Managed Ultimate Package Terms

The Managed Service Terms apply to these terms. In this Managed Package references to days and Business Hours means Mondays to Fridays 09.00 – 17.30, excluding Bank Holidays. The Managed Ultimate package is our top level package, bar some services you can add-on. If you need anything more, talk to us, we'll be happy to help.

Support and Maintenance

Support - What's In		
Service Components	**Our Responsibilities**	**Your Responsibilities**
60 day launch assistance	Uplifted support, debugging and deployment assistance during the first 60 days to help get you going faster.	Get your applications up and running quickly on the new environment so you can make full use of the first 60 days help.
Engineer assistance	Our specialist engineers are here to help you 24/7.	Call or email us up and ask us for help.
Security advice	We keep up to date with best practises, the latest security threats and monitor your system closely for intruders. We will notify you each time.	You must not circumvent, disable or otherwise change our security measures. Avoid uploading insecure code. Never reveal your passwords or even share them amongst your team. You should follow the advice we provide on how to improve your systems and implement it in the shortest time possible.
Future planning & architecture advice	We'll help you architect new systems or plan for future changes in your requirements. This means reviewing your requirements, making recommendations on how you can prepare now and planning those changes for you. We may sometimes charge an additional fee for complex projects where a lot of research is required on our part.	Tell us when you're planning something new, have a big project coming up or expect to have to scale up. The sooner we know the better, and it costs you nothing to talk to us about it.
Dev server management	We manage the development environment in the same way as we do your production. We will keep settings in sync between the two as much as possible.	To let us know if you make any changes to the development environment and if you do/do not want those copied to production.
Dedicated Pod / Team	We make a dedicated team available to you. The team will be allocated to you on sign up. All support requests will be	-

	routed through your team in the first instance.	
Monitoring	We monitor the critical system resources and the system state of servers in your production environment. We also monitor other services that make up your environment where possible. We will also monitor your application or websites uptime. We may also put basic uptime monitoring on your development environment.	You must tell us what endpoints / pages to monitor in your application (URL, ports and other special settings). You must also tell us how frequently you'd like these monitored and who to notify if we detect a problem.
Code	We help debug your applications if things aren't quite right using code level analysis. We also help identify database errors and slow downs. Specific DBA work is not included.	You will act on the information we provide you to improve the problem. If the same problem causes issues on the system 3 or more times, we'll stop notifying you about it. You must maintain adequate backups of your code in another location for extra safety.
Continuous Integration	We will manage and monitor any auto deployment or continuous integration pipelines you have. We will also help you set up new ones (although this may be chargeable).	You will ensure that your code can be deployed using these methods and that no data corruption or other problems result.
Management reports	Upon request by you, at the end of each month we will let you know what we've done that month, what your system uptime was, what issues we had and make any recommendations on how you can mitigate those issues in the future. Every 3-6 months we will review your environment and make additional recommendations on how to improve your systems.	Read the information we send you – it's important stuff. The security and reliability of your systems depends on it. You must make every effort to follow our recommendations – it will result in a better system for you and will mitigate your risk profile. If there is a technical reason why you cannot, please let us know.
Hardware	Where you have hardware in a rack that we look after, we'll physically replace components, upgrade the hardware, swap out blades and other replaceable parts, install firewalls, ups equipment and switching as well as replace hard drives and enclosures for SAN and other storage arrays.	You must pay for any upgrade or replacement parts and provide us with an ideal time to do the work. There must be enough space in left in your rack to complete the work. If the servers are in a datacentre that we don't have access to directly, you will make sure we can gain access at the agreed time by providing us with all

		codes, passes or keys as needed.
CMS Recipes	We provide tailored server setups for some CMS systems. These will be specifically configured to give the best performance for that CMS.	You must test your website or application works with the server recipe – sometimes code changes can mean we need to customise setups for you. You must tell us what CMS you want to use before we setup the server.
Management tools	N/A	Additional services on your servers such as caching, software firewalls, compilers and code obscurification plugins etc will need to be fully supported by your team alongside your application.
Network	We support your internal networking. This means firewalls, load balancers, internet connections, switches, security groups, gateways and IP addressing.	You must ensure we have access to the entire network, including giving us username/password credentials where needed.
Web Technologies	We support Apache, Ngnix, IIS, PHP and .NET technologies in your environment.	You must ensure that your code is compatible with versions of software installed on your server.
Database Technologies	We support MySQL, MariaDB, and MS SQL database technologies. We do not manage the data that you store in these databases. We will not fix data corruption or other issues that have been caused by the result of poor code. In these cases we will restore a backup copy of the data for you.	You must ensure your code is tested in a development environment before pushing it to the production environment - most data corruption issues are caused by poorly written code.
Mail Technologies	We'll provide debugging and support for POP, IMAP and SMTP technologies inside your environment. We cannot provide support for issues with mail where the issue occurs outside of our control.	You will not use these servers to send Spam or otherwise unsolicited mass email. You will keep your passwords secure at all times and make sure they are a mix of upper/lower case characters and a minimum of 12 characters in length.
Logs	Use logs and log aggregation data to quickly diagnose problems with your servers and network devices. We may insist on log aggregation software if you have a large	Allow us to send your logs to a 3rd party software provider. Pay the licensing for the third party log aggregation software.

	amount of devices producing log data.	
Chaos Monkey	A little inspiration from Netflix here. If you run a platform inside the AWS infrastructure we take a leaf out of Netflix's book and create real life simulations of infrastructure, network, server, etc failure. The purpose of this is to make sure that we identify any weak points in your platform.	You must tell us what we need to monitor (in monitoring above), what tolerances are acceptable and approve when we can run the tests.
Worldwide	We support worldwide platform replication, sync, management, and failover. This is ensuring your worldwide locations all work as if they were a single platform.	Ensure your application is able to handle worldwide replication and failover.

Maintenance – What's In		
Service Components	**Our Responsibilities**	**Your Responsibilities**
Monitoring	We monitor the critical system resources and the system state of servers in your production environment. We also monitor other services that make up your environment where possible. We will also monitor your application or websites uptime. We may also put basic uptime monitoring on your development environment.	You must tell us what endpoints / pages to monitor in your application (URL, ports and other special settings). You must also tell us how frequently you'd like these monitored and who to notify if we detect a problem.
Physical / Virtual Hardware	We will update, patch and maintain the Physical / Virtual Hardware in accordance with warranty and support agreements.	You will allow Us to carry out necessary work assuming a documented change process is followed.
Operating Systems	We will update, patch and maintain an installed supported Operating System. We will support all versions of Windows that are also supported by Microsoft and all versions of Linux Red Hat, Debian, CentOS, SuSe, Ubuntu, Fedora and CoreOS that are currently officially supported by them; excluding preview and beta versions.	You will allow Us to carry out necessary work assuming a documented change process is followed.
Backups	Where backup software is provided by Us as part of a managed service, We will ensure database, code and system backups run successfully in accordance with the agreed schedule and retention policy. We reserve the right to not support certain backup software at Our discretion. Where You are unsure of a backup strategy or software, We can make recommendations to You.	You will provide Us with Your required retention policy (a standard policy is available if You are unsure). You must ensure the backup software is suitable and compatible to backup your environment and data, and adhere to the recommendations We make.
SSL / Secure Certificates	Setup and maintenance of any secure certificates required by You on the Service(s) as agreed.	You will pay Us for, or supply, the appropriate level of SSL certificate for Your Service(s).
User Management	This means Creating, deleting and updating user details and	You will provide Us with a list of users and required permission levels during

	permissions as required by You.	onboarding and additionally notify Us of any changes to Your staffing or permissions.
Security	We will publish and follow a best practise for firewall rules, security settings and any specific setup required by Your Code or requested and approved by You.	You will provide Us with any exceptions in writing (such as IP whitelisting) that You require.
Service Resources	We will supply, manage and monitor the resources, such as power and network connectivity, that the provisioned Service(s) require to function.	You will allow Us to carry out necessary work assuming a documented change process is followed.
Network	We ensure your internal networking is online, operating efficiently and as secure as possible. This means firewalls, load balancers, internet connections, switches, security groups, gateways and IP addressing.	You must ensure we have access to the entire network, including giving us username/password credentials where needed.
Web Technologies	We'll ensure that Apache, Ngnix, IIS, PHP and .NET components are running and configured correctly. We update them on a regular schedule.	You will need to allow us time to perform the maintenance (ideally every month). If you don't have a resilient setup, this may mean downtime.
Database Technologies	We'll ensure that your MySQL, MariaDB and MS SQL database setups are as secure as possible using industry best practises. We also ensure they are running and configured correctly and update them on a regular schedule.	You will need to allow us time to perform the maintenance (ideally every month). If you don't have a resilient setup, this may mean downtime. You must also ensure you are accessing these databases in a secure way and do not reveal your connection details.
Mail Technologies	We'll ensure that your POP, IMAP and SMTP installations are as secure as possible using industry best practises. We update these services on a regular schedule.	You will need to allow us time to perform the maintenance (ideally every month). If you don't have a resilient setup, this may mean downtime.
Auto Scaling & Recovery	We manage auto scaling, monitoring, thresholds, recovery, server images and automatic repairs in the event of a fault in the cluster(s).	Your code, and specifically database, must be able to operate in an auto scaling environment.
Server Recipes	We'll manage, maintain and update Chef, Puppet, Docker and Ansible server recipes for you. This means rapid deployment and faster	You will ensure that your applications are compatible with these technologies.

	recovery. We may manage other similar systems if we agree in advance in writing.	

When will We carry out maintenance?

1. You may be notified of planned maintenance by Us in writing including by email, or any form of cloud based platform or tool which invites collaboration as specified by Us from time to time.
2. Where maintenance work requires interruption of the Service We shall try to work around Your business peak periods.
3. Planned work will take preference over unplanned work; if there is a resourcing conflict We will inform You as soon as possible and work with You on a revised date.
4. We perform Planned Maintenance during these times ("Standard Maintenance Hours") between the hours of 06:00 and 22:00 Weekdays excluding all Bank Holidays
5. Any Maintenance or work outside of Our Standard Maintenance Hours is charged separately to Your Managed Service, according to Our rates at the time. If You require regular work outside these times to suit Your business, We recommend taking Our Managed Ultimate plan, as it includes scheduled Maintenance work at any time of day.
6. We aim to complete critical patches within 1 calendar month and other patches within 2 calendar months.
7. If You prevent Us from completing maintenance (due to deferring, lack of approval or otherwise) and a fault or breach occurs as a result, We will not be held liable
8. Whilst We will use Our reasonable endeavours to minimise downtime; We cannot and do not warrant that the Services provided will be error free or without interruption. Unless otherwise expressly stated in the Relevant Product Terms We offer no service credits for any form of downtime or unavailability.
9. We do not warrant that all errors can and will be corrected. We shall endeavour to correct errors which We are contracted to try to fix so long as the errors are replicable by Us, or to provide a software patch or to bypass around such error.

Getting In Touch & Response Times

We will aim to respond in the following timescales

1. Should You determine that the Service(s) include a defect, a member of Your Team shall file error reports or support requests. We shall provide technical support services only to Your Team.
2. We shall accept voicemail, email and web form-based incident submittal, telephone calls (for English language telephone support) and notices via any web based collaborative tool (such as Slack) specified by Us from time to time, from Your Team 24 hours a day, seven days a week. (Out of hours calls may be handled by a third party who will request information from Your Team to validate the caller).
3. We shall use reasonable endeavours to process support requests, ticket tracking or incident numbers if necessary, and determine the source of the problem and respond to You. We shall endeavour to respond to all support requests from Your Team within the time periods specified below, according to priority. We shall determine the priority and category of any fault in accordance with the following tables:

		Call type (see Category table).		
		Incident	**Question**	**Task**
Priority (see Priority table)	**Urgent**	0-1 hours†	1-4 hours	1-4 hours
	High	1-4 hours	0-1 Days	1-2 Days
	Normal	0-1 Days	1-2 Days	2-3 Days
	Low	2-3 Days	2-3 Days	2-3 Days
†Outside of Business Hours urgent incident response is 0-2 hours.				

Priority	
Low	An incident which is not important to the day to day running of systems
Normal	An incident which has/may have an impact to systems, but doesn't stop You working
High	An incident which stops a person(s) working or affects a small group of users
Urgent	An incident that impacts a group/site or the business as a whole and is considered business critical

Category	
Incident	A technical issue which needs investigating
Question	A query or question about the Service or infrastructure
Task	Changes, improvements to the Service and/or infrastructure

Your Team

1. Within three days of the start of the Minimum Term You will need to give Us details of the members of the Team who You want Us to liaise with, in relation to the Managed Services ("Your Team").
2. You will need to fully complete a Permissions Sheet, which You must send to support@scholarwebservices.com or submit through Your account portal (https://portal.scholarwebservices.com). The Service(s) cannot commence, though the Minimum Term will, until We have this information from You.
3. You should give Us details of a minimum of two members of Your Team including one Primary and one Escalation contact.
4. By giving Us these details You are giving Us Your permission for Us to accept instructions from Your Team.
5. You must notify Us in writing of any changes to Your Team or changes to the Permissions Sheet or Roles to support@scholarwebservices.com.
6. You shall ensure that Your Team are appropriately qualified and experienced to liaise with Us and act on Your behalf for the matter in hand.

Roles (Permission Groups)

This section explains the Roles that people have associated with their Permissions Sheet (below). If You feel that a Role is too broad or too specific please let Us know and We'll make it better. To help You and Us, We will also provide reports of permission groups so that You can make sure that You are happy with the level of access Your staff have and You can correct that, in writing, to support@scholarwebservices.com

1. Service Admin (Senior Role)

Scope: Typically signs off contracts, costs and can make any changes to the service. The Service Admin can be the technical escalation point, if the technical escalation contact is not available.

2. Technical Admin (Senior Role)

Scope: Typically used as the senior technical point of contact for services and escalation point of contact for outages and technical issues/changes requiring sign off.

- Approve scheduled maintenance, shutdowns and restarts
- Approve new people additions, updates to permissions and roles (starters and leavers).
- Approve decommissioning or deletion of data, config changes etc.

Restrictions: Cannot sign or amend existing contracts, without prior agreement from the Service Admin.

3. Technical Points of Contacts

Scope: These are typically developers working internally or outsourced development teams, which we will be liaising with to manage your environments.

- Raise Support Tickets
- Work with to troubleshoot issues
- Make small config changes

Restrictions: Cannot order new services, make large changes to set-up or configuration without prior sign off from the Technical Admin.

4. Billing

Scope: This is for your accounts team and bookkeepers. They can view, download and pay invoices on our system. They cannot change contracts, payment terms or users.

- Access invoices

- Raise billing queries
- Pay invoices online.

What's Out?

With Our Managed Services, unless it's In or We've specifically agreed otherwise in writing, it's Out. Here's a list of a few things that are Out:

1. Changes;

a) Issues caused by changes made by You or Your developers, including if Your developers have Root, Admin or Sudo access to Servers.
b) Unauthorised changes: Problems resulting from any modifications or customisation of the Relevant Products or Services not notified AND approved in writing by Us. For the avoidance of doubt, modifications to the Service shall include changes to the hardware, resources, operating system, the software stack or any configuration.
c) A change to the configuration with hardware, operating systems or other supporting software from the original configuration as detailed in the Service Schedule, unless agreed in writing with Us.
d) Relocation of the Service(s) unless agreed in writing with Us.

2. The Service(s);

a) Application debugging help and support for issues that arise from your code, 3rd parties or other systems outside of our control.
b) Code repositories, server images, server recepies (Docker, Ansible, Chef, Puppet, etc).
c) Auto-scaling setups and related services or monitoring
d) Central log management services
e) Load testing applications and support
f) Real Time Slack Support and/or other types of instant chat support
g) Any other Service(s) not supplied by Us unless otherwise agreed in writing.
h) We will supply and, where appropriate, charge for cabling and interconnects between equipment in a rack.

3. Your Team and Code;

a) Any issues related to Your Code, Database or Application.
b) While We can assist in debugging Your code (We will inform You in advance if this is a chargeable service) We will not do Your development or write any Code for You.
c) Any faults, problems or malicious events that happen after We've made a recommendation to You e.g. We will make security recommendations, but if You choose not to follow them and something goes wrong as a result, any remedial work is not covered.
d) Any breach of Your obligations under this Agreement or having the Service(s), or any part of it, maintained or fixed by a Third Party without Our approval.
e) Any act or omission by You including as detailed in clause 6 of the General Terms.
f) Monitoring of Your Code or Application and its correct function.

4. Incorrect Use;

a) Incorrect or unauthorised use of the Service or operator error.
b) Use of the elements of the Service(s) in any combination or set up other than those specified in the Documentation.

5. External Problems;

a) Problems arising from viruses, unauthorised access, hacking or other malicious acts or code and any subsequent remedial action that's required.
b) Any fault in the Service(s) or Product(s) provided by Third Parties

c) Any issues arising from Third Party software releases whether installed by Us or You e.g. if the latest Operating System contains a bug that adversely affects Your Service(s).
d) Issues with Your computers or devices (laptops, desktops, tablets, phones, etc). This includes settings problems on these devices that are preventing them from working with the services provided by Us.
e) Issues with networking, internet connections, firewalls or any other devices or services that You use to access the services provided by Us.

Support & Maintenance;

a) Where We have fixed the same problem three times, and We consider that the reason for the issue recurring is outside of Our control, this issue will no longer be an In-Scope Service.
b) Scheduled Maintenance on Your Service(s) outside of Our Standard Maintenance Hours.
c) We will not be responsible for backup of any data held on the server unless We have agreed otherwise in writing.
d) Any DBA (Database Administrator) work or work that a DBA would usually undertake unless We have specifically agreed otherwise in a Service Schedule.
e) Hours required by our engineers to support your systems over and above the hours allocated in your contract (hours cannot be carried over between months).