

## Contents

Contents .....	1
1 Overview.....	2
1.1 Why a proactive managed service.....	2
1.1.1 Benefits of proactive managed services.....	3
1.2 Helpdesk Portal.....	3
1.3 Helpdesk Priorities explained .....	3
1.4 Helpdesk Timers explained .....	3
2 Service Level Agreements .....	4
2.1 Platinum SLA.....	4
2.2 Gold SLA.....	4
2.3 Silver SLA .....	4
2.4 Bronze SLA .....	5
3 Additional Services .....	5
3.1 Server Cloud Backup.....	5
3.2 ESET Advanced Cyber Protection & Encryption.....	5
3.3 Advanced Network Support.....	5
3.4 Advanced Application Support.....	6
3.5 Advanced SharePoint Support .....	6
3.6 Microsoft Office 365 Administration Support.....	6
3.7 SaaS Protection for Office 365 .....	6
3.8 SaaS Protection for Google .....	6
3.9 SaaS Protection for SharePoint.....	7
3.10 File Protection Backup (PC/MAC).....	7
3.11 Cloud Protection Backup (PC).....	7
3.12 Workplace Desktop .....	7
3.13 Workplace Server.....	8
3.14 Remote Security Auditing .....	8
3.15 BCDR Solution .....	8
Appendix A – Managed Service SLAs.....	9

Appendix B – Platinum SLA with optional services.....	10
Appendix C – Gold SLA with optional services.....	11
Appendix D – Silver SLA with optional services .....	12
Appendix E – Bronze SLA with optional services .....	13

## 1 Overview

LazenbyIT has developed a proactive managed service model and portfolio of additional services to deliver professional services to align with the specific needs and budgets of our clients. These are offered via a range of service level agreements, which our managed service helpdesk is designed to provide.

Many MSPs provide one level of SLA for everything, we believe businesses require more flexibility to give better response times for critical systems or teams and for business-critical situations. This also allows businesses to save costs on less critical devices or teams, that don't need such a quick response, but all systems are still monitored and managed.

### 1.1 Why a proactive managed service

The old break fix service appears to be a cheap option, you only pay for support/help when it is needed. However, this typically results in longer response and resolution times and longer outages or downtime and usually costs businesses more in staff payments while they are unable to work or impacts productivity or deliveries to clients.

The managed service model comes from the corporate environment to monitor and identify issues before they cause downtime or outages during the working period and resolve out of hours and rapidly during business hours. However, without monitoring and alerting this is still a response driven solution.

Having over 30 years working in managed service environments it is clear there is a more enhanced level of managed service that can be applied, that of **proactive** managed service where the helpdesk and remote monitoring and management (RMM) system has policies and alerts that warn and can act automatically.

Some of these monitors are:-

- disk space running out
- computers running at 100% processor for more than 5 minutes
- memory utilisation exceeding 95% consistently
- operating system updates that need applying
- virus detection
- security protection systems that are not operating fully or have been disabled

- servers going offline

### 1.1.1 Benefits of proactive managed services

The driver for this type of service is achieving certain benefits for our clients; to minimise outages, downtime and therefore support calls and improve confidence in IT services, which helps businesses to focus on their own services and not worry about the technology letting them down or disrupting business as usual.

## 1.2 Helpdesk Portal

To ensure this service is managed effectively LazenbyIT provides a helpdesk portal, that can be accessed from our website, scroll down to the footer and click Support. We still have the dedicated phone line and email for the times our clients are unable to reach the portal.

## 1.3 Helpdesk Priorities explained

When a ticket is generated within our system, the overall SLA level is applied and the default priority of P3 – Medium set, our helpdesk team will be advised of this and the respective response times advised and the count down started, however, if the device or person is in a higher SLA level this ticket will be escalated to that level and timers adjusted to that SLA. In addition, when the ticket is raised via the portal each client can set one of four Helpdesk Priorities from P1 - Critical, P2 - High, P3 - Medium, P4 – Low, should P1 be selected then this relates to business-critical incident and the timers adjusted.

## 1.4 Helpdesk Timers explained

Within the helpdesk system we have three timers to assist with the performance of the helpdesk, where timers have reached 50% without action an alert is triggered to the assigned technician, where it has reached 70% without action an alert is triggered to the helpdesk manager.

1. First Response – This is the maximum target time for the helpdesk team to respond to the ticket, this relates to the active SLA and the helpdesk priority selected
2. Resolution Plan – This is the maximum target time for the resolution plan to be implemented, the value varies with the active SLA and selected helpdesk priority
3. Resolved – This is the maximum target resolution time for the technician to resolve the ticket, the value varies with the active SLA and selected helpdesk priority

In general, LazenbyIT helpdesk responds, plans and resolves tickets well within 50% of the target times, there are times when the resolution is outside of the helpdesk teams' control and dependant on other parties to resolve the issue, which may result in these targets being extended, this will be notified to clients and a running commentary where necessary will be maintained.

## 2 Service Level Agreements

There are four levels of service level agreement (SLA) offered, these control the response time parameters applied within the helpdesk. As businesses depend on certain critical services, these can be set at same or a higher SLA level to the management of end user devices. In appendix A is a matrix of the standard services and the inclusion within the various SLA levels.

The reporting and account management activity is also linked to the service levels selected for a majority of services.

The frequency of backup monitoring, operating system monitoring and the service reviews change with the SLA level chosen.

### 2.1 Platinum SLA

The platinum service level agreement offers the highest level of maintenance time and frequency of monitoring, checks and updates of operating systems and best response times.

A more detailed breakdown of proactive managed services and costs of optional services can be found in Appendix B.

LazenbyIT recommends this for critical business services that impact the whole or major systems functionality, and the business cannot function without them.

### 2.2 Gold SLA

The gold service level agreement offers a high level of maintenance time and frequency of monitoring, checks and updates of operating systems and quick response times.

A more detailed breakdown of proactive managed services and costs of optional services can be found in Appendix C.

LazenbyIT recommends this for critical business services that impact major functions, and the business needs quick response and resolution.

### 2.3 Silver SLA

The silver service level agreement offers a reasonable level of maintenance time and frequency of monitoring, checks and updates of operating systems and quick response times.

A more detailed breakdown of proactive managed services and costs of optional services can be found in Appendix D.

LazenbyIT recommends this for servers or important business services for micro or smaller enterprises that depend on them to function normally.

## 2.4 Bronze SLA

The bronze service level agreement offers a cost-effective level of maintenance time and frequency of monitoring, checks and updates of operating systems and reasonable response times.

A more detailed breakdown of proactive managed services and costs of optional services can be found in Appendix E.

LazenbyIT recommends this for end user systems for micro or smaller enterprises that depend on them to function normally while working to tight budgets.

## 3 Additional Services

LazenbyIT offer an extensive range of professional service beyond managed services, such as policy templates and advice, business continuity, backup, data leak and encryption services, security auditing and design, network design and implementation, VoIP telephony, application design and development, domain management and hosting and website design and management. These are provided on a project basis through our professional service team.

In respect of additional monthly managed services that complement the solutions for each client we offer the following services, that are all available to each client and again linked to one of the four service levels. Separate detailed brochures are available for each product:-

### 3.1 Server Cloud Backup

Unless the data exists in three locations, it is considered not to exist, as if deleted, corrupted it can't be recovered. Protecting data by backup is critical to every business, although without encryption access to the backup could result in a breach of data protection, therefore all backups provided by LazenbyIT are encrypted at source and maintained on cloud backup. Test restores of data are also important and periodic tests are carried out. For large data sets this solution may require a long period of recovery to complete restoration in a disaster situation. In this case LazenbyIT recommends a BCDR solution.

### 3.2 ESET Advanced Cyber Protection & Encryption

LazenbyIT recommends ESET protection solutions, which work on multiple platforms, server, windows, apple and Linux systems as well as tablets and mobiles. As an ESET partner we attend regular training to maintain current knowledge of products and upcoming solutions.

### 3.3 Advanced Network Support

Management of perimeter firewalls and routers is a key defence for every company. Many systems provided by the internet providers are either less secure or outside the control of the business, therefore most companies prefer to have internal security devices to prevent unauthorised access to their networks which could breach data protection regulations.

LazenbyIT provides monitoring, security auditing and maintenance of these devices to protect our clients' networks and data.

### 3.4 Advanced Application Support

Most companies have critical applications which the business depends upon such as Accounts, HR, ERP systems. LazenbyIT provides bespoke software update support which ensures the process is completed without causing undue downtime or impact upon other dependant systems.

### 3.5 Advanced SharePoint Support

With Microsoft 365 licencing comes access to 2TB of storage, management of access permissions and sharing to external organisations or persons can result in loss of control over business information. LazenbyIT provides advanced support for SharePoint, advice and training as well as user guides to assist our clients maintain control. The backend management and permissions of SharePoint sites, libraries are complex, LazenbyIT has over 18 years' experience of designing, migrating data and protecting data in SharePoint to assist our clients.

### 3.6 Microsoft Office 365 Administration Support

Managing users, groups and managed services, passwords, permissions and licencing are reasonably straight forward but to configure retention policies to avoid loss of data, configuration of alerts and protections to detect unauthorised access and breaches is more complex. This is where LazenbyIT can utilise our knowledge and management of many installations to assist clients manage joiners, leavers and movers in a timely and accurate manner.

### 3.7 SaaS Protection for Office 365

Microsoft in their terms and conditions recommend all Office 365 users to utilise a 3<sup>rd</sup> party backup solution. Within Office 365 deleted files, emails are retained for a period and then deleted permanently, this does not protect against ransomware. LazenbyIT recommends the use of SaaS Protection which takes three backups daily of emails or selected accounts, protects Team's data, personal files in OneDrive. This saves the data in separate data centres that are replicated in one or more countries, ensuring data is stored in more than 3 locations.

### 3.8 SaaS Protection for Google

Google in their terms and conditions recommend all business users to utilise a 3<sup>rd</sup> party backup solution. Within Google deleted files, emails are retained for a period and then deleted permanently, this does not protect against ransomware. LazenbyIT recommends the use of SaaS Protection which takes three backups daily of emails or selected accounts, protecting your data in a separate data centre, with rapid restoration.

### 3.9 SaaS Protection for SharePoint

Microsoft in their terms and conditions recommend all Office 365 users to utilise a 3<sup>rd</sup> party backup solution. Within SharePoint deleted files are retained for up to a maximum of 92 days and then deleted permanently, this does not protect against ransomware. LazenbyIT recommends the use of SaaS Protection which takes three backups daily of all or selected sites and all content within them. This allows indefinite restoration of deleted files or restoration of specific versions to restore after a ransomware attack.

### 3.10 File Protection Backup (PC/MAC)

Some businesses prefer to store files on their own laptops and desktops, or they store files in a cloud solution such as Dropbox. Without a backup, this information can be lost. Encryption tools such as bit locker without the decryption code could result in loss of access if the motherboard dies. File protection is designed to backup your personal data on one or more drives. As soon as you save a file it is uploaded to the cloud storage, this is encrypted and secure. Restoration of previous versions is easy and rapid.

### 3.11 Cloud Protection Backup (PC)

This backup is designed to protect the data on the system drive as well as the operating system, so the whole computer and data can be recovered should the computer be stolen, destroyed, or faulty, the whole system can be rapidly restored to a new device or run up in the cloud so can be used quickly from anywhere in a disaster situation.

### 3.12 Workplace Desktop

Many companies have clients and the need to share certain files with their clients or have their clients share documents securely and confidentially. Workplace Desktop provides a local application like Dropbox, only every file is encrypted and automatically backed up. The data can be stored on the cloud system and accessed via a browser or file explorer as well as locally synchronised for working without internet access.

Project areas can be created for internal teams, with permissions to certain staff as well as Shared folders that can be shared with clients, this can be public without password or requiring a password and two factor authentication to ensure the highest level of security.

One of the key differences with Datto Workplace is it includes the unique Ransomware protection within the workstation agents. There are agents for Windows and Mac, as well as Android and iOS apps so you can access your files from anywhere in the world on any of your devices.

Each user granted access also has three levels of access; full, edit or read only.

This system also works with DocuSign to allow clients to electronically sign documents within their shared folder(s).

The fees for Workplace reduce with the volume of end users signed up.

### 3.13 Workplace Server

The workplace server is designed to work in a similar way but focused on shared folders that are synchronised in real time with a cloud server (data centre) offering archive functionality, work anywhere capabilities as the Workplace Desktop can be granted access to the Workplace Server storage. Again, the advantage of this solution is it includes encryption and backup and restore services built in along with managed user access controls.

Workplace Server has an agent for Microsoft Windows Servers only.

### 3.14 Remote Security Auditing

Maintaining Cyber Essentials accreditation or regular checking of your security protection systems requires a security audit. LazenbyIT utilises Nessus auditing software, trained and qualified staff to provide regular auditing services to ensure compliance and peace of mind for business owners and leaders. For more details please ask.

### 3.15 BCDR Solution

Standard backup and restoration systems can protect businesses however this may result in periods of downtime or outage should vital equipment fail or be damaged by flood, fire or theft otherwise called a Major Incident. BCDR provides a "Business as Usual" service, which minimises downtime to minutes not hours, days, or weeks. Replacing a server could take 2 or 3 days, restoring the data from cloud backup could take multiple days, this could stop the business working, delaying production or delivery to clients. BCDR provides a local backup system that can boot into a virtual server within minutes to function as the original server to maintain service while the original is repaired/replaced, then makes the rebuild and recovery easier out of hours. The backup can be as regular as 5 minutes so the most data than can be lost is 5 minutes. The data is backed up to a data centre regularly and as short as every 30 minutes. So, if the computer room and all kit are destroyed, the server can be run as a virtual server at the data centre and access granted to the business to carry on. For more details please ask for our customised BCDR services.



## Appendix A – Managed Service SLAs

Below is an overview of the standard services which include firmware and software updates, remote access agents, incident reporting, total support times and total maintenance for servers.

Service Levels / Packages	Bronze		Silver		Gold		Platinum	
	PC/ Laptop / Mac	Server	PC/ Laptop / Mac	Server	PC/ Laptop / Mac	Server	PC/ Laptop / Mac	Server
Phone Support	✓	✓	✓	✓	✓	✓	✓	✓
Helpdesk Portal & Email Support	✓	✓	✓	✓	✓	✓	✓	✓
Account / Report Review (Months)	12		6		4		3	
Weekly SaaS/Backup Monitoring	✓	✓	✓	✓		✓		✓
Daily SaaS/Backup Monitoring				✓	✓	✓	✓	✓
Bi-monthly Server Check & Updates		✓		✓				
Monthly Server Check & Updates						✓		
Bi-Weekly Server Checks & Updates								✓
ESET Protection (from) per device per month	£1.60	✓	£1.60	✓	✓	✓	✓	✓
Firmware / Software Updates	✓	✓	✓	✓	✓	✓	✓	✓
Remote Access Agent(s)	✓	✓	✓	✓	✓	✓	✓	✓
Reporting	✓	✓	✓	✓	✓	✓	✓	✓
SLA Target Response P2 Time (hrs)	3	3	2	2	1	1	1	1
SLA Target Fix Time P2 (Hrs)	16	16	8	8	8	8	6	6
Total support time per User/year (hrs)	2		3		4		6	
Total Maintenance & Support per Server/year (Hrs)		8		12		16		24
Managed Service Fees / Month per User or Server	£16.00	£70.00	£24.00	£100.00	£30.00	£140.00	£45.00	£200

- SLA Based on normal support services 9 to 5 working hours Monday to Friday excluding bank holidays as well as Disaster Incidents.
- Servers can be at a different service level to PC / Laptop / Mac as can certain nominated teams
- Monitoring of backups and server availability are checked daily with alerts being monitored

## Appendix B – Platinum SLA with optional services

SLA Target Response Time (Hrs)	1		
SLA Target Fix Time (Hrs)	6		
Helpdesk Priority	First Response	Resolution Plan	Resolved
P1 Critical	0.5	2	4
P2 High	1	3	6
P3 Medium	2	6	12
P4 Low	4	12	24
<b>Proactive Managed Services</b>		PC/ Laptop / Mac	Server
• <b>Helpdesk &amp; Phone Support</b> : During working hours initial response to phone or email or text within 1 hours		✓	✓
• <b>Helpdesk &amp; Phone Support</b> : Outside work ours will respond within 2 hours between 6pm – 10pm M-F		✓	✓
• <b>Backup Monitoring + Server Monthly Updates</b> : Monitoring of daily backup jobs (week days)		✓	✓
<b>Managed Service Fees per month per User or Server</b>		<b>£45.00</b>	<b>£200.00</b>
<b>Firmware / Software Updates</b>		✓	✓
<b>Remote Access Agent(s)</b>		✓	✓
<b>Incident Reporting</b>		✓	✓
<b>Total support time per User/year (Hrs)</b>		5	
<b>Total Maintenance &amp; Support per Server/year (Hrs)</b>			20
<b>Optional Services</b>		PC/ Laptop / Mac	Server
<b>Server Cloud Backup Space (price per GB per month)</b>			<b>£0.03</b>
<b>ESET Security per device per month</b>		✓	✓
<b>Advanced Network Support /month</b>			<b>£200.00</b>
<b>Advanced Application Support /month</b>			<b>£75.00</b>
<b>Advanced SharePoint Site Support / Month (Hrs)</b>		<b>£90.00</b>	1
<b>Office 365 Support per User /month</b>		<b>£2.00</b>	
<b>SaaS O365/Team/OneDrive Backup per user/per month</b>		<b>£2.40</b>	
<b>SaaS SharePoint Backup all sites per month</b>		<b>£5.00</b>	
<b>File Protection Backup (PC/MAC) per month</b>		<b>£10.00</b>	
<b>Workplace Desktop (unlimited retention) per User / Month</b>		<b>£12.00</b>	
<b>Workplace Server (unlimited retention) / per Server / Month</b>			<b>£60.00</b>
<b>Remote Security Audit (monthly / quarterly / annual)</b>		quoted	
<b>BCDR Solution (monthly)</b>			quoted

## Appendix C – Gold SLA with optional services

SLA Target Response Time (hrs)	1		
SLA Target Fix Time (Hrs)	8		
Helpdesk Priority	First Response	Resolution Plan	Resolved
P1 Critical	0.5	3	6
P2 High	1	4	8
P3 Medium	2	8	16
P4 Low	4	12	24

  

Proactive Managed Services	PC/ Laptop / Mac	Server
• <b>Helpdesk &amp; Phone Support</b> : During working hours initial response to phone or email or text within 1 hours	✓	✓
• <b>Helpdesk &amp; Phone Support</b> : Outside work ours will respond within 2 hours between 6pm – 10pm M-F	✓	✓
• <b>Backup Monitoring + Server Monthly Updates</b> : Monitoring of daily backup jobs (week days)	✓	✓
<b>Managed Service Fees per month per User or Server</b>	<b>£30.00</b>	<b>£140.00</b>
<b>Firmware / Software Updates</b>	✓	✓
<b>Remote Access Agent(s)</b>	✓	✓
<b>Incident Reporting</b>	✓	✓
<b>Total support time per User/year (Hrs)</b>	4	
<b>Total Maintenance &amp; Support per Server/year (Hrs)</b>		16
Selected Services	PC/ Laptop / Mac	Server
<b>Backup Space (price per GB per month)</b>		<b>£0.03</b>
<b>ESET Security per device per month</b>	✓	✓
<b>Advanced Network Support /month</b>		<b>£140.00</b>
<b>Advanced Application Support /month</b>	<b>£62.50</b>	
<b>Advanced SharePoint Support / Month (Hrs)</b>	<b>£60.00</b>	1
<b>Office 365 Support per User /month</b>	<b>£2.00</b>	
<b>SaaS O365/Team/OneDrive Backup per user/per month</b>	<b>£2.40</b>	
<b>SaaS SharePoint Backup all sites per month</b>	<b>£5.00</b>	
<b>File Protection Backup (PC/MAC) per month</b>	<b>£10.00</b>	
<b>Workplace Desktop (unlimited retention) per User / Month</b>	<b>£12.00</b>	
<b>Workplace Server (unlimited retention) / per Server / Month</b>		<b>£60.00</b>
<b>Remote Security Audit (monthly / quarterly / annual)</b>	quoted	
<b>BCDR Solution (monthly)</b>		quoted

## Appendix D – Silver SLA with optional services

SLA Target Response Time (Hrs)	2		
SLA Target Fix Time (Hrs)	8		
Helpdesk Priority	First Response	Resolution Plan	Resolved
P1 Critical	1.5	3	6
P2 High	2	4	8
P3 Medium	3	8	16
P4 Low	6	18	36

  

Proactive Managed Services	PC/ Laptop / Mac	Server
<ul style="list-style-type: none"> <li><b>Helpdesk &amp; Phone Support</b> : During working hours initial response to phone or email or text within 2 hours (normally within 30 minutes)</li> </ul>	✓	✓
<ul style="list-style-type: none"> <li><b>Helpdesk &amp; Phone Support</b> : Outside work ours will respond within 3 hours between 6pm – 10pm M-F</li> </ul>	✓	✓
<ul style="list-style-type: none"> <li><b>Backup Monitoring + Server Monthly Updates</b> : Monitoring of daily backup jobs (week days)</li> </ul>	✓	✓
<b>Managed Service Fees per month per User or Server</b>	<b>£24.00</b>	<b>£100.00</b>
<b>Firmware / Software Updates</b>	✓	✓
<b>Remote Access Agent(s)</b>	✓	✓
<b>Incident Reporting</b>	✓	✓
<b>Total support time per User/year (Hrs)</b>	3	
<b>Total Maintenance &amp; Support per Server/year (Hrs)</b>		12
Selected Services	PC/ Laptop / Mac	Server
<b>Server Cloud Backup Space (price per GB per month)</b>		<b>£0.03</b>
<b>ESET Security per device per month</b>	<b>£1.60</b>	<b>£1.60</b>
<b>Advanced Network Support /month</b>		<b>£100.00</b>
<b>Advanced Application Support /month</b>		<b>£50.00</b>
<b>Advanced Managed SharePoint Support / Month (Hrs)</b>	<b>£30.00</b>	1
<b>Office 365 Support per User /month</b>	<b>£2.00</b>	
<b>SaaS O365/Team/OneDrive Backup per user/per month</b>	<b>£2.40</b>	
<b>SaaS SharePoint Backup all sites per month</b>	<b>£5.00</b>	
<b>File Protection Backup (PC/MAC) per month</b>	<b>£10.00</b>	
<b>Workplace Desktop (unlimited retention) per User / Month</b>	<b>£12.00</b>	
<b>Workplace Server (unlimited retention) / per Server / Month</b>		<b>£60.00</b>
<b>Remote Security Audit (monthly / quarterly / annual)</b>	quoted	
<b>BCDR Solution (monthly)</b>		quoted

## Appendix E – Bronze SLA with optional services

SLA Target Response Time (Hrs)	3		
SLA Target Fix Time (Hrs)	16		
Helpdesk Priority	First Response	Resolution Plan	Resolved
P1 Critical	2	6	12
P2 High	3	8	16
P3 Medium	4	12	24
P4 Low	8	24	48
Proactive Managed Services		PC/ Laptop / Mac	Server
• <b>Helpdesk &amp; Phone Support</b> : During working hours initial response to phone or email or text within 3 hours		✓	✓
• <b>Helpdesk &amp; Phone Support</b> : Outside work ours will respond within 4 hours between 6pm – 10pm M-F		✓	✓
• <b>Backup Monitoring + Server Monthly Updates</b> : Monitoring of daily backup jobs (week days)		✓	✓
<b>Managed Service Fees per month per User or Server</b>		<b>£16.00</b>	<b>£70.00</b>
Firmware / Software Updates		✓	✓
Remote Access Agent(s)		✓	✓
Incident Reporting		✓	✓
Total support time per User/year (Hrs)		2	
Total Maintenance & Support per Server/year (Hrs)			8
Selected Services		PC/ Laptop / Mac	Server
Server Cloud Backup Space (price per GB per month)			<b>£0.03</b>
ESET Security per device per month		<b>£1.60</b>	<b>£1.60</b>
Advanced Network Support /month			<b>£70.00</b>
Advanced Application Support /month		<b>£42.00</b>	
Advanced SharePoint Support / Month (hours)		<b>£30.00</b>	1
Office 365 Support per User /month		<b>£2.00</b>	
SaaS O365/Team/OneDrive Backup per user/per month		<b>£2.40</b>	
SaaS SharePoint Backup all sites per month		<b>£5.00</b>	
File Protection Backup (PC/MAC) per month		<b>£10.00</b>	
Workplace Desktop (unlimited retention) per User / Month		<b>£12.00</b>	
Workplace Server (unlimited retention) / per Server / Month			<b>£60.00</b>
Remote Security Audit (monthly / quarterly / annual)		quoted	
BCDR Solution (monthly)			quoted