Principle networks

Service Description

Managed Service

Table of Contents

Introduction

This Service Description is provided as a supplement to Principle Networks General Terms and Conditions. Principle Networks may update this Service Description from time to time without notification.

This document sets out the service levels and parameters for the services provided by Principle Networks.

This Service Description applies specifically to Principle Networks '**Managed Service**'.

Service Overview

Principle Networks offer one level of Managed Service. This ensures that Principle Networks are consistent with their approach to every managed customer and can offer a high-quality service. The following is what is included within the Managed Service:

- Proactive/Reactive Monitoring of Solution and Services
- 24x7 Service Operation - Access to 3rd line engineers
- Incident management (In accordance with service SLAs)
- Change Management (Utilising Pre-Paid Days Contracts)
- Hardware Break Fix (24/7, 4 Hour or NBD)
- Backup / Configuration management
- Escalation and management of issues to vendors / suppliers
- Principle Networks Service Escalation
- Reporting (High Level Ad-Hoc Reporting Upon request – via Service Request)
- Co-Management Arrangements
- Continuous Service Improvement

Additional bolt-on services can be added such as:

- Documentation – Solution Documentation / Solution Diagrams
- Security Review - Firewall / Vulnerability Scans
- Business Review – Service & Incident Reporting / Security, Technology and Business Review

Pre-Paid Days Contracts

Pre-paid days contracts are a way whereby customers can pay for Change as part of their Managed Service contract. This can be agreed as part of a monthly allowance or purchased on an ad-hoc basis depending on customer preference.

Pre-paid days contracts may only be utilised for change and works in relation to services Principle Networks support, unless explicitly agreed. They may not be utilised for break fix or high priority problems and faults.

Anything that is estimated to take over 4 hours or more may be classed within project scope and will need the appropriate resource assigned to fulfil the requirement. Pre-Paid days can still be used in this scenario and therefore may require a full scope of works and project management.

Management & Support

Solution Monitoring

The hardware or software on which the Managed Service will be provided will be built and configured through consultation between Principle Networks consultants and the customer based on clearly understood requirements. Installation and configuration details will be fully captured and documented by Principle Networks consultants to ensure ServiceDesk have all the details requested to support the service.

Availability Monitoring

Hardware will be pro-actively monitored for availability 24 x 7 x 365 by Principle Networks monitoring platform to which the customer can request access in order to review historic availability statistics and other related information.

Monitoring of endpoints will typically be managed by SNMP, WMI, API or ICMP and from Principle Networks monitoring platform. Three consecutive failed responses to monitoring pings will result in the automatic generation of a fault, for investigation within the prevailing Service Level by Principle Networks Servicedesk.

Ongoing Management

The ongoing management of the service will include, but may not be limited to: -

- Availability Monitoring
- Pro-active and re-active fault resolution
- Hardware maintenance (Including Health Status)
- Change Management / Internal Problem Management (Utilising Pre-Paid Days Contracts)
- Back Up Configurations.

Backups

Regular backups are taken on all managed devices against solution specific Recovery Point Objectives (RPOs). Backups are securely stored, either within Public or Private cloud and follow industry best practices for security. These backups can be called upon within the solution specific Recovery Time Objective (RTO) in the event they are required.

Stateful Application backups are also supported for typical database applications such as SQL and Microsoft Active Directory.

For configuration backups, application features such as configuration difference comparisons can be used to checked for changes within a troubleshooting scenario, or they can be called upon for compliance purposes should this be necessary.

Fault Reporting

Faults or Requests can be reported to Principle Networks Servicedesk in the following ways: -

- Email - servicedesk@principle-networks.com
- Phone - 0333 012 4003 (Option 1)
- Customer Portal - http://portal.principle-networks.com

Servicedesk (24x7)	Business Hours	Servicedesk available
Tel: 03330 124 003 (Option 1)	08:00 – 17:30 Monday – Friday	24 x 7 x 365

Priority 1 and Priority 2 level incidents should be followed up by a telephone call should these faults be customer initiated.

Any fault or service- affecting issue will be dealt with by the Principle Networks Servicedesk.
Where subject matter experts input is required, cases will be escalated to the appropriate engineers accordingly within the prevailing Service Levels. Alternative Service Levels will apply to Change Requests.

Minimum Data Set

It is the responsibility of the customer to provide a minimum set of information to the Servicedesk upon logging a case.

- Date and time problem occurred:
- Detailed Description of the fault/change request:
- Asset(s) affected if known:
- Any recent changes made:
- What is the impact to the customers business (often dictates the priority):
    - No. Sites affected:
    - No. Users Affected:
- Has the kit been power cycled (if applicable):
- What is the hardware (Router/NTE etc) light status (if applicable):
- Site contact and access times:
- Specific error messages (if applicable):
- Screenshots attached? Yes/No:
- Troubleshooting steps tried to resolve the issue:

Services

Connectivity

Connectivity services within a solution as part of the overall service will be fully managed by Principle Networks. This includes fault logging with our service partners, fault progression and updates through to resolution. Feedback on root cause analysis will be provided upon case closure or via specific request.

Cloud

Public and private cloud hosted services within a solution as part of the overall service will be fully managed by Principle Networks. This includes fault logging with our service partners, fault progression and updates through to resolution. Feedback on root cause analysis will be provided upon case closure or via specific request.

SaaS

SaaS services delivered within a solution as part of the overall service may be fully managed by Principle Networks, co-managed with the customer or unmanaged such as where licensing alone was purchased without defined solution support. Both fully managed and co-managed services include fault logging with the associated service partner, fault progression and updates through to resolution. Feedback on root cause analysis will be provided upon case closure or via specific request.

Vendor Escalations

Any supplier and vendor escalations will be managed by Principle Networks as part of the service, except where a service is unmanaged.

Hardware and Service Maintenance

Operating System Patching & Upgrades

Application of critical or high risk patches to appliance Operating Systems will be carried out by the Principle Networks Servicedesk team under the change management procedure during working hours (out of hours patching is available) within 14 days. Any non critical or high risk patches will follow the usual change management process and pre-paid days contracts may be used.

Hardware Upgrades

Due to End-of-Life status or changing requirements of the customer, appliance upgrades may from time to time be necessary. Any such upgrades will attract the appropriate charges from Principle Networks.

Hardware – Vendor Support

Principle Networks will manage all vendor technical support requests to ensure technical expertise are available that understand the technical solution to assist and provide a resolution faster.

Hardware Replacement or Fix

All hardware is covered by hardware replacement or fix warranty (unless exceptions have been made, which will be clearly identified In the scope of works document). This service is initiated and managed by Principle networks but will be operated by third party companies who specialise and have access and availability of replacement parts worldwide. Hardware warranty starts upon first delivery to customers premises.

An attempt to fix the faulty hardware or component will be made, however in most circumstances under hardware warranty the equipment will be replaced. A 4 hour on site response or Next business day options are available with engineer and remote specialist support.

Change Management

All changes will be categorised as a change request within Microsoft Dynamics and will be sub categorised into three types. Standard, Normal and Emergency Changes.

All changes are chargeable with time taken from the customer pre-paid days contract, as described earlier in the document. Changes adhere to Principle Networks' standard Service Levels defined within this document. As standard, all changes are prioritised as P4 and completed in hours defined in the SLA.

Changes may be completed out of hours at customer request when Principle Networks resource is available. Out of hours change time is taken from a customer pre-paid days contract at double time.

Standard Change Request

Standard Changes have been defined as a 'Business as Usual' task and do not follow the full normal change management process. All standard changed requests will be give the P4 SLA.

A Standard Change request is categorised as a low risk / low impact change which is usually commonly requested and frequently implemented. They follow company work processes where appropriate and have a proven history of success.

Types of changes covered by a standard change (Subject to complexity):

- System reboot
- Minor software and OS patching
- Security Policy additions
- Traffic Routing (Minor)
- Port and or VLAN Configuration
- Port Channel
- Existing VPN Configuration
- Firmware Upgrade

Multiple changes of the above types within reason could be seen a larger piece of work. Pre-Paid Days or project work will be called off at this point.

Normal Change Request

Normal change requests are considered those that do not fall into either a standard or emergency change scenario. The impact is often moderate to very high and holds a medium to very high risk. Formal procedures must be followed to ensure that each step of a normal change request case is completed in line with this process.

Every normal change must undergo a detailed review of the customers requirement which comprises of:

- Change Reason and Justification
- Change Details and Associated Equipment
- Post Change Test Details
- Impact Analysis, Highlighted Risks and Mitigation
- Rollback Details

Pre-paid days' time will be called out for all normal change requests.

Emergency Change Request

The emergency change process is in place to work around or resolve high impact and high-risk incidents that are causing substantial business disruption. An Emergency Change could also be utilised to protect the customer's business from threats such as are likely to result in an incident if not addressed promptly, for example a critical security vulnerability that could result in a cyber-attack. Emergency changes should follow the incident management P1 process and ensure that the case type is "Change Request".

Service Request

Customers can make service requests in relation to their Principle Networks managed service. For example, ask question about their service or VPN user creation.

Where a request type is deemed as a chargeable requirement the customers pre-paid days contract can be used for professional services time. Should a request fall out of scope of a pre-paid day's contract then the request will be passed onto the customer's account manager to progress as a project opportunity.

There are two case types that Principle Networks use within Microsoft Dynamics to categorise service requests; these are:

Query – A query can be a question or request for information about a customer's existing service or a service a customer may want to consume. Often queries develop into a change request or a referral to the customer's account manager should any further actions be required such as scoping requirements for a project.

Service Request – Is a formal low risk request for something to be provided. For example, this could be a password reset, or a new VPN user request. These requests a low impact changes that are quick to action which save the use of having to go through the change management process.

Change Request Authorisation

Change requests will only be accepted by authorised contacts within your organisation pre agreed with the company change delegate contact often, IT Director/Manager position or equivalent. Principle Networks have these named contacts stored on Microsoft Dynamics CRM for security purposes.

Planned Maintenance

Principle Networks work with several service partners who from time to time perform planned maintenance to continuously improve the stability of their products and services. Using downtime schedules Principle Networks will ensure that any notification of planned works that they receive that is service affecting will be added to a downtime schedule and a calendar invite will be sent to the Primary service desk contact to ensure the customers are also informed of the works.

Where applicable Principle Networks will also agree recurring maintenance windows in association with standard changes to support on-going software maintenance such as patching in line with ISO27001 and Cyber Essentials Plus.

Customer Maintenance

It is the customers responsibility to notify in advance any planned work taking place that will affect the managed service solution supported by Principle Networks. A downtime schedule will be created for the

date/time of the work and a description will be added including the Dynamics case number to ensure the ServiceDesk team are aware.

The downtime schedules ensure that alarms are suppressed for the duration of planned work. Once the end date and time has lapsed alarm suppression is lifted automatically and normal service monitoring of the solution is resumed.

Co-Management

Principle Networks provide customers with co-management access, this can be restricted to a level to allow customers to undertake minor changes or complex changes depending on their requirements and experience. As part of co-management customers are free to manage their own internal change process or are welcome to use principle networks to peer review or as an escalation point for changes where appropriate. Generally, we expect customers to have access to their own hardware equipment or environments (Microsoft Azure, Zscaler, Microsoft Security or Meraki Dashboards for example).

It is the customers responsibility to ensure any changes made have been verified and tested prior to implementation to ensure no unnecessary downtime to their network services is made. We recommend customers utilise their own UAT plans (user acceptance testing) after each change. Should any support on changes be required it is strongly advised that customers log the change request to the principle networks servicedesk for the ServiceDesk team to verify and implement.

Service Level

Principle Networks Managed Services are monitored 24 x 7 x 365. Within contracted support hours, Principle Networks will respond to autogenerated cases raised by the monitoring systems or to cases raised by the customer within the Service Level Agreement terms.

See the below the description of Service Level against the target response and resolve times:

Priority	Description
P1	A Critical business service is non-operational impacting the customer organisation, multiple users or multiple sites; or Severe functional error or degradation of service affecting production, demanding immediate attention. **Business risk is high, with immediate financial, legal or reputational impact.**
P2	The client is experiencing failure or performance degradation that severely impairs operation of a critical business service; or the client or service has been affected, although a workaround may exist; or Application functionality is lost; or significant number of users or major site is affected. **Business risk is high.**
P3	The client is experiencing a problem that causes moderate to low business impact. The impact is limited to a small number of users; or incident has moderate, not widespread impact; or the customer or service may not have been affected. **Business risk is low.**
P4	Standard service request; Change request; Enquiry; or updating documentation; system patch or upgrade. **Low or Minor localised impact.**

The following table describes the target response and fix times for the levels of service for incidents raised.

Priority	Response Time	Target fix time *	Working time
P1	30 minutes	2 hours – resilient solution 4 hours – hardware replacement 5 hours – leased-line connectivity	24 hours, 7 days a week, 365 days a year
P2	30 minutes	8 hours	24 hours, 7 days a week, 365 days a year
P3	120 minutes	32 hours	Monday – Friday 8am – 5:30pm
P4	240 minutes	48 hours	Monday – Friday 8am – 5:30pm

***Target fix times may be limited by 3rd providers and their associated SLA, which may hinder Principle Networks ability to fully restore service.**

Fault Resolution

The Fault Resolution measures apply to Incidents which represent a Service Failure. The duration of a Service Failure and related target maximum Resolution Time is measured, during Contracted Hours, from the point at which the Customer or Principle Networks register the fault within Principle Network's IT Service Management (ITSM) to the point at which Service Failure is no longer present.

Fault Response and Resolution

Principle Networks shall endeavour to respond to and resolve Service Failures within the Response Times and the Target Resolution Times stated above. If it is identified during fault investigation that due to circumstances beyond Principle Networks control, restoration times will exceed the stated target Resolution Times, the Customer will be notified. Principle Networks shall not be liable to the Customer should the Response Times and Target Resolution Times not be met.

Escalations Process

Please raise your escalation by emailing directly to the intended recipient and cc any relevant parties. All previous correspondence should be included. Also please note that when the next escalation has more than one contact, all parties should be included.

Our escalations contacts can also be reached by phone call. If the contact is unavailable, please leave a message and wait for their reply. In the absence of any contacts listed, please be directed to the secondary contact stated in their out of office message.

Should you not receive an acknowledgement to your escalation within the stated timeframe, please escalate to the next level.

A service case priority level is agreed between the customer and Principle Networks when the initial call is raised. The priority level of a given case may be increased by the customer due to a change in circumstances or the amount of time elapsed during the support process. Should a customer feel a case is not being handled as expected the following escalation paths can be followed and available 24/7, also known as a hierarchical escalation:

Escalation Level	Contact	Telephone	Email
Level 1	Senior ServiceDesk Engineer	0333 012 4003	servicedesk@principle-networks.com
Level 2	Head of Service Operations	07572 160 006	richard.tm@principle-networks.com
Level 3	Technical Director	07738 022 937	alex.steer@principle-networks.com

Complaints Process

Principle networks takes great pride on delivering an exceptional service to its customers. Should a customer feel that Principle Networks high standards have fallen short of their expectation the customer should contact the head of service operations by email at:

richard.tm@principle-networks.com

Upon receipt of correspondence from the customer, Principle Networks will respond to the customers complaint within (5) business days.

Continuous Service Improvement (CSI)

Principle Networks take pride in continuously improving and involving its service. We want to work closely with our customers and encourage feedback of the service and where we feel we can add more value and improve.

We encourage feedback after closure of every service case and all feedback is reviewed. Feedback can be about the service, a service feature request or feedback to an individual ServiceDesk engineer. Improvement suggestions and feature requests will be added to Principle Networks continuous service improvement (CSI) register and will be reviewed regularly. Strategic focus for service operations is mainly define by what can be achieved through our continuous service improvement program.

Service Reporting

Service reports such as availability, number of incidents and SLA can be completed on request. The request can be made as a service request, where the service management team will provide appropriate reports based on a customer's requirements this maybe subject to a charge using pre-paid days contracts.

Principle Networks offer a dedicated service management service, please contact your account manager for further details.

Principle networks

Technology Delivered Better

03330 124 003
enquiries@principle-networks.com
www.principle-networks.com