Service Definition

Version 3.0
Date: 10th January, 2018

Tel: 01275 240500
Fax: 01275 240501
sales@simplisys.co.uk
www.simplisys.co.uk

Table of Contents

Tel: 01275 240500
Fax: 01275 240501
sales@simplisys.co.uk
www.simplisys.co.uk

Tel: 01275 240500
Fax: 01275 240501
sales@simplisys.co.uk
www.simplisys.co.uk

Background

Simplisys Service Desk is designed, developed and supplied by SimpliSys Ltd, a UK registered company based in Bristol specialising in Service Management and Service Delivery software. The company is ISO 9001 and ISO27001 registered, all solutions comply with the quality and security standards outlined in an Operating Procedures Manual authenticated by external auditors, CQS Ltd.

An Overview of the Simplisys offering

Simplisys has been designed from the ground up with the Hosted platform at its core. Careful design consideration has been given to the four key areas of Security, Performance, Capacity and Redundancy. These areas are supported by the Application design, Infrastructure design and the Processes used.

Simplisys Service Desk provides a cloud based ITIL aligned service management solution, highly configurable but with an intuitive interface.

- Incident, Problem and Change processes integrated with CMDB, Services and End User details
- Configurable Customer portal.
- Comprehensive suite of standard reports, including report generator allowing custom reports to be created.
- Integration with Active Directory and Customer Email infrastructure
- Dynamic knowledge management, selectively available to analysts and End Users.
- Business rules processing configurable via an intuitive interface – Automation with no programing skills required.
- Work Flows. Underpin your working practices – Drag and Drop design and maintenance.

Frequent releases ensure that updates and enhancements are available to users to enable them to take advantage of new features quickly. Along with the quick start package and two levels of functionality, Professional and Enterprise, this enables users to be productive from day 1.

- Quick start Package covering common setup and configuration tasks.
- Functionality tailored to your needs, If you do not use Change or Problem management our Professional edition is for you

Security

Security is supported at every level of the platform architecture from the external connections through to the SaaS infrastructure, application and database. Within the application architecture, there are several levels which all support the security of the application.

Tel: 01275 240500
Fax: 01275 240501
sales@simplisys.co.uk
www.simplisys.co.uk

Connections

All connections to the platform are via a secure connection supported by SSL encryption. This includes all user interface connections and as well as any components which may be installed on the customer network which will connect to the hosted platform. This includes Active Directory synchronisation, Email integration, integration with other systems and any use of the API. All of these integration options may connect to an external interface either directly from the hosted

platform or from within the customer network and so any such connections do not have to be exposed to the internet other than via the secure connection back to the hosted platform. This also means that the external interfaces can remain internal to the customer network and do not need to be internet facing.

Authentication

The security of username and password authentication in Simplisys is supported in a number of ways.

Passwords are NOT stored in plain text but use a non-reversible encryption technique including the use of individual 'Salts'. When SSL connections are used passwords are never transferred either externally or internally in plain text. Additional authentication is required between the tiers within the application ensuring that only authorised systems are able to access the database.

User passwords will not become visible to any person including any user with administrative permissions to the database nor to any individual which may have access to reporting information or database access. This includes customer personnel, reseller personnel and Simplisys personnel. Self Service passwords are covered by the same rules as the main application passwords.

When using windows authentication on the hosted platform, a component is required to be installed on the customer network. The windows infrastructure on the customer network will then handle the basic authentication of each user. Specific details of the user which is to access the application is then passed to the hosted application via a secure web connection from the onsite component. The onsite component is then given an authentication key which is then passed back to the client pc to be submitted by the user's browser. This authentication key is temporary and is invalidated after its first use or after a short time period if it is not used.

Database Security

The database is not available on the platform DMZ and is not available via direct remote connection. Access to the data in the database must go via the application or API and so always includes the application controls on permissions.

The database connection between the application and the database uses a database user account which only has access to the customer database being accessed. The user account does not have any permission for any of the other customer databases available on the hosted platform. This means that if an attacker ever managed to get past the other layers of

Tel: 01275 240500
Fax: 01275 240501
sales@simplisys.co.uk
www.simplisys.co.uk

security and compromise the database from within the web interface to the application, they would still be limited to data from their own database and not any other customer databases.

General Application Security Features

- When error messages are displayed, no technical information about the inner workings of the application is displayed.
- After logout, a user's session is completely invalidated and removes access to all system resources.
- A user may not bypass the permissions allowed by their role using direct modification of the URL.
- All data entry fields are protected from various types of injection attacks.

General Infrastructure Security Features

- Only components of the application which should allow direct connections are available on the DMZ.
- All infrastructure is behind a firewall.
- Windows Updates are kept up to date.
- Frequent Virus scans with McAfee anti-Virus.
- Annual Server Security Audit and monthly vulnerability scans.

Data Centre Security

Our data centres operational business infrastructure is compliant to the PCI DSS, which is a worldwide security standard assembled by the Payment Card Industry Security Standards Council (PCI SSC) and BS27001. Security features of the data centre include the following:

- 24 hour onsite security personnel
- CCTV security systems
- Cage and entry door access control
- All security systems constantly monitored

Security Review

Security reviews are to be carried out as and when significant changes have been made to the platform or in reaction to security related incidents. This will include penetration testing, a review of security related incidents, a review of technical logs and any additional information gained by technical personnel. The aim of the review is to identify any weaknesses in the security of the platform and any potential threat areas and to make recommendations to improve the security of the platform.

Security related processes will also be reviewed annually along with all other processes as part of our ISO 9001 / ISO 27001 certification requirements.

Tel: 01275 240500
Fax: 01275 240501
sales@simplisys.co.uk
www.simplisys.co.uk

Performance & Capacity

Infrastructure

Careful consideration has been given to the performance and capacity of the hosted platform in the design of the server architecture. Load balancing on the web front end ensures that no individual server becomes overloaded. The database servers gain similar benefits with a SQL cluster configuration. For areas of the application where heavy processing may take place, components are installed on servers separately to the web and database servers e.g. reporting. This ensures that spikes in the use of these features e.g. end of month reporting, does not affect the operation of the rest of the application.

Scalability

The architecture of the server environment means that additional servers can be added easily as the user base grows. Servers may be added to the infrastructure which increases the capacity of the overall platform.

Load Times & Data Volume

The table below shows the target load times for pages in the application. The target figures represent the desired outcome during general performance testing of the application. Where these targets are not met we will aim to make improvements to the application or infrastructure until the target figures are met.

The incident threshold figures show the minimum load times which will be considered to be an incident when performance issues are reported by a customer. To ensure that performance issues are not caused by customer's local network performance, a performance incident will only be accepted if the reported results can be verified by a technical support analyst from outside the customer network.

Target Load Times

Access Type	Target (s)	Incident threshold (s)
Updates to a page which is already loaded	0.1	2.5
Loading a new page, dialogue box or tab	1	5
Generating a standard system report	4	10
Performing a simple free text search	3	N/A
Bulk record updates	4	10
Loading a system dashboard with standard content	2	10

Tel: 01275 240500
Fax: 01275 240501
sales@simplisys.co.uk
www.simplisys.co.uk

File uploads, API Calls, custom reports, custom dashboards and complex searches	N/A	N/A

Data Volume

Record type	Volume
Task	100,000
Incident, Problem	50,000
Change	20,000

Application Performance and Capacity

The data access layer of the application has been designed with a number of efficiencies to keep a high level of performance in the application. A caching system has been developed whereby information which is not frequently updated is stored on the web server and so requests for this data are significantly faster.

Monitoring & Maintenance

Infrastructure & Application Monitoring

The infrastructure is continuously monitored at a number of levels. This monitoring includes server availability, Server Load and performance, and application availability.

Server Availability

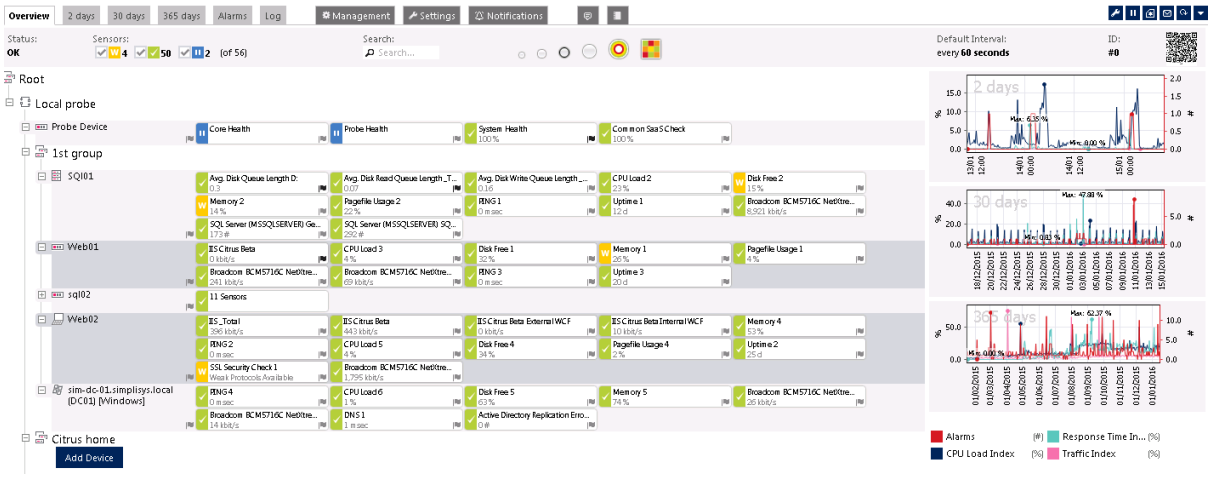
The servers are monitored for availability by a distributed monitoring infrastructure internal to the hosting, data centre environment. This monitoring is active 24/7 and will alert the on call Simplisys Infrastructure staff via email and SMS messages should any of the servers fail to respond. Additionally a ticket alert will automatically be sent to on site data centre staff informing them of the failure condition.

Server Load and performance

Each server within the Simplisys infrastructure is monitored 24/7 by state of the art network monitoring software. This system will monitor whole application stack monitoring and recording Operating system and application level sensors.

Abnormal conditions are alerted to Simplisys staff via wall board displays and alert conditions automatically generating an ‘event’ ticket within the Simplisys Service Desk application used by Simplisys staff.

Tel: 01275 240500
Fax: 01275 240501
sales@simplisys.co.uk
www.simplisys.co.uk



Trend Analysis

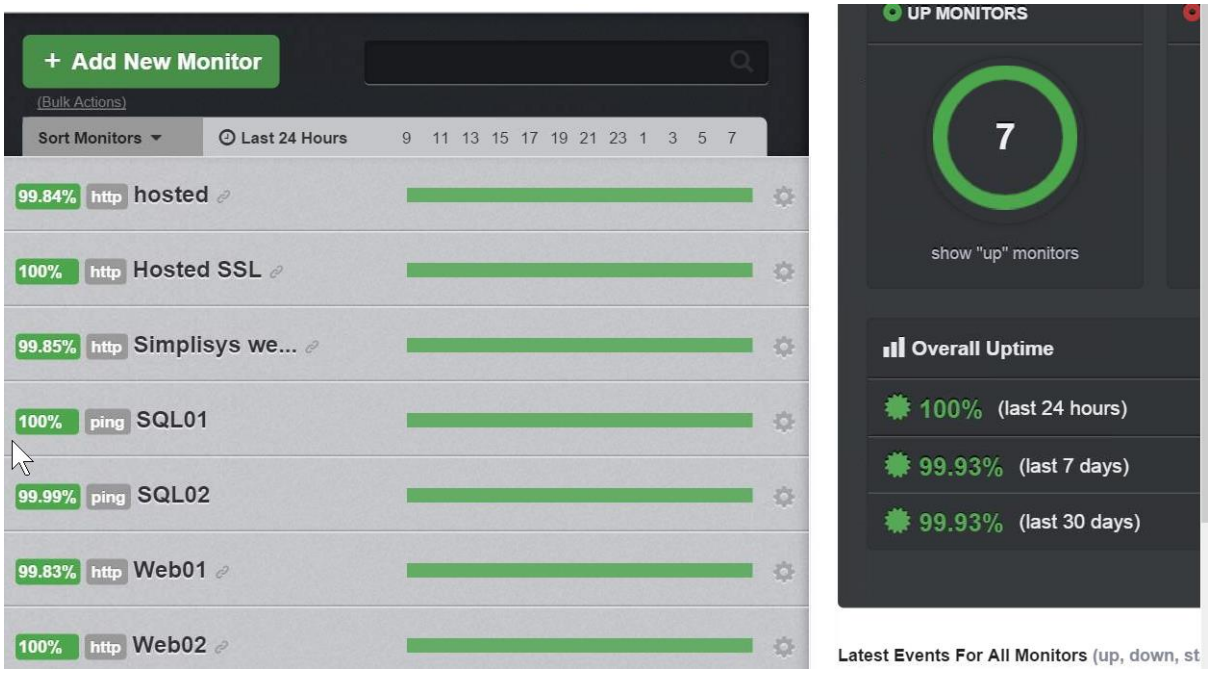
Data from the infrastructure monitoring is recorded and used to provide trend analysis information. This information allows Simplisys Infrastructure staff to proactively predict capacity and performance bottle necks and initiate preventative actions.

Application Availability Monitoring.

The availability of the application is monitored 24/7 via a monitoring platform external to the Simplisys infrastructure and Datacentre environment. This mimics the ‘Customer’ experience in accessing the application over the public internet.

Abnormal conditions are alerted to Simplisys staff via wall board displays and alert conditions automatically generating an ‘event’ ticket within the Simplisys Service Desk application used by Simplisys staff.

Tel: 01275 240500
Fax: 01275 240501
sales@simplisys.co.uk
www.simplisys.co.uk



Infrastructure Maintenance.

Scheduled Maintenance includes Operating system and application patching, Server housekeeping activities such as disk defragmentation and application level maintenance such as database index rebuilds and Statistics refreshes. This maintenance is carried out on a rolling monthly schedule designed to ensure that application availability is maintained.

Patching Policy

The patching policy defined in the Simplisys Security policy

Maintenance Schedule

The system maintenance schedule defined in the Simplisys Security policy

Redundancy & Availability

Power

The total power serving to our data centres is 2MVa. The facilities are also fully equipped with redundant power provided via 3 10000kva, 48 hour bundled diesel generators and full UPS power provided.

Using only industrial grade UPS power, the devices utilise battery power that is stored in a separate cooled plant room on the ground floor with their own fire suppression system and cooling units. Under full load the batteries can last around 5-7 minutes to give the generators time to start up and providing enough time for several failed generator starts.

The UPS' and generators are fully maintained and regularly start-up and failover tested to ensure the highest levels of availability and minimal downtime.

Fire suppression

There are 3 separate systems installed in our data centre. They are located throughout the suites and plant room. The data centre is equipped with NOVEC1230 gaseous based suppression systems using world class VESDA (Very Early Smoke Detection) and alarm systems.

This is in contrast to using older inert based systems, which drop the level of oxygen to around 15% at which most combustible materials cannot burn, whereas the NOVEC systems absorb the heat rapidly.

Network Redundancy

The network connection from the hosted platform to the internet utilises multiple ISP's, where fibre optic lines connect directly to our data centres and are failed over seamlessly. Our data centre providers reliable peering strategy combined with state of the art Cisco and Juniper hardware ensures a network with no single point of failure.

Our data centres are connected to London via two 1GB rings with another dark fibre ring connecting five data centres around London itself. This means that, in the unlikely event that any one data centre goes offline there will always be an alternate route which can be utilised to avoid any downtime or disruption.

The data centre has eight transit links into London from seven different clients including: AboveNet, Telia, Verion, Global Crossing, Level 3 and Tiscali. Each and every one of these clients has been selected for their global reach and reliability.

Server Architecture

The load balancing configuration means that in the event of a failure to a web server, another available web server will take over a user's session meaning that a user will continue to access the application without even being aware of the failure. The database server configuration also means that the application can continue to run even if a database server goes offline.

Data Centre SLA's

In the event of any failure to the infrastructure, we will work closely with our data centre provider to ensure that normal service operation is restored as quickly as possible. This is supported by the SLA's we have with our data centre provider.

- 100% network availability
- 15 minute rapid response promise
- 24/7 reboot guarantee
- 1 hour hardware replacement guarantee
- 24/7 emergency support
- Calls answered in 3 rings Level 3 qualified support engineers

Tel: 01275 240500
Fax: 01275 240501
sales@simplisys.co.uk
www.simplisys.co.uk

Monitoring

The platform is configured with Proactive Uptime monitoring of its servers. This ensures that not only is the server online and available but also that it is still able to serve web requests to the user base.

Planned Updates

We take the stability of the live platform very seriously and so any updates to the platform are made in a controlled way. Updates are planned well in advance so that we are able to make all necessary arrangements to ensure a smooth update and so that customers can prepare for any possible disruption. Updates will always be carried out with the minimum possible disruption to the service and the amount of disruption will depend on the nature of the update.

For updates which require changes to application files, this will not usually involve any downtime but will sometimes require active users to log back into the application. For updates which require database changes, this will usually involve a small amount of downtime for each database while it is going through the update. This downtime will usually be around 10 minutes. For updates which require changes to the server operating system, this will often require a server restart. Due to the load balancing and database server configuration, this will usually result in no downtime to the application.

On rare occasions we may decide to schedule some prolonged downtime e.g. to carry out penetration or load testing on the platform. On these occasions, customers will be notified well in advance. Also on rare occasions, we may need to carry out an emergency update. On these occasions we will notify customers as soon as we know that an emergency update is required and if possible we will schedule it for a time which is the least disruptive to most customers.

Updates will be tested before being made to the live environment and if we are not completely happy with the test results than we may decide to postpone the update. Maintaining the stability of the live platform will be given priority over the release of normal bug fixes, planned enhancements and server operating system updates. Non-emergency updates will always be carried out during the standard maintenance window on a Sunday.

Changes to the application will usually be rolled up into releases containing several changes and deployed to the hosted platform infrequently. This will minimise the disruption to the hosted environment and allow suitable periods of stability. The hosted platform will have two installations of Simplisys running: a stable version and a beta version. All releases will first be deployed to the beta installation for a suitable period of time before being deployed on the stable version.

Simplisys Helpdesk - Architecture

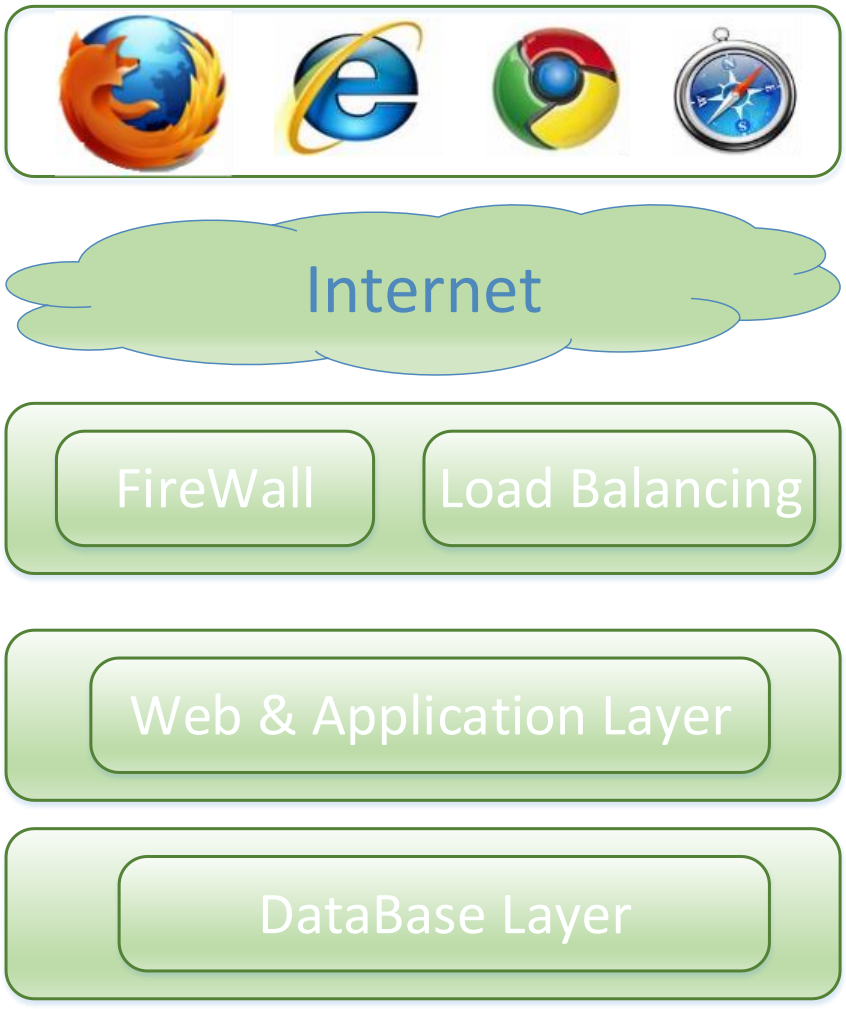
Simplisys Service Desk is a multi-layered architecture (see figure below), comprising a Microsoft stack (IIS, .Net and SQL Server database. The Application server provides a number of enablers:

Tel: 01275 240500
Fax: 01275 240501
sales@simplisys.co.uk
www.simplisys.co.uk

- Service level management, escalation, notification, email, connectivity, enterprise integration
- Sophisticated yet user-friendly graphically-driven workflow automation engine

Each Simplisys Service desk instance has its own database, so it is not possible for one customer to see or have access to another customer's data. **Simplisys** instances are security hardened as standard and locked down so that only a select number of the Simplisys cloud team, who are security trained, are able to remote desktop to the cloud servers.

Your **Simplisys** instance is accessible via the internet and can be connected to via most industry standard web browsers across most platforms.



Customers have Web Self Service included in their **Simplisys** offering; this is purely web-based. The appearance of web Self Service can be adapted to align with your particular branding; for example, inclusion of a corporate logo and adoption of corporate colours.

Technical Requirements

Simplisys Service Desk has a very low footprint within your organisation just requiring:

- A browser, namely IE 9-11, Edge, Firefox, Chrome, Safari (MAC)

- An internet connected device such as PC, Mac, IPad or Android Tablet

For more advanced integration services

- TCP/IP over ports 80 (http) and 443 (https) for user connectivity and 25 (smtp) and 110 (POP3) for email integration if required
- A mail server supporting SMTP and POP3(s)– optional as Simplisys can host email
- Microsoft AD for password authentication via LDAP(s) (optional)

Data Security & Backups

This policy has been designed for disaster recovery/business continuity (i.e. the ability to recover recent live data in the event of a partial or total loss of data) as key deliverable and is not therefore designed as a method of archiving material for extended periods of time.
The 'data' backups cover all data logged in Simplisys Service Desk application managed by Simplisys Ltd at its managed service data centre… Data held and managed in companies where Simplisys Service Desk is installed locally is excluded from this policy.

See the Simplisys Backup Policy for details of the Backup Policy.

Tel: 01275 240500
Fax: 01275 240501
sales@simplisys.co.uk
www.simplisys.co.uk

Contacting the Simplisys Helpdesk

Customers requiring support should call the Simplisys Helpdesk as below:

By Email: support@simplisys.co.uk
By Fax: 01275 240501

By Post: Simplisys Ltd,
Top Floor
42 High Street
Portishead
Bristol,
BS20 6EL
United Kingdom.

By Telephone: 01275 240500

Via Web Portal: www.simplisys.co.uk

Simplisys Helpdesk is closed for business outside normal office hours and on UK National & Public holidays, unless prior cover has been formally arranged.

See below for details about Simplisys Service Cover.

Priority Definitions and Turnaround Targets

Customers to indicate the impact of the incident related to their operation. Simplisys will then prioritise the urgency of the technical diagnosis and resolution turnaround. Simplisys will use best endeavours to meet the response target

'Service Levels' defined below.

- 'Response Target' is defined as the mean time to the first 'useful contact'.
- 'Workaround Target' is the time to the first available feasible solution.
- 'Resolution Target' is the time to the first available solution.

Customer Priority	Response	Workaround	Resolution	Contact / Action
1-Urgent Product operation unusable. High customer business procedure at risk. A time-critical service unavailable.	30 mins	2 hours	4 Hours	SIMPLISYS CARE Helpdesk Telephone/email initial response Hourly monitoring of progress Mandatory positive response required.
2-Major Product component/important facility unusable. Software/data files not accessible. Time-critical service schedule endangered.	30 mins	4 hours	16 Hours	SIMPLISYS CARE Helpdesk Telephone/Email initial response. Bi-daily monitoring of progress. Mandatory positive response required.
3-Default Level Product/component will not run/job impaired. Workaround to problem has been found	4 hours	1 day	5Days.	SIMPLISYS CARE Helpdesk Daily monitoring of progress Telephone/Email response.
4-Not to Spec Product will not run as documented but issue is not critical – Bug Fix	1 day	2 days	Next release.	SIMPLISYS CARE Helpdesk Weekly monitoring of progress Telephone/Email response.
5-Not Clear Non-critical issues. E.g.; Documentation Errors, Usability suggestions, etc.	1 day	5 days	No SLA	SIMPLISYS CARE Helpdesk Weekly monitoring of progress Telephone/Email response.

Simplisys Service Cover

Tel: 01275 240500
Fax: 01275 240501
sales@simplisys.co.uk
www.simplisys.co.uk

Simplisys can provide service-cover to meet a customer's support needs and this is defined within the contracted 'Service Maintenance Agreement' outlined below: -.

'Standard Service-Cover' [5 x 9 hours]	08:30 to 17:30 hours Monday to Friday	Excludes all public holidays and week-ends
'Extended Service-Cover' [5 x 14 hours]	08:30 to 22:00 hours Monday to Friday	Excludes all public holidays and week-ends
'Premier Service-Cover' [7 x 8 hours]	8:30 to 17:30 hours Saturday, Sunday and all UK public holidays	Excludes Christmas Day and Boxing Day
'Bespoke Service Cover'	Up to 7 x 24 as required.	To be agreed

Privacy Policy

What this policy covers

Simplisys Service Desk ("we", "us" or "our") is committed to ensuring that your privacy is protected (and in this policy, "you" and "your" includes your employees and consultants if applicable and where such persons are authorised users of our services). This privacy policy explains how we use the information we collect about you, how you can instruct us if you prefer to limit the use of that information and the procedures that we have in place to safeguard your privacy.

Under the Data Protection Act 1998 we must comply with certain regulations which are designed to ensure that any data you provide to us is processed with due care and attention.

Your consent

By submitting your data you consent to the use of that data as set out in this policy. If you do not agree to our processing of your data as set out below, please do not submit any personal data to us.

If we change our privacy policy we will post the changes on this page, and may place notices on other pages of the website. If we make any substantial changes we may provide you with email notification. Continued use of the service will signify that you agree to any such changes.

Tel: 01275 240500
Fax: 01275 240501
sales@simplisys.co.uk
www.simplisys.co.uk

The information we collect and how we use it

We collect data about you, both personal data such as your name and contact details, and sensitive personal data. The relevant personal data may then be processed, used and disclosed by us in the following ways:

- to enhance the services which we provide to you;
- to communicate with you on any matter relating to the provision of our services and to answer your questions and enquiries;
- to market our range of services to you;
- to disclose to regulatory and law enforcement agencies if we believe in good faith that we are required by law to disclose it in connection with the detection of crime or in order to comply with any law or any order of a court of competent jurisdiction, or in connection with any legal proceedings.
- to disclose to third parties, on a confidential basis, where we have retained them to provide services that you have requested in writing, or verification of the details you have provided from a third party source;

From time to time we may seek your consent to process, use or disclose your information for any other purpose not listed above. We will, however, keep your information confidential except where we disclose it as set out above and subject to the below paragraph.

Information provided about employees and consultants

You undertake that any data or other information which you provide about your employees or consultants (if applicable) is accurate and not misleading, that in each case you have obtained informed consent from each employee or consultant (as the case may be) to use their personal data for the purposes listed above, and that each employee or consultant (as the case may be) is aware of the existence and location of this privacy policy.

How we protect your information

The Internet is not a secure medium. We have put in place various procedures including firewalls and limited access backed by passwords as appropriate. Due to the nature of the internet, however, we cannot guarantee the security of any information you transmit to us via the internet.

How long will your information be held for?

We will hold your information for as long as is necessary to comply with our contractual and statutory obligations and in accordance with our lawful interests as a data controller.

Tel: 01275 240500
Fax: 01275 240501
sales@simplisys.co.uk
www.simplisys.co.uk

Can you find out what information we hold? Can you amend such information or require it to be deleted?

You may at any time request us to confirm data we hold about you and may request us to amend, delete or update such data. We may ask you to verify your identity and for more information about your request. If we are legally permitted to do so we may refuse your request but in such circumstances we will give you reasons for doing so. If you wish to contact us with respect to the above matters, please email us at enquiries@Simplisysservicedesk.com.

Sale of business

If Simplisys Service Desk is sold or integrated with another business your details may be disclosed to our professional advisers and will be passed on to the new owners of the business.

Tel: 01275 240500
Fax: 01275 240501
sales@simplisys.co.uk
www.simplisys.co.uk