Principle networks

Service Description

Zscaler 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 describes the Zscaler managed service, service levels and enhanced options provided by Principle Networks. This Service Description applies specifically to Principle Networks '**Zscaler Managed Service**'.

Our solutions, services and support are certified against the following standards:

Principle Networks are an Authorised Zscaler Delivery Services and Managed Services Partner.

Zscaler Managed Service Overview

Principle Networks will offer the following as part of the managed service, enhanced options are available to add-on to the service. Please note that Zscaler ZIA/ZPA/ZDX options will be defined within the Scope of works. These Zscaler options can be combined or can be selected on their own.

Service	Managed Service	Enhanced Options
Zscaler Specialised Support	✓	
Continuous Enhancement	✓	
Zscaler Business Review	✓	
Annual Health Check	✓	
Zscaler - Secure Internet & SaaS Access (ZIA)		✓
Zscaler - Secure Private App Access (ZPA)		✓
Zscaler - Digital User Experience (ZDX)		✓
Service Management	✓	
Pre-Paid Days Contracts		✓
Ad-Hoc Service Reporting	✓	
Principle Networks Customer Portal Access	✓	
24/7 Servicedesk	✓	
Access to 3rd Line Engineers	✓	
Failover Testing (Scheduled Intervals)		✓
Co-Management Arrangements	✓	
Escalation Management	✓	
Maintenance Notifications	✓	

Details of the services offered above can be found throughout this document.
Zscaler ZIA/ZPA/ZDX options will be defined within the Scope of works.

Zscaler Managed Service

In today's digital age, cyber security is crucial for protecting your business. Small and medium-sized enterprises (SMEs) often face challenges in keeping up with the evolving landscape of cyber threats. At Principle Networks, we provide a fully managed Zscaler service designed to meet the specific needs of SMEs. We handle the deployment, management, operation, and support of Zscaler's state-of-the-art cyber security solutions — keeping your organisation always protected and resilient.

Supporting a Secure Hybrid Workforce

Enabling a hybrid workforce requires flexible solutions that support employees and third parties wherever they work, using any device. Our Zscaler managed service ensures a fast, secure, and reliable user experience when accessing applications and data. Unlike traditional solutions, Zscaler's modern approach scales with your business and prioritises data protection at every step.

Simplified Security Through Our Zscaler Managed Service

We eliminate the complexity of managing multiple security products by offering a comprehensive cloud-based Zscaler platform. Our managed service reduces operational overhead, allowing you to focus on running your business while we manage your cyber security needs.

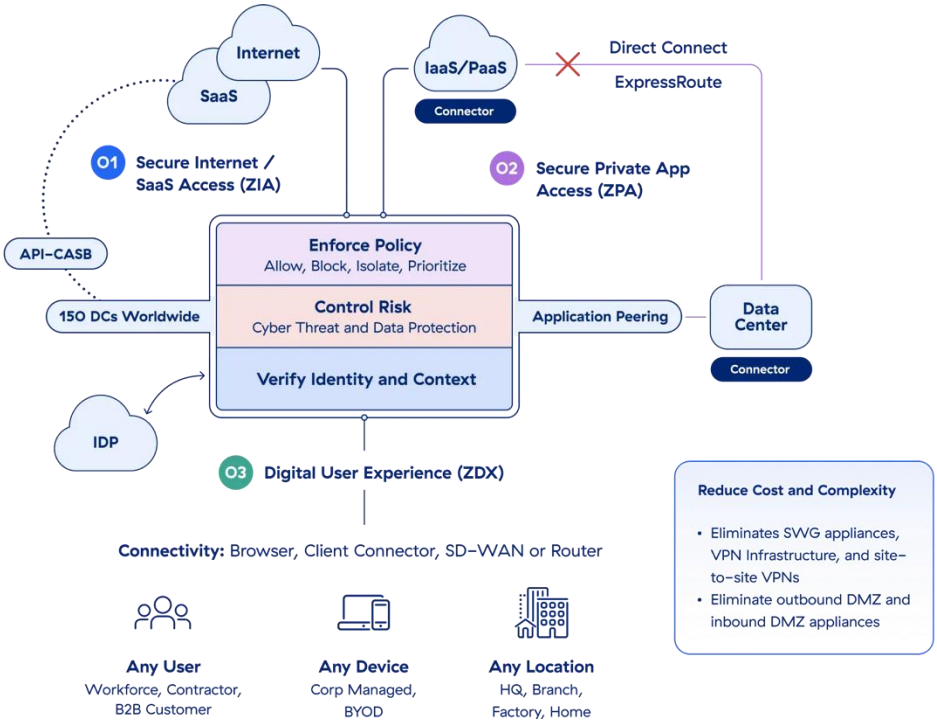
Key Benefits of Our Zscaler Managed Service:

- **Cyber Threat Protection** - A holistic approach to securing users, workloads, and devices against evolving cyber threats.
- **Data Protection** - Complete data security through full TLS/SSL inspection at scale within the Zscaler Secure Service Edge (SSE) platform.
- **Zero Trust Connectivity** (ZTNA) - Secure access to applications — not networks — preventing lateral movement and ensuring a Zero Trust security model.
- **Digital Experience Management** - Continuous monitoring to identify and resolve performance issues, ensuring seamless user experience and productivity.

With Principle Network's Zscaler managed service, you gain peace of mind knowing that your business is protected by experts who manage and maintain your security infrastructure. Stay secure, resilient, and focused on your core business while we handle your cyber security needs.

Zscaler for Users

Zscaler for Users comprises three areas of functionality to improve security, data protection, and digital experiences, all powered by the Zscaler Zero Trust Exchange.



Deployment

The service begins with a comprehensive deployment process. At Principle Networks, we understand that every company is unique, so we take the time to fully understand your specific requirements. Our experts carry out a detailed analysis of your existing infrastructure and workflows to identify your company's needs. Using this insight, we configure and implement the cyber security solution seamlessly, ensuring it integrates smoothly with your systems and operations. Our goal is to deliver a deployment that minimises disruption while maximising protection and efficiency.

Specialised Support

We understand Zscaler's service intimately and have a proven record of accomplishment with customers for delivering excellent solutions with Zscaler at the heart. Like all areas of Principle Networks service, we provide access to our experienced 3rd line Certified Delivery and Support engineers to get problems and queries resolved quickly. Our goal is to minimise prolonged email exchanges that do not lead to resolutions. We encourage our engineers to proactively engage with customers via phone conversations to fully discuss and comprehend the issues at hand.

Principle Networks will add support policies to the customer Zscaler tenant. With customer approval, our engineers can use a secure sandbox to connect to the tenant, reproduce issues, test fixes, confirm changes needed, or escalate to Zscaler, as necessary.

Continuous Enhancements

At Principle Networks we like to approach things a little bit differently. We try to put ourselves in a customer's position and understand what we would want to achieve from a service. We used our knowledge of the service and feedback from existing customers to produce a service that delivers on what customers need and want. We incrementally expand and improve the Zscaler service to deliver the maximum level of security and value from a customer's decision to select Zscaler as a vendor.

We achieve this through regular engagements, where we do the heavy lifting and allow the customer to make the strategic decisions most appropriate for their organisation.

Zscaler Business Reviews

A Zscaler Business Review (ZBR) is a regular scheduled meeting or discussion between Principle Networks and their customer, provided as part of the Zscaler Managed Service. The purpose of this review is to assess the ongoing performance of Zscaler's solutions, discuss key metrics, address any challenges, and ensure that the customer is achieving their desired outcomes from Zscaler's services.

Business Update

Principle Networks have a well-defined business review process broken down into key areas.

Service Management Review

During the review we discuss the current level of service and challenges and then dive into the current state of the Zscaler environment where we can flag any potential issues.

For example:

- We will discuss how well Principle Networks met Service Level Agreement (SLA) Key Performance Indicators (KPIs).
- We will discuss challenges related to service delivery within the customer's business context are addressed.
- High-risk events or security cases are discussed.

Security Review

During the meeting we review the organisations information such as risk and secure score and how those levels compare to other similar organisations and how the posture can be improved. We will also highlight any software upgrades that may be required and implement them as agreed.

Technology Review

This is a key area of the Regular Business Review, during which an experienced presales or Zscaler Certified Delivery Specialist will talk about a key component of the Zscaler solutions that may already have been purchased but are not currently being leveraged. Although not an exhaustive list, example topics discussed during the technical review have been included in the table below.

Zscaler Technology Areas (example)
Disaster Recovery
Browsing Isolation and Privilege Remote Access (PRA)
Data Loss Prevention (DLP) Strategy and Configuration
Zscaler Client Connector Strict Enforcement
ZDX End Users Experience Alerting and Reporting
Sandbox Advanced
Full Zero Trust Network Access (service isolation)
Deception
Source IP address Anchoring
Zero Trust SD-WAN (Branch Connector)

After a knowledge sharing on the agreed discussion area, we can offer several days professional services to implement the technology and support it as part of the managed service moving forwards.

Further to discussing enhancements and improvements to the Zscaler service we end the meeting discussing changes to your business and how that might impact the requirements of your Zscaler solution, the network or security in general. This is a chance discuss what is important to you and your organisation and to ensure

Principle Networks are ready to help adapt or respond to any challenges coming down the road in a proactive manner.

Annual Health Check

As well as the Regular Business Review process described above, once per annum Principle Networks will do a full environment health check of your Zscaler tenant to ensure everything is still configured correctly and to best practice and present the findings during a standalone meeting. Where discrepancies or issues are identified, we will plan and implement Change Requests to implement and rectify them as part of the service.

Secure Internet & SaaS Access (ZIA)

Provide users with fast, secure, and reliable internet and SaaS access while protecting against advanced threats and data loss.

- **Secure web gateway** - Control and protect web traffic from sophisticated threats; includes full TLS/SSL inspection.
- **Cloud firewall & IPS** - Secure all traffic on every device with superior access control and vulnerability protection.
- **Sandbox** - Stop emerging threats with AI-powered malware prevention and inline quarantine.
- **Data loss prevention** - Control and protect web traffic from sophisticated threats; includes full TLS/SSL inspection.
- **Cloud access security broker** - Protect data-at-rest and ensure compliance across SaaS applications.
- **Browser isolation** - Isolate users from suspicious web content without disrupting business workflows.

Secure Private App Access (ZPA)

Connect users seamlessly and securely to private apps, services, and OT devices with the industry's only next-gen zero trust network access (ZTNA) platform.

- **Private cloud and data centre** - Deliver secure access to private apps from anywhere with direct connectivity.
- **Public cloud** - Gain secure zero trust remote access to internal applications running on AWS and Azure.
- **Adversary engagement** - Lure, detect, and analyse attackers with proactive decoy apps that generate high-confidence alerts.

Digital User Experience (ZDX)

Monitor digital experiences from the end user's perspective to optimize performance and rapidly fix application, network, and device issues.

- **Hybrid workforce experience monitoring** - Detect issues that impact user experience, reduce mean time to resolution, and keep employee's productive no matter where they are.
- **UCaaS monitoring** - Ensure optimal experiences with an integrated view of application, network, and device health as well as the audio, video, and sharing quality of Microsoft Teams and Zoom calls.
- **ZTNA (Zero Trust Network Architectures) Visibility** - Regain end-to-end visibility to operate effectively, optimize performance, and rapidly fix issues impacting end user experience and productivity.

Service Management

Principle Networks operate under an ISO 20000:1 accredited Service Management System with telephone, email, and web portal access to raise Incident and service requests which are managed against the following target service levels.

Offering	Description
Network Managed Service	Principle Networks will respond to Service Requests, Change Requests and reports of Incidents submitted by Customers through its Authorised Contacts.
Coverage Hours	24 x 7 x 365
Incident Response Times	Target Response times for Incidents are dependent on the severity level: • P1 - Critical event will be responded within ≤30 Mins. • P2 - Urgent event will be responded within ≤ 30 Mins. • P3 - Important event will be responded within ≤2 hours. • P4 - A request will be responded within ≤4 hours. ***Please see "Service Levels" section of this document for more detail.***
Target Fix Times	Target Fix times for Incidents are dependent on the severity level: • P1 - Critical event, target fix within ≤4 hour • P2 - Urgent event will be responded within ≤8 hours. • P3 - Important event, target fix within ≤32 hours • P4 - A request will be actioned within ≤48 hours. ***Please see "Service Levels" section of this document for more detail.***
Vendor Support Escalation	Principle Networks will escalate items which the Principle Networks Servicedesk team are unable to resolve.

Contacting the Servicedesk

Principle Networks Managed Network Customers have access to the Principle Networks Servicedesk team. Principle Networks Servicedesk can be contacted as follows:

Contact Method	Details
Email	Servicedesk@principle-networks.com
Portal	https://portal.principle-networks.com
Telephone	03330 124 003 (Option 1)

Priority 1 and Priority 2 incidents should be raised via a telephone call to our 24/7 servicedesk number above.

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, 3rd parties or vendors in accordance with prevailing Service Levels. Alternative Service Levels will apply to Change Requests.

Servicedesk Communication and Customer Contacts

Principle Networks Servicedesk communicates with customers through various methods and maintains contact lists with tiers of authority for added security. These contacts can be added to/updated via service request or the customer portal by the named '**Authorised - Including Delegation**'. There are three main contacts that our Servicedesk engineers use to contact customers:

- **Servicedesk Contact** - Is usually a Servicedesk / IT Department distribution list or a named contact who will be contacted by Principle Networks in the first instance.
- **Out of Hours Contact** - Can also be an email distribution list or a named contact who Principle Networks will call/email OOH should this be required.
- **Escalation Contact** - This contact will be used if the Servicedesk and/or OOH contact cannot be reached.

Note: Customer contacts who submit tickets via email or through the customer portal will remain the primary case contact. This can be changed by request, or via the customer portal. In a P1/MSO scenario that is proactively raised by Principle Networks both the Servicedesk Contact and the Escalation contact will be contacted. We recommend that customers use a distribution list (DL) as the primary case contact if more than one person requires updates.

Servicedesk Permissions

For security access reasons Principle Networks has options to set customer permissions for its contacts. These permissions can be updated via service request or the customer portal by the named '**Authorised - Including Delegation**'.

- **Problem Permissions** – Permissions to Raise Problem Cases or Queries.
- **Change Permissions** – Permissions to Authorise or Make Changes, including Service Requests.
- *Options: '**Authorised**' / '**Not Authorised**' / '**Authorised - Including Delegation**'. The latter being a management contact who can manage permissions of other contacts within their business E.g. Head of IT, Director)*
- **Maintenance Notifications** – Will receive notifications relating to maintenance/service. E.g. Planned works or Critical Vulnerabilities effecting supported products. *Options: Allow / Do Not Allow*

Note: Should a contact not be authorised to make changes or raise problems Principle Networks Servicedesk engineers will notify the contact and will request authorisation from a user with '**Authorised - Including Delegation**' permissions.

IT Service Management

The following ITSM processes are implemented:

- Incident Management
- Request Management
- Change Management
- Problem Management
- Configuration Management Database (CMDB) Management
- Continuous Service Improvement

Incident Management

Principle Networks handle Incident Management with precision, adhering to specific Service Level Agreements (SLAs). Each incident is carefully classified and prioritised. Our Servicedesk team then conducts thorough investigations, diagnoses the issue, and ensures swift resolution with root cause, all in accordance with our ISO 20000:1 service management standard.

P1 and MSO Process

Principle Networks have internal Priority 1 incident and major service outage processes to tackle those incidents that need urgent attention.

Request Management

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.

There are two case types that Principle Networks use within our IT Service Management (ITSM) System 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 Management

All changes will be categorised as a change request within with Principle Networks ITSM system and will be sub categorised as Standard or Normal changes. Either change can be assigned a priority level between P1 (Emergency) and P4.

All changes are chargeable with time taken from the customer pre-paid days contract, as described within this 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 as 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.

Multiple changes of the above types or those that are estimated to take longer than 4 hours could be seen a larger piece of work. Where this is the case, the request would be directed through to an account manager to produce a scope of works and will be chargeable based on the scope.

Change Request Authorisation

To ensure security and accountability, all change requests must be submitted by an authorised representative from your organisation. This representative must be pre-approved by an "Authorised - Including Delegation" contact, as defined on page 6. Typically, these individuals hold key roles such as IT Director, IT Manager, or an equivalent position. The "Authorised - Including Delegation" contact is responsible for owning and maintaining the list of approved contacts who are permitted to request or approve changes. For added security, Principle Networks securely stores these authorised contact details within our ITSM system, ensuring that only verified personnel can initiate or authorise change requests.

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) example are:

- Minor software and OS patching
- Security Policy additions
- Traffic Routing (Minor)
- Port and or VLAN Configuration

Normal Change Request

Normal change requests are considered those that do not fall into either a standard change category. 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

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 follow the incident management P1 process and maintain the standard case type of '**Change Request**'.

Problem Management

Principle Networks follows a robust and structured Problem Management process designed to identify, investigate, and resolve the root causes of recurring or major incidents. This process ensures minimal disruption to services and supports continuous improvement in line with best practices. Our approach aligns with the Problem Management guidelines audited and certified under ISO/IEC 20000-1, ensuring compliance with international standards for IT Service Management. Through proactive and reactive problem management, we deliver consistent, high-quality outcomes for our clients.

Continuous Service Improvement (CSI)

At Principle Networks, we are committed to continually enhancing and evolving our services. We actively collaborate with our customers, encouraging feedback on our performance and identifying opportunities where we can add greater value and make meaningful improvements.

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 defined by what can be achieved through our continuous service improvement program.

Pre-Paid Days Contracts

Except for patching for high or critical vulnerabilities, Principle Networks does not include any other changes within the standard service. For other changes, we offer pre-paid day contracts as a flexible solution, allowing customers to incorporate change requests into their Managed Service contract. This can be arranged as part of a monthly allowance or purchased on an ad-hoc basis, depending on the customer's 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 and are handled through the Managed Service for supported solutions.

Time is recorded for all work is in increments of 30 minutes, thus this is the minimum amount of time per change. Anything that is estimated to take over 4 hours or more may be classed within a project scope and will need the appropriate resource assigned to fulfil the requirement and may require a full scope of works and/or project management and may be charged against a separate quote signed by the customer.

Customers have the option to purchase monthly hours that can be used for ongoing service and change. Monthly hours top the customer's recurring hours back to the contracted value of the 1st of each calendar month. Hours not used within the calendar month are lost.

Additionally, there is the flexibility to buy a bank of non-recurring hours, which serve as a reserve that can be utilized as needed. This system provides a convenient way to manage time allocation for services, allowing customers to plan and budget their support needs effectively.

If more time is used in a month than what is contracted, the excess time will be deducted from the non-contracted 'bucket'. If there is no time available in the non-contracted bucket, overuse will result in a negative balance. Any underuse in subsequent months will then reduce this negative balance until it is eliminated. If overuse continues to accumulate, your account manager will reach out to discuss increasing the contracted amount or potentially introducing a hard limit to prevent further overuse of Change time and avoid additional charges.

A monthly report is available to customers to detail hours used and highlight the remaining pre-paid days allowance. This can be enabled by the customer through the Principle Networks Portal or by raising a service request with servicedesk@principle-networks.com.

Note: Pre-paid day time is billed at double the standard rate for out-of-hours (OOH) services. If hours extend into arrears, customers may be required to either pay for the additional time used over the agreed contract or modify their existing agreement to accommodate the increased use of the service. This revision aims to clarify the billing practices for pre-paid time and the options available to customers should they exceed their allocated hours.

Ad-Hoc Service Reporting

High-Level Ad-Hoc Reporting Upon Request (Service Request): Customers can request service reports, including availability, incident counts, and SLA adherence, through a service request. The service management team will generate these reports tailored to the customer's specific needs.

Please note that this service may incur charges, which will be deducted from the customer's pre-paid days contracts. For comprehensive service management solutions, Principle Networks provides a dedicated service. For more information, customers are encouraged to reach out to their respective account manager**.**

Principle Networks Customer Portal

Customers are invited to request access to the Principle Networks customer portal. This portal allows you to track your support tickets, view contracts, and update company contacts. To gain access, please email servicedesk@principle-networks.com. You must be a designated change authority for your organisation, or alternatively, an authorised contact within your company can request access on your behalf.

An existing portal user from your organisation with admin rights can also provide you with portal access by assigning your portal role from the User Management page.

24x7 Service Operation

Managed customers benefit from 24/7 Servicedesk access, ensuring they receive prompt assistance for high-priority incidents or emergency changes. It is important to note that customers need to initiate a phone call to request this level of support. For detailed definitions of each priority level, customers should refer to the Service Level Agreements (SLAs) provided in the appendix of the document. This structure helps maintain an efficient and responsive support system.

Note: Principle Networks collaborate and support your organisation's IT and servicedesk teams, so 1st and 2nd line support for end users within your organisation is still a requirement

Access to 3rd line engineers

Principle Networks ensures that their managed customers have direct access to 3rd line engineers. To delve into what this means:

- Expertise - When you encounter complex technical challenges, our senior engineers bring a wealth of knowledge, skills, and experience to the table. Our engineers swiftly analyse issues, propose solutions, and guide your team effectively.
- Speed - The service operations are automated and technology-driven, ensuring efficiency and saving valuable time. When critical incidents arise, our engineers respond promptly, minimising downtime.
- Quality - Principle Networks adheres to best practice service management standards. Our 3rd line engineers maintain consistency, ensuring high-quality support and governance.
- Assurance - With industry-leading Service Level Agreements (SLAs) and proactive support, you can trust that any network issues will be resolved rapidly, minimising impact on your operations.

Principle Networks' 3rd line engineers play a crucial role in maintaining reliable, secure, and high-performing networks.

Co-Management Arrangements

Principle Networks provide customers with a tiered co-management access (vendor supporting), 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. We expect customers to have access to their own environments (ZPA, ZDX and ZIA administration).

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

Escalation and Management

Any service partner or hardware vendor escalations will be managed by Principle Networks as an integral part of our service. Our commitment extends to ensuring seamless communication and resolution with external partners.

Comprehensive vendor support applies only to Principle Networks managed services. In cases where a service is unmanaged, the responsibility for escalations lies solely with the customer**.**

Principle Networks Escalation

For customers wanting to escalate a part of their Principle Networks service the process can be found in the appendix of this document.

Maintenance Notifications

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 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 selected maintenance contacts to ensure the customers are kept informed of all planned works.

Customers can request maintenance notifications by emailing the servicedesk@principle-networks.com and raising a service request. Notifications can also be stopped using the same method.

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 case number to ensure all parties 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.

False alarms resulting in a pro-active response to the issue by Principle Networks caused by customer maintenance not communicated in advance may be deemed chargeable or recorded against the customer's prepaid days contract.

Service Levels (SLAs)

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	Target 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 party 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	Servicedesk Lead	07399 329 504	adnan.fatah@principle-networks.com
Level 2	Head of Operations	07572 160 006	richard.tm@principle-networks.com
Level 3	Co-Chief Executive Officer	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 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.

Appendix - Minimum Data Set (Incident Ticket)

It is the responsibility of the customer to provide as much information about an incident as possible to enable Principle Networks to respond efficiently and resolve the issue as quickly as possible. Here is a guide to help 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:
- Site contact and access times:
- Specific error messages (if applicable):
- Screenshots attached? Yes/No:
- Troubleshooting steps tried to resolve the issue:

Principle networks

Technology Delivered Better

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