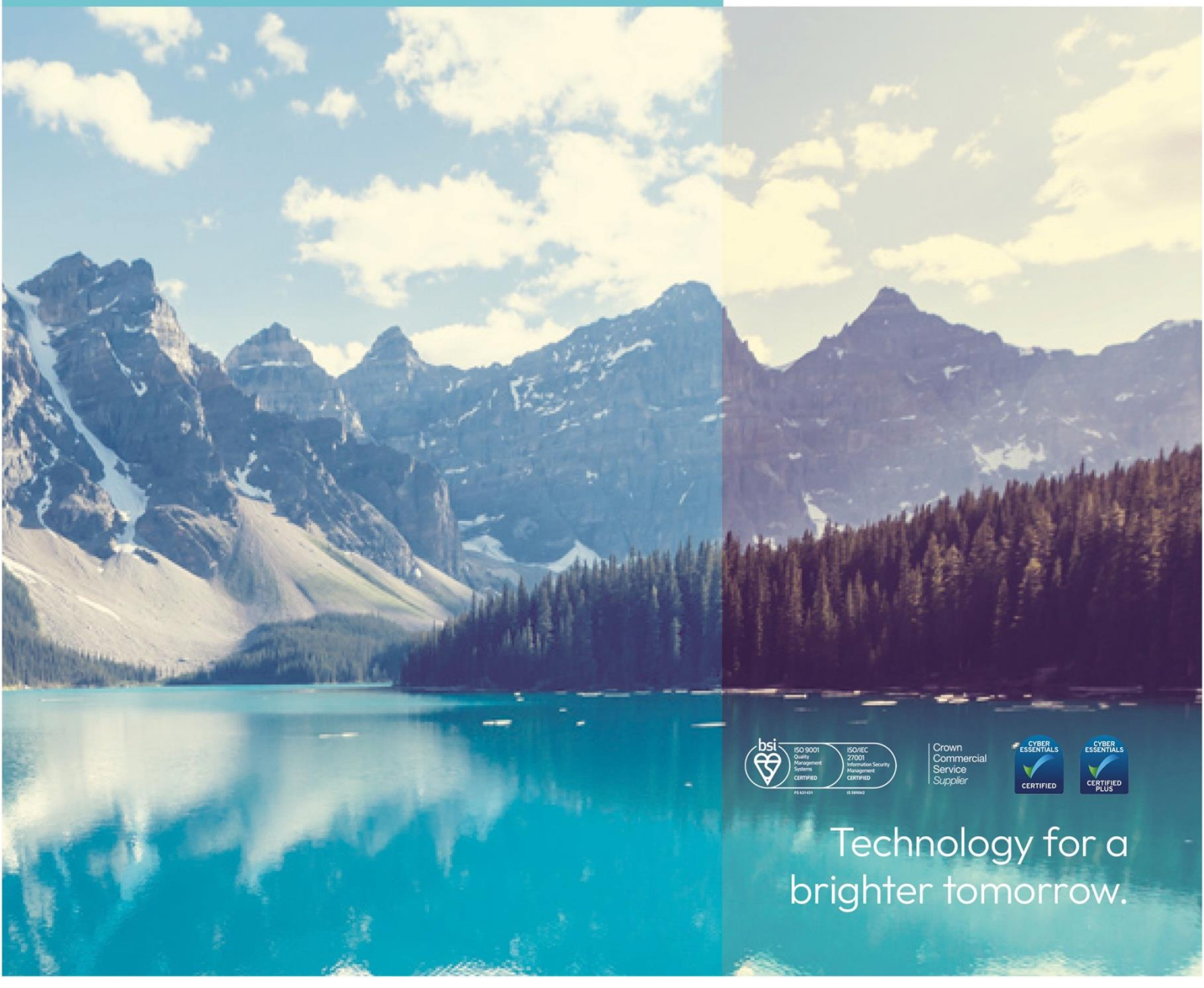
itps

intelligent technology. practical solutions.

ITPS Support & Managed Services (Hardware, Cloud, End User, Network, M365 & Security)

Service Level Description



Registered Office:

IT Professional Services Ltd
Angel House
Unit 5
Angel Park
Drum Industrial Estate
Chester-Le-Street
DH2 1AQ

http://www.itps.co.uk

Contents

Document Control

DOCUMENT TYPE:	**SERVICE LEVEL DEFINITION & DESCRIPTION**
DOCUMENT CLASSIFICATION:	**RESTRICTED**
DOCUMENT VERSION:	**V1.1**
DOCUMENT OWNER:	**LEE NEVIN & STUART GIBB**
CREATION DATE:	**3rd JANUARY 2023**
PRODUCT	**[PRODUCT]**
OFFERING	**[OFFERING]**
COMPONENT(S)	**[COMPONENT]**

Revision History

DATE	VERSION NUMBER	AUTHOR / AMENDED BY	DESCRIPTION OF AMENDMENTS
03/01/2023	1.0	Lee Nevin & Stuart Gibb	
28/09/2023	1.2	Lee Nevin	Rebranded

Distribution

NAME	ROLE	CONTACT NUMBERS

Document Review

This document will be reviewed and updated, when necessary, as stipulated below:

- ✓ As required to correct or enhance the content.
- ✓ Following changes to the ITIL or ISO quality systems standard as defined by ITPS.
- ✓ Following any organisation changes or restructuring.
- ✓ No longer than 12 months after the previous approval date.

	End Point		Microsoft 365		Network		Infrastructure	
	Core	Bolt ons	Core	Bolt ons	Core	Bolt ons	Core	Bolt ons
Support	1st line helpdesk 2nd/3rd line support Personalised number and email Incident Management Problem Management Change Management	Out of hours – 24/7 Onsite Service Engineer	1st line helpdesk 2nd/3rd line support Personalised number and email Incident Management Problem Management Change Management	Out of hours – 24/7 Onsite Service Engineer	1st line helpdesk 2nd/3rd line support Personalised number and email Incident Management Problem Management Change Management	Out of hours – 24/7 Onsite Service Engineer	1st line helpdesk 2nd/3rd line support Personalised number and email Incident Management Problem Management Change Management	Out of hours – 24/7 Onsite Service Engineer
Management	Account manager Onboarding Service Management 3rd Party Management Asset Management Device Lifecycle Management Installs, Move and Changes Health Checks Printer Management	Strategic guidance and Assistance Consultancy PC rollout and Image Management Office Moves and Relocation	Set up Managed licences Account manager Onboarding Service Management 3rd Party Management Asset Management o Device Lifecycle Management Licence Management	End Point Management	Account manager Onboarding Service Management 3rd Party Management Asset Management Device Lifecycle Management Installs, Move and Changes Device / Network monitoring Network Management Internet traffic and application monitoring Bandwidth monitoring Health Checks	Cabling Infrastructure support Cert Management Cabling Surveys Strategic guidance and Assistance Consultancy Traffic analysis	Account manager Onboarding Service Management 3rd Party Management Asset Management Device Lifecycle Management Installs, Move and Changes Infrastructure Monitoring Infrastructure Management Log monitoring Alert monitoring Health Checks	Cert Management Strategic guidance and Assistance Consultancy Performance management
Reporting	Major incident reporting Service review SLA Performance metrics	Enhanced Service, Availability and Security Reporting	Major incident reporting Service review SLA Performance metrics		Network reporting Major incident reporting Service review SLA Performance metrics		Infrastructure reporting Major incident reporting Service review SLA Performance metrics	
Data Resilience		Arcserve backup		Arcserve SaaS backup	Network config backups			Backup as a Service Replication as a Service DRaaS
Security	Patching (Workstation) AV management	Policy definition / management	Secure score review	Policy application Policy definition / management Windows Defender	Security reporting Patching (Firewalls, routers, switches) Patching (hardware)	Annual pen test with report Annual pen test with report and Remediation assistance Vulnerability assessment Event monitoring (Sentinel)	Security reporting Patching (Servers) Patching (hardware) AV management	Environment monitoring Annual pen test with report Annual pen test with report and Remediation assistance Vulnerability assessment Event monitoring

1.0 Detailed Description

Managing technology infrastructure is now more complex, and security threats are ever more sophisticated. Our complete and flexible, end-to-end, Managed IT Service includes UK-based telephone support, remote device monitoring, endpoint security, service management and reporting.

We proactively monitor your infrastructure and/or network to prevent problems from arising and respond quickly when issues appear. Our expertise means we can keep your end point devices working to the best of their ability and do all the admin required to support you with your Microsoft 365 licences.

Switch to our comprehensive Managed IT Services solutions and you will benefit from predictable and flexible costs, proactive support, and expert help in creating and maintaining a productive, secure and future-proof IT infrastructure for your organisation.

We have the right skills and capabilities to work with you as technology evolves, supporting your changing business, delivering tailored IT solutions and adding value as your trusted technology partner.

Onboarding

Ensuring everything required to manage the account is set up and in place.

Responsible teams include:

- Accounts
- IT Service Desk Management
- Data Centre Service Team
- Managed Service Team
- Field Engineer Team

Role	Step	Description
Accounts	1	When accounts process purchases and contracts to customers with maintenance elements, the accounts team create an on boarding ticket, they enter on to the system and subsequent automatic weekly reports alert the Service Desk Management by email.
ITPS Service Desk Management	2	The type/item of “On Boarding” creates tasks to steer the service team into specific activities to review the level of support required.
Accounts	3	The accounts team work with the salesman to resolve any issues from 2 and then relay the answers back to the service desk management.
ITPS Service Desk Management	4	This is an iterative process that concludes only when the Service Desk Management are happy that they have all the information they need to understand the service the customer purchased.
ITPS Service Desk Management	5	Once the support contract has been defined, the service team review the technical information to establish whether there is enough detail to deliver a technical service.
ITPS Service Desk Management	6	When the information has been collected, the info is updated on intranet and the relevant settings put in place such as the default contact used for that customer.
ITPS Service Desk Management	7	The customer is sent our standard call logging information, which describes how they raise support issues and also how to escalate a matter if required.
ITPS Service Desk Management	8	Finally, the new customer tasks checklist is completed and the ticket closed.

Management

Account Manager

As a managed service customer, a dedicated account manager / director shall be assigned and own the overall business relationship with the Customer and provide strategic and operational direction for the ITPS Account Delivery Team that will support a successful, ongoing business relationship.

They will be responsible for developing and maintaining the relationship with the senior stakeholders with the Customer through planned, formal and informal one to one meetings. Define a strategy for the Customer Account that is in line with their business objectives and that can be used to set in year goals for the ongoing delivery to the customer.

2.0 Incident Management

The ITPS Incident Management function ensures that all Incidents are managed in a consistent and structured manner and that normal service is restored as quickly as possible, minimising disruption and adverse impact to customer services. The process ensures that all Incidents are investigated through the utilisation of appropriately skilled resource and resolved to the satisfaction of the user. The Incident Management team, in place to support the process shall:

- Ensure that escalations are managed appropriately.
- Assist with the correct assignment of incidents.
- Ensure that Incidents are accepted into Resolver queues.
- Ensure that SLA's are managed.
- Assist more actively in the resolution of high priority Incidents.
- Ensure that failed SLA's are managed.
- Assist the Service Desk in the management of Incident updates and chase.

Where necessary, the invocation of a Major Incident Management process shall occur which involves the construction of a Major Incident Team who are dedicated towards the management of Incidents that meet customer specific Major Incident Criteria.

Incident Handling

Once logged, incidents are managed within ITPS Halo Manage system in-line with the assigned priority. All actions and associated updates are logged throughout the incident lifecycle with periodic updates sent to the call originator.

Please Note: ITPS operate a "three strike" rule whereby the MSD Service Desk will make 3 attempts to contact the incident originator to confirm the authority to close the ticket. However, if all three attempts to contact the originator are unsuccessful, the incident will be closed automatically with the notification sent via email to the originator.

First Contact Fix

Activities within the First Contact Fix procedure are as follows:

- Attempt to restore service for defined Incident types remotely after logging the Incident (with the User on the phone)
- If unable to restore service, attempt a 'Warm Pass' to second line remote support who will try to restore service (with the User on the phone)

If First Contact Fix is not possible, the Incident should be saved and assigned to the appropriate Resolver Team.

Investigate and Diagnose

Activities within the Investigate and Diagnose procedure are as follows:

- Resolver Team investigations in order to ensure the most appropriate restoration

- Submission of Requests for Change (RFC) in order to resolve Incidents if it is deemed that an RFC is the most appropriate approach to resolution
- Determining if the Incident should be passed to a Third Party
- Ensuring that service restoration was successful prior to resolution

Incident Resolution

Activities within the investigate and Diagnose procedure are as follows:

- Ensuring that resolution information detail is informative and satisfactory
- Ensuring that correct Resolution categories and codes are applied
- Ensuring that the Incident is set to a status of Resolved

Ensuring that the Incident is passed back to Contact Management for closure. The resolution criteria are agreed as part of the impact assessment. When the criteria are met, the incident is deemed resolved. Once resolved, the ITPS MSD engineer will contact the originator to confirm the authority to close the incident.

Sample Priority Definitions

Support is accessed through ITPS's dedicated support line, call routing to the ticket owner or the relevant incident team can be made from this point to ensure the Client reaches the expertise needed in a timely manner. All incidents will be recorded on ITPS Service Desk system under the Incident Management workflow. ITPS will record the name of the persons reporting the incident, time of call, detail of the fault and any other pertinent information, along with the criteria for resolution to ensure the workflow is imitated correctly.

It should be noted that the client must report a Business-Critical Incident (P1) via telephone only. ITPS cannot offer any priority-based Service Levels for Business-Critical Incidents via email, as email is not a guaranteed medium.

ITPS will carry out priority assessment on incidents, but we encourage our service users, when reporting an incident, to advise us on the priority level you would like attached. Within standard SLA's ITPS will endeavour to process incidents according to their priority. A guide is included below to help clarify how priorities are determined.

Initially the urgency and impact will be assessed, using industry standard metrics outlined in the tables below.

Category	Urgency – Description and examples
High (H)	The damage caused by the Incident increases rapidly. The work that cannot be completed by staff is highly time sensitive. A minor Incident can be prevented from becoming a major Incident by acting immediately. Several users with VIP status are affected.
Medium (M)	The damage caused by the Incident increases considerably over time. A single user with VIP status is affected.
Low (L)	The damage caused by the Incident only marginally increases over time. The work that cannot be completed by staff is not time sensitive.

Category	Impact - Description and examples
High (H)	A large number of staff are affected and/or not able to do their job. A large number of clients are affected and/or acutely disadvantaged in some way. The damage to the reputation of the business is likely to be high. Someone has been injured.
Medium (M)	A moderate number of staff are affected and/or not able to do their job properly. A moderate number of clients are affected and/or inconvenienced in some way. The damage to the reputation of the business is likely to be moderate.
Low (L)	A minimal number of staff are affected and/or able to deliver an acceptable service, but this requires extra effort. A minimal number of users are affected and/or inconvenienced but not in a significant way. The damage to the reputation of the business is likely to be none or minimal

Having determined the urgency and impact, we can then score the priority level.

		Impact		
		H	M	N
Urgency	H	1	2	3
	M	2	3	4
	L	3	4	5

This can also be represented using the terms below.

Priority Code	Description
1	Critical
2	High
3	Medium
4	Low
5	Very low

Priority 1 (P1)

At this priority level ITPS and the client must commit to round-the-clock response times and involvement by all necessary and appropriate personnel/systems until a mutually agreeable workaround is provided and the priority is no longer considered P1. ITPS classify all P1 incidents as Major Incidents (MI).

Examples of a P1 incident may include server, node, system, network or cluster down, unable to serve data, is in a state of frequent or repeating crash, panic or hang, or is in a state of degraded performance sufficient to prevent critical business applications operations.

Priority 2 (P2)

At this priority level, ITPS are committed to provide a commercially reasonable workaround and/or restore normal operation as quickly as possible during Normal Business Hours.

Examples of a P2 incident may include server, node, system, or cluster experiencing an infrequent, isolated, intermittent crash, panic, hang, or in a state of degraded performance that allows business operations to continue but at an inconsistent or less than optimal rate.

Priority 3 (P3)

At this priority level, ITPS will, during Normal Business Hours, work towards a viable and mutually agreeable workaround or propose an upgrade or replacement to mitigate the problem.
Examples of a P3 incident may include server, node, system, or cluster experiencing an issue, an anomaly, cosmetic defect that has little or no business impact.

Priority 4 (P4)

At this priority level, ITPS will, during Normal Business Hours, provide advice on whether a workaround, upgrade or replacement to mitigate an issue is available.

Priority 5 (P5)

At this priority level, ITPS will, during Normal Business Hours, provide answers to questions and “How do I” type queries.

Out of Hours Service

ITPS provide 24/7x365 access to its Service desk as a costed option for critical system down scenarios – Priority 1 (P1) only

ITPS has several technical engineers available covering multiple technologies. Once your call is logged in our Service Desk system, is it then then passed to a Technical Engineer with the appropriate speciality in that technology. The Out of Hours Service also provides access to senior level consultants should further escalation or assistance be required.

To access the Out of Hours Service, please call the Out of Hours’ number as defined in the onboarding documentation.

Major incident reporting

Reason for outage (RFO)/ Root cause analysis (RCA) issue within 7 days

3.0 Problem Management

A problem may be the cause of one or more incidents. The cause is not usually known at the time the problem is recorded. To prevent problems and resulting incidents from reoccurring, our problem management process is used to determine the root cause. The process is also designed to minimise the impact of problems that cannot be avoided.

A problem can be detected via several sources, including, but not limited to:

- The Service Desk from a specific incident
- Monitoring alerts
- Incident trend analysis
- Notification from Vendor/Security Incident
- ITPS know issues/error list

When a problem is raised, ITPS will gather all necessary information and perform a Root Cause Analysis. When a solution is possible it will be applied and documented. However, if the managed service engineer cannot find a solution, the problem will be escalated internally, then to the relevant vendor, as necessary. When a change is needed to fix a problem, then a Request for Change will be initiated and put through the Change Management Process. At the point of resolution, the Service Desk will contact the originator to gain approval to close. Any open or held, problem related incidents will then be subsequently resolved and closed.

4.0 Change Management

The ITPS Change Management function provides a single process for the management of changes to infrastructure, applications, and systems which make up the services for which ITPS are responsible.

All related changes are managed by the Change Management process and includes repeatable changes such as patching and other changes that have varying degrees of complexity and risk and are non-repeatable.

The purpose of Change Management is to:

- Ensure that changes are accurately recorded and have an identified Owner
- Ensure that the impact of changes is assessed, that changes are feasible and that changes are justified
- Ensure that changes are classified:
    - Emergency P1
    - High P2
    - Normal P3
    - Retrospective
- Ensure the correct level of authorisation is applied
- Establish appropriate mitigating and preventative controls prior to the implementation of an Request for Change (RFC)
- Schedule changes to the live environment
- To ensure that changes can be regressed in the event that they are unsuccessful

- Review change implementations to ensure continuous improvements and lessons from good and bad practice are fed back into the organisation
- Work with other support teams to assess changes to ensure continuous improvement
- Closure activities

The Change Management Team shall be responsible for the Ownership of the process ensuring that the process is fit for purpose and adopted across all stakeholders providing a consistent level of governance.

Request for Change (RFC)

All change requests must be submitted using the ITPS Request for Change Form. The RFC form should then be submitted as a support request.

Upon receiving the RFC, a Managed Service engineer will evaluate the form and will categorise the type of change before confirming back to the requestor. Once accepted the Standard Changes will be forwarded for scheduling whilst normal changes will be submitted for Subject Matter Expert (SME) review before CAB approval.

Standard Changes

These are pre-approved changes that have passed through the full Change Management Process, including Change Advisory Board (CAB) approval at least once. Standard changes can be implemented without requiring approval from the CAB.

Emergency Changes

An emergency change is a change required to resolve or implement a tactical workaround for a P1 incident. All emergency changes are subject to approval by both the ITPS Emergency CAB and the client before implementation.

Normal Changes

Normal changes are all changes that are not standard or emergency. Once logged all normal changes are assessed against the following risk matrix and assigned a CR ranking:

Impact of Service	High	Significant 3 CR3	Major 2 CR2	Critical 1 CR1
	Medium	Minor 4 CR4	Significant 3 CR3	Major 2 CR2
	Low	Candidate for Standardisation 5 CR5	Minor 4 CR4	Significant 3 CR3
		Low	Medium	High
		Probability of Negative Impact until Change is Successfully Completed		

Once assessed, the change will then be submitted for further technical review by an ITPS Subject Matter Expert (SME) before submission to CAB. Normal Changes will not be implemented until they have been reviewed and approved by the ITPS CAB.

Please note: A normal change may be added to the standard changes list if appropriate and the CAB approves it.

Change Advisory Board (CAB)

The ITPS Change Advisory Board (CAB) convenes each Tuesday and Thursday during normal business hours. The function of the CAB is:

- To review and approve or reject all normal change requests logged since the last CAB meeting.
- A review of all failed or rejected changes since the last CAB meeting.
- Review list of standard changes and make additions or changes as appropriate.
- Emergency Change Advisory Board (ECAB)
- The Emergency CAB is available 24/7 and convenes as soon as an emergency change request is raised. A named contact from the client business must also approve all Emergency Changes before implementation. Once approved, the Emergency change will be implemented as soon possible/safe to do so.
- CAB Approval and Rejection of Changes
- If the CAB approves the change, they will inform the ITPS Managed Service Engineer who logged the Request for Change (RFC) that it can proceed. However, If the CAB rejects the RFC, they will provide reasons and further actions for the Managed Service Engineer to give to the change originator. The change should then be re-submitted and will be reviewed at the CAB meeting.

ITPS will also work with customer CAB process as necessary.

5.0 Service Hours

Priority 1 Incidents	24 x 7 x 365
Priority 2, Priority 3, Priority 4, Change Management and General Enquiries.	08:00 – 18:00, Monday to Friday
Extended Support	Bespoke service priced and defined on an ad-hoc basis

6.0 Client Responsibilities

Depending on your agreed level of service from ITPS there are some requirements for you to maintain and care for your environment and adhere to some guidelines throughout the term of your service.

Maintenance and Care

Including but not limited to:

- Outside Normal Business Hours you must undertake appropriate triage methods to ascertain whether an incident is of P1 status.
- You must undertake an initial impact assessment before logging the incident with ITPS. This assessment is to include:
    - Affected Services
    - Business Impact
    - Number & type of users affected
    - Recent changes on affected infrastructure (regardless of perceived impact)
- You must provide full 'administrative' access to ITPS for all the services outlined in the impact assessment and any subsequently identified services.
- You must ensure that all Client Supported Assets are appropriately licensed.
- You are responsible for completing the RFC Form in accordance with the Change Management Process.
- You are responsible for ensuring that valid backups are taken of your environment and where necessary the configuration repository. These backups should be available should the need arise to reinstate configuration on an asset. This only applies if ITPS do not provide a managed backup service.

7.0 Business Benefits

- Allow experts from ITPS to look after the support
- Improved cost savings
- Reduce strain on in-house staff
- Full package of options to tailor support
- UK based support
- Improved risk assessment
- Increased user productivity
- Improved IT Service quality and enhanced customer satisfaction
- Minimised business disruption as service is restored as quickly and efficiently as possible
- Efficient and consistent management of Incidents
- Reduction in number of failed SLA's
- Improved Customer Satisfaction
- Reduction in time taken to Resolve Incidents
- Ensures appropriate skills and resource are obtained to support the service restoration.

8.0 Service Exclusions

Including but not limited to:

- Issues resulting from misconfiguration by Client Employed persons
- Failures in maintenance /administration by Client Employed persons
- Incidents arising from lack of training of Client Employed persons
- Data restoration caused by any Unauthorised Change.
- End user support or technical advice to any persons not listed as a Named Contact
- Changes that relate to services that are not owned by ITPS
- Services that sit outside the scope of services offered by ITPS

9.0 Toolsets

- Halo
- MS Teams for managing change requests
- Bomgar – Remote Control

10.0 Assumptions

- Resolver teams have access to log Changes
- Customers manage their own Third Party Suppliers Changes
- Standard escalations lists and contacts have been provided by all relevant areas (especially the resolving teams)
- Service Desk tool is correctly configured

11.0 Terms

Scheduled Maintenance:

Clients are required to agree with a forward schedule of maintenance – within the Forward Schedule of Change (FSC). The service shall not be guaranteed during scheduled maintenance work. All scheduled maintenance work will be notified to you via the FSC. However where, in our reasonable opinion, an emergency situation exists, we also reserve the right to carry out emergency maintenance outside the normal notification period.

Termination:

We shall cease providing the service on termination of the contract.