ManagedCare™ Complete

Worry-Free Proactive IT Services

CONTENTS

ManagedCare™ Complete

Statement of Work

This Statement of Work ("SOW") is governed under the Master Service Agreement (The "Agreement") between Reis Informatica Inc. ("Reis") and the client whose name and authorized signatory appear in the signature block of the Master Service Agreement ("Client"), below. Capitalized terms in this SOW will have the same meaning as those in the Agreement unless otherwise indicated below.

Scope of Services

"ManagedCare™ Complete" is meant to deliver proactive preventative maintenance of the agreed-upon network devices (Switches, Wireless access points, UPS units, SAN/NAS, etc.), servers, workstations, and connected systems, as well as helpdesk and remediation services, for one low monthly price. Projects and IMAC tickets (installs/moves/additions/changes) are excluded and delivered at a discounted hourly fee.

The unit of measurement for this service is per seat, server, network switch, firewall, or any other device listed in Schedule "A" under the "System Count" section that falls under the agreement.

As mentioned in item 9 ("Additions") of the contract, If Client wants to add/delete/modify services and equipment to those listed in Schedule "A" under the "System Count" section of this agreement, it may do so subject to the agreement of Reis' Client Success Manager. It shall result in a change to the client's monthly fees.

The following services (collectively, "Services") will be provided to client:

Service Type	Description	Included or Excluded
Proactive Services	• Windows patch management • Infrastructure (Switches, Firewalls, NAS/SAN, Servers, etc) patch management (Firmware/Software) • Virus and spam defense management • Desktop optimization and routine preventative maintenance tasks • Automated Preventative maintenance • Asset management • Warranty management • Monthly health reports • Backup monitoring – detect missed backups • Implementation of basic security practices (For more comprehensive Cybersecurity, we recommend our CYBERSCOPIC SOC-as-a-Service) • Monitoring of systems and detect failures in critical systems	Included
Reactive Services	• End-user help desk support • Troubleshooting for desktop, server, and network issues • Desktop hardware/software installations and upgrades for items in System Count (Schedule "A") with same	Included

	versioning (charges may apply for net-new hardware >2 hours) • Answers to "how to" questions • Mobile device support • Printing assistance • Virus remediation • Response and remediation to alerts raised by our monitoring system. • Onsite Support (travel charges may apply for travel beyond local)	
Cybersecurity Breach Remediation	• If client has subscribed to our CYBERSCOPIC services	Included
	• If CLIENT has NOT subscribed to our CYBERSCOPIC SERVICES	Excluded
vCIO Services	• Strategic planning assistance Performance reporting • Budget planning assistance • IT asset management • Technical Account Manager (TAM) advice as your Virtual CIO/CTO • Quarterly Service Review (QSR)	Included
Network Administration	• Best practices analysis and implementation • Server and network management	Included
Wifi Surveys	WIFI Site Surveys and heatmap reports.	Excluded
After Hours Services	• After hours service for high priority issues only • After hours emergency service is not to be used for general day-to-day admin work, moves, adds or changes.	Emergency Service Included
Data Centre Services	• Services available upon request as part of a separate Statement of Work	Excluded
Basic Security Services (More comprehensive plan available with our S3NTIN3L package)	• Firewall Updating and patching • Updates to antivirus software – not including EDR unless you subscribe to our CYBERSCOPIC services. • Server and workstation security best practices (eg. Enforcing password policy and 2FA) • Removal of users from the local Admin users' group	Included
Public Cloud Operations	• Cloud Management	Excluded Cloud Mgmt. fee needed

IMAC Tickets	• Installs/Adds/Moves/Changes
	  ○ Machine removal
	  ○ Moving Machines/printers (single device)
	  ○ Net New Addition (Hardware/Software)
	  ○ Machine service suspension
	
	• Any significant changes (over 1 hour of time) will require a pre-approved Project SOW
		Included
		Included
		Excluded
		Excluded
		
		Excluded

Systems not covered under the ManagedCare Agreement.

Reis' services under this agreement DO NOT apply to the following types of equipment and hardware (unless purchased through Reis):

- Terminal Server Applications
- Phones/Systems – VOIP, Smart Phones
- Projectors
- Security Systems
- Video Systems, video cameras
- Fuel charging systems
- PLC's or other industrial equipment
- Video Conference Systems

Assumptions & Minimum Requirements

The scheduling, fees and provision of the Services are based upon the following assumptions and minimum requirements:

1. Reis maintains exclusive control over the computer network, firewall, and administrative credentials. You will have access to the administrator credentials. Disclosure of these credentials by the Client to a third party may result in additional fees or, in Reis' discretion, the termination of this SOW for cause.
2. All line-of-business hardware and applications managed under this SOW must always be covered by a vendor support contract at the Client's cost.
3. A vendor support contract must always cover All managed server systems at the client's cost.
4. The client is responsible for providing safe, accessible, clean, consistent, and reliable power to all managed equipment and components, as well as a client environment (including, but not limited to the following, free from excessive heat, cold, static, humidity, water, dust, dirt, vibration, animal or insect infestation). This usually requires a battery UPS on the applicable server system(s) and active line conditioners on the workstation systems. The client must ensure that all electrical outlets are fully grounded. Failure to do so may result in extra charges to repair the resulting damage.
5. If at any time during the term of this SOW, the Client's network firewall is deemed by Reis to be insufficient (no longer under a manufacturer support contract or is end-of-life) for business use, the Client agrees to upgrade the firewall within ninety (90) days of notice of the deficiency from Reis.

Exclusions

The following services are expressly excluded under this SOW:

1. Application development and customization of third-party applications of any kind
2. Modification of Client data in any way
3. Industrial Computing Systems, sensors, RFID or other niche products.
4. Support for operating systems, applications, or hardware no longer supported by the manufacturer
5. Any major operating system version upgrade
    - Example(s): Windows 7 to Windows 10, Server 2012 to Server 2019
6. Data/Voice wiring or cabling services of any kind
7. Entertainment devices
8. Consumer or Prosumer (non-business class) computing or network equipment
9. Database administration (programming, maintaining or other work performed by a DBA)
10. The cost to bring the System up to the Minimum Requirements (unless otherwise noted in "Scope of Services" above)
11. The cost of repairs to hardware or any supported equipment or software, the costs to acquire parts or equipment, or shipping charges of any kind

12. In the case of our data center services, all software licensing is purchased by the client and belongs to the client, including:
    - Hypervisor and/or Server Operating System licenses
    - Client access licenses
    - Remote Desktop Client Access licenses
    - Line-of-business software, its licenses and support contracts

Special Inclusions:

1. We will schedule a maintenance visit, as needed, to do a visual inspection of the systems.
2. We will perform a quarterly test/verification of your data backup system.
3. Other than the scheduled maintenance visit, our technicians don't have regular scheduled visits. However, a technician can be scheduled to visit your location to solve problems or review your systems (Extra charges may apply).

Special Projects Policy

The client may request additional work outside the services listed in this SOW, provided all requests must be finalized in writing between the parties before the extra work commences. These requests will be deemed "Special Projects" and supplied by Reis according to the agreement if the project is expressly approved by Reis in writing (email would be sufficient for this purpose). The following provisions govern Special Projects:

1. Reis will try their best to schedule and complete the Special Project according to the client's requirements, but deadlines cannot be guaranteed.
2. Fees for Special Projects will be assessed hourly (at the current project rate) OR on a fixed-fee basis. Reis and the client will agree.

The general rule of thumb to determine what is considered a project is as follows:

- If the work will affect more than five users
- If the work will affect more than five devices
- If the work will take 5 hours or more to complete

Hardware, Software and Licensing Purchases Policy

Procurement of Hardware, Software, and Licensing requires a 100% pre-payment deposit before Reis can order it from our distributors. We will invoice the client immediately and order the equipment upon receipt of payment.

I understand that all Hardware, Software and Licensing purchases will be invoiced and must be paid for at the time of order.

_____

Authorized Signatory for the Client

_____

Printed Name

Schedule "B"

ManagedCare™ Complete Service Level Agreement

Introduction

As most traditional IT services are based around site visits by technicians, often an SLA has come to be based around that deliverable, meaning the measurable standards are how quickly you see someone on site.
Many services delivered under a Reis ManagedCare™ Complete SLA can be 'invisible' in many ways to a non-technical end user. We seek to make this ' visible ' to ensure that our clients get value for money. To do that, we outline here all tasks carried out as a part of the SLA, what they do, how they work, and how you can tell quickly if they are being done as per the SLA.

Reis's fundamental premise is to avoid on-site visits wherever possible, as this drives up the cost of providing support and slows down the provision. Our service levels are designed to avoid on-site visits and provide better service remotely, which benefits all of our clients.

Response times & Time to Repair Objective

It is challenging to set response times for many of the services that Reis Informatica Inc. ("Reis") provides, as many of them are complex automated services, so the response is immediate. These need much care and attention to ensure they all work correctly, but this maintenance is ongoing and continuous.
However, when you contact us, we will prioritize the incident in the 'Setting Priorities' section and agree to respond within the given time frames.

A response does not merely mean we will let you know we have received your message; it means we will look at your issue, start diagnosis, and we will respond to you respecting four things:

1. An explicit agreement of what the incident is about
2. An owner for the problem both at Reis and your company
3. A clear outline from Reis as to what the next steps are
4. A time to repair objective (an anticipated 'Fix' time)

In furnishing you with this information, Reis has satisfied the 'Response' constituted by this service agreement.

It is extremely important that you discuss the Priority clearly with the Reis representative, as the priority will be set by agreement. The default priority (Low) will be used if you do not specify a priority. It would help if you also were realistic about an incident's priority.
Any incidents set above their allotted Response will be dropped to the appropriate Priority by a senior member of Reis, who will also reset the count time for the incident.

The target Response times set out for ManagedCare™ Complete SLA are as follows:

Priority	Business Hours Response Time	After Hours Response Time	Time to Repair Objective*
Critical (1)	30 minutes	60 minutes	2 hours
High (2)	60 minutes	4 hours (same day)	8 hours
Medium (3)	4 hours (same day)	Next business day	72 hours
Low (4)	72 hours	72 hours	To be discussed

* We strive to take every possible measure to ensure your issue is solved quickly. Specific problems are complex and/or have many variables that may lengthen the repair time. We list a Time to Repair Objective that we have been historically able to achieve however this is not a guarantee.

Priority Definitions

As the setting of Priority for an incident carries such an important weight in service delivery, this must be carried out consistently and fairly for all clients. To ensure this, clear definitions exist to decide what priority any incident will be assigned, and this is based upon the business impact. These definitions are:

Priority	Definition	Example
Critical (P1)	Service not available (all users and functions unavailable)	• Virus Outbreak • Email server failure • Server crash • Network failure
High (P2)	Significant degradation of service (large number of users or business critical functions affected)	• Single virus • Users machine crashed • Internet Outage* • Important file unavailable • Device problem for important meeting
Medium (P3)	Limited degradation of service (limited number of users or functions affected, business process can continue)	• Application fault • File unavailable
Low (P4)	General question, enquiry or problem that does not affect any user's ability to work	• Installs/Moves/Adds/Changes • How do I…? • How much would ….cost?

*Note that an Internet outage is not an emergency priority as it is the responsibility of a third party—your ISP. While Reis will endeavour to identify this as quickly as possible, it is ultimately outside of our control.

If you feel that your incident has not been given the appropriate priority or is not being dealt with quickly enough, you should contact your account manager, as listed in this document. Of course, you are also welcome to contact our Service Manager at any time at escalations@reisinformatica.com.

Privacy & Data Protection

Each party shall ensure that it complies with all the provisions and obligations imposed on it by data protection legislation at all times during the term of this agreement.

For the purposes of this agreement, data protection legislation shall mean the Personal Information Protection and Electronic Documents Act (PIPEDA) of Canada, the General Data Protection Regulation (GDPR), or comparable applicable legislation.

The Reis support system holds only technical data and any contact data as supplied by the client to Reis. Reis will not use this data other than to provide service as outlined in this document. Reis will not share your information with any third parties or use it for its purposes.

Security

Network Access

To provide IT support, Reis must have full administration access to your network and any supported machines. You must agree to this to allow us to fulfill the service's requirements. You must allow access to the Reis support system by opening port 5721 on your network for outbound access or giving permission for Reis to set up such access (a site visit to set this up may incur a charge).

Passwords

Reis will need passwords to access the network environment, including but not limited to Windows Domains, Local Windows admin accounts, Routers, Firewalls, or other critical infrastructure
Reis will set up Admin accounts for its technical access to your systems. We will use a strong password technique. This also means your password is unique to your business but is based on a formula so that it cannot be guessed and does not need to be written down or stored. Reis does not reveal this information to clients, and clients asking for password information will be refused. It is a breach of employment terms for any Reis staff member to disclose any Admin passwords to anyone outside the Reis security team. Doing so will result in the immediate dismissal of the offender.

Security Features of ManagedCare™ Complete

Listed below are the security features implemented by Reis as part of its management system:

The Reis management system is designed with comprehensive security throughout. The Reis system's design team brings years of experience creating secure systems for government and commercial applications.

Reis Agent

The Reis platform architecture is central to providing maximum security. Each computer managed has a lightweight agent installed. The agent initiates all communications with the server.

Firewalls

Reis does not need any input ports opened on client machines. This lets the agent do its job in any network configuration without introducing susceptibility to inbound port probes or new network attacks.

Encryption

Reis protects against man-in-the-middle attacks by encrypting all communications between the agent and server. Since no plain-text data packets are passing over the network, an attacker cannot exploit this.

Secure Access

Administrators access the Reis server through a Web interface after a secure 2FA login process. The system never sends passwords over the network or stores them in the database. Only each administrator knows his or her password. The client-side combines the password with a random challenge issued by the Reis server for each session. The server side tests this result to determine whether or not to grant access. The unique random challenge protects against a man-in-the-middle attack sniffing the network, capturing the random bits, and using them later to access the Reis server.

Web Access

The website itself is protected by Reis Patch Management. The Reis Patch scan is run on the Reis server every day. As soon as new patches are released, the Reis Patch scan automatically detects that they are needed and applies all security patches automatically.

Basic Requirements

Description

This lists the minimum requirements for clients to be able to receive any of the Reis remote management services.

Requirements/Pre-requisites

A supported Windows, Mac, and Linux Based Operating System (server and workstation)
Where the manufacturer drops support for a product, Reis will let you know, and a separate arrangement will be made to upgrade existing hardware/software to meet the manufacturer's new requirement.
All servers/workstations must perform to the specification as outlined by the manufacturer for the given operating system or application system.
Reis Agent installed and working (supplied by Reis)
Broadband or equivalent 'always on' internet connection with at least 10 Mb/s spare capacity. For sites with more than 10 PCs, a higher specification connection may be required.
A firewall/router or similar port-blocking device is set to block all inbound traffic (except where required for internal functionality).
Access to change the firewall device above to allow outbound traffic on port 5721
Machines are left on continuously where possible (unless agreed otherwise) with a power-saving setup to minimize wastage.
A Reis Asset Tag will be displayed on the workstation to help identify the machine for support purposes. It must not be removed.
All hardware and software must be covered by a valid manufacturer/third-party support agreement/warranty. If the client decides not to keep all hardware and software covered by a valid contract, Reis Informatica assumes no liability.
All servers/workstations must have an active SMB grade (or better) anti-virus package.

Client Obligations

Where some part of a client environment does not meet the criteria as specified above, Reis will be unable to set up any service or continue to deliver service to that device or site (if the item affects an entire site) until the environment is brought back in line with Reis's minimum requirements.
Where service is already being delivered by Reis and the environment is changed outside the aforementioned requirements either by the client or a 3rd party, Reis will, at its discretion, continue to deliver service to that environment until it can be brought back into alignment with the requirements, for a period of up to 14 days, or until next payment date is due for the client, whichever is sooner. After this time, if support is to continue, an extra charge will be levied to support a machine outside of the required specification. Generally, this will be three times the typical monthly cost of supporting a machine per month or part thereof.
Unless the changes are directly a result of negligence on the part of Reis or its partners, the client will pay all costs involved in bringing an environment back in line with requirements. Reis will not pay any costs incurred as a result of third parties' actions.
Reis will make all endeavours to warn the client of the costs before undertaking any work, but it will also try to operate in the best interests of the client and the continuation of its business. It may take it upon itself to deliver chargeable services where this would be continuing to operate in the spirit of the previous spending and decisions made by that client in accordance with the perceived business impact or possible service disruption.

ManagedCare™ Complete Managed Services

Continual Review

Requirements/Pre-requisites/Limitations

As per Reis minimum requirements

Frequency

Machines will be set to renew review information every 7 days and to skip if they are not available at the time of the audit.

Deliverable

Upon Request
Report of Licensed Software (as per management software License database)
Complete installed application list (note, this is an extensive report and can only be run as a one-off and not continuously. If this is required in hard copy, the client may incur a printing cost)
Operating System report
Hardware report
System settings

Capacity Monitoring

Requirements/Pre-requisites/Limitations

As per Reis minimum requirements.

Frequency

Machines will be set to provide Capacity Monitoring continuously.

Deliverable

Monthly Executive Report showing available space & total space % breakdown.
Detailed Capacity report available upon request.

Actions

If disk space falls within 15% of the total on any fixed partition, Reis will contact you with this information and suggest corrective action.
Upon disk space reaching 15% of the total on any fixed partition, Reis will run an automatic clean-up to try to free up any unnecessary system files and delete any temporary user files. This is done in the best interests of a machine's health, as a full HDD/SSD on a Windows machine can cause complete failure, so all attempts will be made to avoid that happening.

Exceptions

This service only covers standard fixed HDD/SSD partitions, not external devices such as USB or mapped drives.
The automatic cleanup will not run if the disks are already clean and no further room can be made.
If the disk is filling up extremely fast (within seconds or minutes), then the Reis alert may not be quick enough to catch this. Something would have to already be seriously wrong for this to take place, and under such circumstances, Reis cannot accept responsibility for the capacity of the machine or any failure of the device caused by such. Recovery or fix would be at the discretion of Reis and may be chargeable depending on the circumstances.

Weekly OS Inspection and Cleansing

Requirements/Pre-requisites/Limitations

As per Reis minimum requirements

Frequency

Machines will be set to provide OS Inspection and Cleansing every 7 days and to skip if the machine is not available at the time of the service.

Deliverable

Reis System script and clean up tool using Windows Disk Cleanup.
Entry of cleanup into Reis System logs.
A local pop-up on the machine will warn users that a reboot is pending due to patch management.

Next Generation Anti-Virus Active Protection (Cyberscopic Service Fee required)

Requirements/Pre-requisites/Limitations

As per Reis minimum requirements.
Reis hosted the next-gen anti-virus software.
Reis may remove other anti-virus programs from your machine if they interfere with service delivery.

Frequency

Continually active scanning ensures the anti-virus program is activated.

Deliverable

The executive summary includes a list of all machines with active anti-virus protection.
A log entry will be created on Reis's system so that separate reports can be generated if necessary.
Anti-virus is up to date.

Actions

If a virus is found on a machine, an alert will be sent to the Reis SOC (Security Operations Centre). The automatic cleanup should remove it, but the ticket this alert will raise will be followed up to ensure this is the case.

Exceptions

While Reis will make every effort to ensure your machine is safe from viruses, we do not guarantee that your machine cannot be infected in exceptional circumstances. Where this does happen, any resulting support or service required may be chargeable to the client at the discretion of Reis but with consultation with the client.

Desktop Policy Enforcement

Requirements/Pre-requisites/Limitations

As per Reis minimum requirements.
Windows active directory and group policies (or Azure active directory).
Professional operating system.
Explicit agreement with Client regarding current corporate policy.

Frequency

This is a continuous service, but the details of the desktop policy will be reviewed annually or more often on request.

Deliverable

Login policy (times, places, etc.).
Accounts policy (admin settings, user account usage, own account, etc.).
Corporate Screensaver.
Block Access to agreed-upon programs.
File Shares on machines (should be none).
Installation of other Applications:
Must be performed only by Reis staff.
Must meet both a business requirement and will not affect the security and/or the stability of the network, computer or any other system managed and maintained by Reis.

Actions

Reis will consult with the client to create a policy if there isn't one already.
Reis will set up a way to implement the policy.
Reis will monitor the policy through software.

Exceptions

Users who are given local admin rights will always be able to circumvent policies; therefore, Reis cannot enforce a policy where the user is a local administrator.
Please note that policy enforcement can restrict users' ability to perform actions on their machine(s) which may mean they need to contact Reis to execute some actions on their machines, causing delays to some actions. Reis will always try to keep these delays to a minimum but accepts no responsibility for any inconvenience caused by such delays, as this service is in place to protect the client's security.

Security updates to Microsoft Software

Requirements/Pre-requisites/Limitations

As per Reis minimum requirements.

Frequency

Daily scans to assess patch requirements.
Daily patching of workstations to ensure reliability, security, and compliance.
Servers are patched weekly based on an agreed-upon schedule.
Exceptions – by mutual agreement (Reis and client) – client to accept inherent risks.

Deliverable

As per Microsoft's recommendations, the latest patches will be installed on all managed machines.
Executive Summary of machine patch compliance.
Script log entry, so a separate report is possible.
Detailed patch report available on request.
If a patch fails to install, an alert will be raised to the Reis SOC (Security Operations Centre).

Actions

Any issues raised to the Reis SOC will be dealt with as a medium-priority ticket.

Exceptions

Where a patch/hotfix causes system problems on a client machine, Reis staff will roll back the patch/hotfix to try to resolve the issue.
Patches come from Microsoft, not Reis; therefore, Reis cannot be responsible for any adverse reaction that a patch might have to any machine's configuration.

Onsite Visit Policy for ManagedCare™ Complete SLAs

Requirements/Pre-requisites/Limitations

Reis will only send a technician onsite where all other options have been exhausted.
The Technician will only stay onsite for the length of time required to address the issue at hand and will not undertake any other work while onsite unless this is agreed to by a Reis Account Manager and any extra time and expense agreed to by the client.

Frequency

If required, regular on-site maintenance visits will be scheduled with the client based on the maintenance plan. Any other on-site visits will be scheduled on an as-needed basis.

Deliverable

Reis will adhere to the client's on-site policies and procedures.
Local travel is not chargeable to the client within the Waterloo-Wellington Region of Ontario.

Exceptions

Where the client site is more than 50 km one-way from Reis, travel will be charged hourly by agreement. Costs may also be incurred for travel by means other than a car, and some reasonable charge for mileage will also be made if the site is over 50 km away from Reis.

Scheduled Maintenance Visit.

Requirements/Pre-requisites/Limitations

Reis may send a technician to your central office location to perform a list of administrative tasks.
The Technician will only stay on site to perform the required administrative tasks and will only undertake other work while on site if a Reis Account Manager agrees. Any extra time may be chargeable.

Frequency

As agreed.

Deliverable

The following is a list of administrative tasks the technician may perform every month.

Verification of Server's memory utilization, CPU performance and free disk space usage
Verification of a workstation sampling of the event logs, looking for anomalies
Verification of processes that are running
Verification of a workstation sampling and ensuring the virus software is installed and operating
Verification of the data backup system and ensuring that backups are being performed
Testing a restore of the data backup system, testing the restore procedures. Correct any problems detected.
Optional maintenance operation of workstations that are having problems with remote management procedures. Correction of our management agent.
Physical inspection of computers, servers and networking equipment.
Ensure that network cabling at the rack isn't being physically strained
Ensure that server lights and sounds are in a normal state and deal with any visible or audible alerts
Verify that there is no potential for equipment that could be physically harmed by cleaning staff (such as computers sitting directly on the floor). Immediately notify if a potential issue is spotted.

Exceptions

Where the client site is more than 50 km travel one way from Reis, travel will be charged hourly by agreement. Costs may also be incurred for travel other than a car and some reasonable charge for mileage if the site is over 50 km away from Reis. This will also be by agreement.
Where the client has more than one site, only the main office or the office with the primary server systems will be visited.

Monthly Reports

Requirements/Pre-requisites/Limitations

As per Reis minimum requirements.
Email address supplied for primary site contact.

Frequency

Updated Monthly.

Deliverable

Executive Summary.
Other reports may be available upon request from your Client Success Manager.

Maintenance Windows

Requirements/Pre-requisites/Limitations

Please ensure you save all open documents and work before the end of the day to avoid data loss if your system reboots overnight.
Normal server maintenance will be conducted on a scheduled basis. A designated time frame (weekly) will be used to maintain the servers during a 2-hour outage window. The servers may or may not be available for use during this period.
Email address supplied for primary site contact.

Frequency

Server Schedule: Updates will be checked and installed once a day from 12 a.m. to 6 a.m. The server will be rebooted once weekly (day of the week). A one-hour extension may be required during the Server patching window.
Desktop/Laptop Schedule: Updates will be checked and installed daily, and a reboot will be prompted only if one is required. The daily reboot can be deferred up to three (3) times before it is enforced. A weekly reboot will also be executed on Sunday from 1 a.m. to 6 a.m. as part of our proactive maintenance program.

Deliverable

Notify site contact if maintenance was performed and if there are any noticeable changes or action items for which users must be notified.
This process will allow us to stay on top of the latest updates and patches to improve issues and the overall security of your systems.
Monthly patch management reporting.

Unscheduled Downtime

Requirements/Pre-requisites/Limitations

An unplanned outage may occur without adequate user notification.
Reis Informatica Inc. will make a "best effort" to notify the main contact in certain circumstances, such as when the network (whole or part) is effectively out of service due to hardware or software failure.

Deliverable

Notification to site contact if such unscheduled downtime was performed and if there are any noticeable changes or action items that users must be notified of.
The downtime will be investigated, and its findings and any actionable items will be conveyed to the site contact.

Scheduled Downtime

Requirements/Pre-requisites/Limitations

The site contact will be notified via email at least 7 working days (or a mutually agreed-upon time) in advance of any planned maintenance or upgrades likely to affect service availability.
Downtime will be scheduled outside core business hours when possible.
Urgent downtime notices will be sent via telephone to the designated Contact Person, who will notify the users appropriately.

Frequency

As required – outside the patch management pre-authorized downtime window.

Deliverable

Notify site contact if maintenance was performed and if there are any noticeable changes or action items for which users must be notified.