

• Service name

Service name

- TRUSTMARQUE SNOW ITAM SOFTWARE HOSTED AS A SERVICE

• About your service

Service description

- Trustmarque's hosted Snow Software Service is designed to help customers manage their software estates more efficiently/save money, and mitigate risk. As the Public Sector transitions towards consumption cloud ICT, traditional software assets will need to be managed as digital assets, making Trustmarque's Snow Software Service continuously relevant in maintaining assets.

Service categories

- Information and communications technology (ICT)
 - IT asset management
 - Licence management

Multi cloud support

- Yes

• Service features and benefits

Service features and benefits

Service features

- Market leading IT Asset Management technology in Snow Licence Manager
- Software Asset Management
- Hardware Asset Management
- Software Licence Management
- Software Metering
- Cost avoidance
- Cost Savings
- Hosted with automatic updates
- Service Levels

Service benefits

- Have access to experienced SAM consultants to augment/improve the team
- Achieve significant cost reduction
- Improve control of software assets
- Reduce risk through improved visibility of the software estate
- Ensure minimal impact on existing resource and infrastructure
- Identify Software Usage
- Resilient and secure
- Easy to maintain

• **Service scope**

Add-ons and extensions

Software add-on or extension

- No

Cloud deployment model

- Public cloud
- Private cloud
- Community cloud
- Hybrid cloud

Service constraints

- Hosting on Microsoft Azure is an additional cost and needs to be scoped for the customers unique requirements.

System requirements

- Azure hosting through Trustmarque

• **Reselling**

Supplier type

Supplier type

- I'm a reseller providing extra features and support not available from the original supplier

Organisation whose services are being resold

- Snow Software

. User support

Email or ticketing support

Email or online ticketing support

- Yes

Support response times

- Subject to an agreed SLA

User can manage status and priority of support tickets

- Yes

Online ticketing support accessibility

- WCAG 2.1 AA or EN 301 549

Phone support

Phone support

- Yes

Phone support availability

- 24 hours, 7 days a week

Web chat support

Web chat support

- Yes

Web chat support availability

- 24 hours, 7 days a week

Web chat support accessibility standard

- WCAG 2.1 AA or EN 301 549

Web chat accessibility testing

- None.

Onsite support

- Yes, at extra cost

Support levels

- User support is provided by Snow technical experts and the customer will have access to consultants for telephone and onsite support where required.

Support available to third parties

- No

• How users work with your service

Browsers

Web browser interface

- Yes

Supported browsers

- Internet Explorer 11
- Microsoft Edge
- Firefox
- Chrome

Installation

Application to install

- Yes

Compatible operating systems

- Linux or Unix
- macOS
- Windows
- Other

Mobile

Designed for use on mobile devices

- Yes

Differences between the mobile and desktop service

- Different asset type

Service interface

Service interface

- No

User support

User support accessibility

- None or don't know

API

API

- Yes

What users can and can't do using the API

- Snow utilises REST API

API documentation

- Yes

API documentation formats

- Other

API sandbox or test environment

- Yes

Customisation

Customisation available

- Yes

Description of customisation

- Customisation is available to import custom data into the platform

. Onboarding and offboarding

Getting started

- User training is available, delivered by Snow Software. Trustmarque also offer Knowledge Transfer sessions onsite with the customer.

Documentation

Service documentation

- Yes

Documentation formats

- HTML

Documentation accessibility standard

- WCAG 2.1 AA or EN 301 549

End-of-contract data extraction

- Data can be exported from the software by the customer or be provided by Trustmarque at an additional agreed cost.

End-of-contract process

- Snow Software Service Provider licensing only.

• Data importing and exporting

Data export approach

- Users use in built reporting functions to export the required data.

Data export formats

Data export formats

- CSV
- ODF
- Other

Other data export formats

- XLS
- PDF
- XML

Data import formats

Data import formats

- CSV
- ODF
- Other

Other data import formats

- XLS
- XML

• Analytics

Metrics

Service usage metrics

- No

• **Scaling**

Independence of resources

- Single tenant cloud based systems provide customer isolation

• **Public sector networks**

Public sector networks

Connection to public sector networks

- No

• **Data-in-transit protection**

Protection between networks

Data protection between buyer and supplier networks

- Legacy SSL and TLS (under 1.2)

Protection within your network

Data protection within supplier network

- Legacy SSL and TLS (under 1.2)

• **Asset protection**

Data storage and processing locations

Knowledge of data storage and processing locations

- Yes

Data storage and processing locations

- United Kingdom
- European Economic Area (EEA)

User control over data storage and processing locations

- Yes

Datacentre security standards

- Complies with a recognised standard, for example CSA CCM v3.0 or SSAE-16 / ISAE 3402

Penetration testing

Penetration testing frequency

- At least once a year

Penetration testing approach

- Another external penetration testing organisation

Protection of data at rest

Protecting data at rest

- Other

Other data at rest protection approach

- Encryption of raw data

Data sanitisation process

Data sanitisation process

- No

Equipment disposal approach

- A third-party destruction service

. Availability and resilience

Guaranteed availability

- 99.90%

Approach to resilience

- Information available on request.

Outage reporting

- Notified by Service Desk / Auto Alert notifications.

. Governance

Named board-level person responsible for service security

- Yes

Security governance

Security governance certified

- Yes
- Security governance standards
- ISO/IEC 27001

Information security policies and processes

- Please engage Trustmarque for full details of our approach to Security Governance and Policies.

. Operational security

Configuration and change management standard

- Conforms to a recognised standard, for example CSA CCM v3.0 or SSAE-16 / ISAE 3402

Configuration and change management approach

- Please engage Trustmarque for full details of our approach to Security Governance and Policies.

Vulnerability management type

- Conforms to a recognised standard, for example CSA CCM v3.0 or SSAE-16 / ISAE 3402

Vulnerability management approach

- Please engage with Trustmarque for full details of our Vulnerability Management processes.

Protective monitoring type

- Conforms to a recognised standard, for example CSA CCM v3.0 or SSAE-16 / ISAE 3402

Protective monitoring approach

- Please engage with Trustmarque for full details of our Protective Monitoring process.

Incident management type

- Conforms to a recognised standard, for example, CSA CCM v3.0 or ISO/IEC 27035:2011 or SSAE-16 / ISAE 3402

Incident management approach

- Please engage with Trustmarque for full details of our Incident Management Process.

. Staff security

Staff security clearance

- Staff screening performed but doesn't conform with BS7858:2019

Government security clearance

- Up to Developed Vetting (DV)

. Secure development

Approach to secure software development best practice

- Independent review of processes (for example CESG CPA Build Standard, ISO/IEC 27034, ISO/IEC 27001 or CSA CCM v3.0)

. Identity and authentication

User authentication

User authentication needed

- Yes

User authentication

- Username or password

Access restrictions in management interfaces and support channels

- No customer access to management interfaces

Access restriction testing frequency

- At least once a year

Management access

Management access authentication

- Username or password

. Audit information for users

Audit for buyers' users' actions

Access to user activity audit information

- Users have access to real-time audit information

How long user audit data is stored for

- User-defined

Audit for suppliers' users' actions

Access to supplier activity audit information

- Users have access to real-time audit information

How long supplier audit data is stored for

- User-defined

How long system logs are stored for

- User-defined