

Bronze, Silver, Gold and Custom Support Levels are available, charged at the most cost-effective rate for the client and project specific requirement. Our Account Managers will work with you to understand the most suitable Support Level for your needs.

All support levels allow access to expertise from highly qualified and experienced cloud support engineers ensuring the value you derive from the services provide remains as high as possible at all times.

Support available to third parties

Yes

Onboarding and offboarding

Getting started

A host of training options are available both on and off-site. Our Account Managers will work with you to discover the best options for your organisation and your team.

Service documentation

Yes

Documentation formats

- HTML
- PDF

End-of-contract data extraction

Our Cloud Software Engineers will work with you to extract any data in a suitable format for your requirements.

End-of-contract process

The full details of the in-scope services will be agreed at the beginning of the engagement. To fully support your changing requirements, the services is entirely flexible over time. Features or services which attract an additional cost will be clearly communicated by the Account Manager.

Using the service

Web browser interface

Yes

Supported browsers

- Microsoft Edge
- Firefox
- Chrome
- Safari
- Opera

Application to install

No

Designed for use on mobile devices

Yes

Differences between the mobile and desktop service

Completely responsive design means that the user experience is optimised but unaltered on mobile and other devices with a smaller screen size.

Service interface

No

API

Yes

What users can and can't do using the API

Support for and development of cloud API's (REST, SOAP etc.) is provided on a bespoke basis by our experienced cloud software engineers.

API documentation

No

API sandbox or test environment

No

Customisation available

Yes

Description of customisation

We offer a completely flexible service which adapts to your changing requirements over time, enabling it to be flexed up and down in response to changing business need.

Our Account Managers will work with you and keep in constant touch to ensure you are getting the most appropriate service for your requirement.

Scaling

Independence of resources

Independent resources will be assigned to your requirements, ensuring that demand by other customers will not impact your services.

Analytics

Service usage metrics

Yes

Metrics types

Periodic breakdown of service usage is available e.g. on a monthly basis or other period as required.

Reporting types

- Regular reports
- Reports on request

Resellers

Supplier type

Not a reseller

Staff security

Staff security clearance

Other security clearance

Government security clearance

Up to Developed Vetting (DV)

Asset protection

Knowledge of data storage and processing locations

Yes

Data storage and processing locations

United Kingdom

User control over data storage and processing locations

Yes

Datacentre security standards

Managed by a third party

Penetration testing frequency

At least once a year

Penetration testing approach

Another external penetration testing organisation

Protecting data at rest

Physical access control, complying with SSAE-16 / ISAE 3402

Data sanitisation process

No

Equipment disposal approach

In-house destruction process

Data importing and exporting

Data export approach

A number of options are available using common formats. Your Account Manager and Cloud Software Engineers will work with you to discuss the most appropriate solution for your specific requirements.

Data export formats

- CSV
- Other

Other data export formats

Other formats available in discussion with our Cloud Software Engineers

Data import formats

CSV

Data-in-transit protection

Data protection between buyer and supplier networks

- Private network or public sector network
- TLS (version 1.2 or above)

Data protection within supplier network

TLS (version 1.2 or above)

Availability and resilience

Guaranteed availability

Your Account Manager will work with you to form an SLA which meets your specific requirements, guaranteeing you the level of service you require. This will include appropriate schemes of recompense for any SLA conditions not met.

Approach to resilience

Available on request.

Outage reporting

Email alerts, dashboards and more can be configured by our expert Cloud Software Engineers depending on your and your project's specific requirements.

Identity and authentication

User authentication needed

Yes

User authentication

- 2-factor authentication
- Identity federation with existing provider (for example Google Apps)
- Limited access network (for example PSN)
- Username or password

Access restrictions in management interfaces and support channels

Robust Access Control and authorisation mechanisms are in place to ensure only correctly-privileged users gain access to protected interfaces and channels.

Access restriction testing frequency

At least once a year

Management access authentication

- 2-factor authentication
- Username or password

Audit information for users

Access to user activity audit information

Users contact the support team to get audit information

How long user audit data is stored for

At least 12 months

Access to supplier activity audit information

Users contact the support team to get audit information

How long supplier audit data is stored for

At least 12 months

How long system logs are stored for

User-defined

Standards and certifications

ISO/IEC 27001, ISO 14001, ISO 9001, ISO 20000-1 certification

Yes

Security governance

Named board-level person responsible for service security

Yes

Security governance certified

No

Security governance approach

Our CTO (Chief Technical Officer) has overall responsibility for the security of the services provided.

We have a framework for security governance, with policies governing the core aspects of information security relevant to the services provided.

Security matters are considered of the highest importance by the organisation with any issues relating to security or information security being immediately reported to the board of directors.

Constant monitoring of service provision to ensure conformance with all relevant legal and regulatory requirements.

Information security policies and processes

The CTO (Chief Technical Officer) takes overall responsibility for for security and information security. All security and information security matters are reported directly to him and the board of directors. He takes responsibility for ensuring that all security policies are followed and reports to the board on the status of the same.

Operational security

Configuration and change management standard

Supplier-defined controls

Configuration and change management approach

We operate in accordance with a Change Management Plan, documenting how changes will be monitored and controlled. This plan defines the process for managing change on the service.

In addition, we work in accordance with a Configuration Management plan documenting how configuration management is undertaken. It defines those items that are configurable, those that require formal change control, and the process for controlling changes to such items.

A security assessment is undertaken as a fundamental part of any change.

Vulnerability management type

Undisclosed

Vulnerability management approach

We frequently work in conjunction with specialist third party penetration testers to identify threats.

Services under our control are patched as soon as practicable after the release of a relevant update.

Protective monitoring type

Undisclosed

Protective monitoring approach

* Monitoring of access logs.
* Potential compromises are investigated immediately and an appropriate action plan put in place.
* Incidents are responded to as quickly as practicable with significant incidents being given the highest possible priority.

Incident management type

Undisclosed

Incident management approach

We undertake Incident Management in line with ITIL best practice, aiming to restore normal operation of services as rapidly as possible.
Users can report incidents via email, phone or via their Account Manager. Incidents will be dealt with by experienced Cloud Software Engineers.
Incident Reports are provided periodically or as requested.

Secure development

Approach to secure software development best practice

Supplier-defined process

Public sector networks

Connection to public sector networks

No

Pricing

Discount for educational organisations

No

Free trial available

No