IT Support Services & Charter

V1.1

rydal™ Infotech

Making IT work seamlessly

Table of Contents

1. INTRODUCTION

This document specifies the scope and deliverables of the Services delivered to the Client by Rydal Communications Ltd for users/devices on-boarded to Rydal IT Support services.

Rydal may make minor amendments to this charter from time to time for operational reasons, provided that such amendments are reasonable and do not materially affect the nature and scope of the Services to be provided to the Client.

2. NATURE OF SUPPORT SERVICES

Rydal's IT Services comprise remote device management designed to troubleshoot issues with IT applications and services, including the provision of remote technical services required to resolve issue(s) detected by our Remote Monitoring and Management (RMM) Software. IT Support services are only provided directly to the Client, not to third parties. IT Support Services are provided to the Client via one of the following options:

2.1. Directly Supported RMM software (Rydal Provided)

If the Client is using our RMM software that is directly supported by Rydal, IT Support Services will be provided using Rydal's own instance of that software.

Where the Client is using directly supported RMM software, they will be required to assist the Rydal IT team with access to end user devices as and when reasonably required to provision such software, in order for IT support services to commence. Such assistance should be given within a reasonable timescale and should not be unreasonably withheld.

2.2. Unsupported RMM software (Third Party Provided)

Where the Client is using their own unsupported RMM software, Rydal IT Support services will need to be provided access and relevant training to ensure we understand how to effectively use the tool available to best provide support. We will include optional anti-virus and anti-malware software if requested.

Client Responsibilities

In all cases the Client is responsible for informing the Rydal IT team if a monitoring agent has been decommissioned or is no longer required. If a supported device is shown as unavailable and the monitoring agent is not able to accept maintenance tasks, the Rydal IT team will communicate with the Client to verify whether the agent has been decommissioned or has connectivity issues. If the Client confirms that the device has been decommissioned, then the Rydal IT team will remove the monitoring agent and notify the Client's Account Manager accordingly. Maintenance tasks for workstations that are unavailable during the agreed maintenance window will be re-scheduled to the next agreed maintenance cycle.

The Client is responsible for ensuring that the Rydal IT team can access the relevant supported devices for scheduled maintenance and remediation as required.

• Wherever possible, we ask you to e-mail us your request so we can:
o Log and track issues accurately.
o Offer you the expertise of all our staff.
o Better understand and direct your query.
o Reduce the time spent transcribing calls.
o Ensure we have an accurate record of all communications.

We ask for 72hrs notice for changes/additions to your IT system including:
o New us-ers, software or hardware installations and office reorganisation.
o All calls will be prioritised according to the response times set out in your Managed Services Agreement

2.3. Coverage

IT Support Services will be provided according to the hours of coverage per service detailed on the relevant e-Quote/Order. Services are provided on the following basis:
• 24/7/365 – 24 hours a day, 7 days a week, 365 days a year
• In hours – your normal business hours, Monday to Friday only, excluding public holi-days
• Out of hours – outside of your normal business hours, 7 days a week including public holidays

3. TYPES OF SERVICES DELIVERED

The following core services are delivered via the Rydal IT Support Services:

3.1. Monitoring & Noti ication Services

IT Support Services use the customised notification profiles created based on Rydal's best practices that have been defined for each server, product or role by the Rydal IT Support team. These will be pre- selected during the on-boarding process and are not customisable. However, from time to time the Rydal IT Support team will update the best practices monitoring templates and notification profiles to reflect new up-dates and product enhancements released by the respective vendors. If required by the Client and if deemed feasible by the Rydal IT Support team, the best practices notification profiles can be customised either during the on-boarding process or later, as required. The Rydal IT Support team will only provide support for those templates that the Client has pre-selected. Where the Client requests a change to be made to Rydal's monitoring template, for example, adjustment of the monitoring threshold, such requests should be put forward to the Rydal IT team for review in the first instance.

3.2. Remote Remediation
Remediation work will only be carried out for monitored services via Rydal's monitoring templates. The Client can request the scheduling of an issue remediation task out of office hours to avoid disruption to the Client Customers If the client has appropriate OOH (Out of Office hours) coverage, they can request to schedule any remediation work out of office hours to avoid disruption to the client customers.

3.3. Automation
Where the facility exists within the Client's or Rydal's Remote Monitoring and Management (RMM) Software, remediation work may be automated to increase the efficiency of service delivery if deemed advantageous by the Rydal IT Support team.

3.4. Root Cause Analysis (RCA) Services
Root Cause Analysis (RCA) will be carried out by the Rydal IT Support team for unexpected shutdown/reboot of servers only. RCA will be carried outside the standard Service Level Agreement.

3.5. Rydal Best Practices
During the On-Boarding process Rydal will review the existing policies setup and apply Rydal best practices to certain monitors. This might result in adjusting delays and threshold modifications or creating new monitors (where the facility exists). This will help Rydal to reduce white noise and increase the efficiency of monitoring.

3.6. Preventive Maintenance
Planned maintenance activities will be carried out to avoid any unplanned outages within an IT infrastructure. The service covers the following:
• Windows Patch Management – security and critical patches are deployed on a scheduled basis via the RMM.
• Anti-virus/Anti-malware updates – maintenance of definition updates for supported anti-virus and anti-malware products
• Disk clean-up & temporary file deletion
• Disk health check

3.7. Triaging Service
Received alerts will be triaged by the Rydal IT Support team and failed alerts will be escalated back to the Client's Primary Technical Contact or other designated parties as per the defined escalation process.

3.8. Third-party Vendor Coordination & Management
As required, the Rydal IT Support team will make first contact with relevant third-party vendor(s) on the Client's behalf, provided that the vendor(s) details have been supplied by the Client during the on- boarding process. Once first contact has been made, the Rydal IT Support team will carry out any vendor recommended diagnostics in the first instance. If the issue persists and/or cannot be progressed further, the Rydal IT Support team will escalate the incident back to the Client for further action, according to the escalation process detailed in the Service Level Agreement below.

3.9. Projects

A Project is defined as an out-of-scope planned task, (or series of planned tasks) that has a defined start and end date, along with definitive milestones (if applicable). Project work can be requested for both monitored and unmonitored devices for supported technologies. A current list of supported technologies can be found within Supported Items and Services. Projects will be billed at Rydal's Standard Project Rate.

3.10. Types of device

The Rydal IT Support team will deliver Services for the following device classes including virtualised environments.

- Workstations
- Servers
- Network devices

If monitoring and management of multiple VLANs on a network device is required, each VLAN will be treated as a separate network device.

4. SCOPE OF SERVICES FOR IT SUPPORT SERVICES

The scope of Services offered is dependent on the package and type of Support Services taken. Services are packaged as follows:

4.1. Workstation standard.

Alerts received for Windows Patching and anti-virus/anti-malware definition updates will be analysed, prioritised and corrective action will be taken. Detected AV threats will be triaged and escalated to partners' attention.
Package includes: Windows Patch Management, AV Management.
Root Cause Analysis (RCA) services and service requests are not included.

The Rydal IT Support team will monitor and take corrective action based on the notifications received. The following standard monitors will be configured.

- Patch failures
- Reboot required status
- AV definition update
- AV threat detection

The standard polling level for workstations is every 4 hours.

* In order to regulate alert frequency within acceptable parameters, the Rydal IT Support team will configure an appropriate delay trigger for certain monitored services.

Preventive maintenance

The Rydal IT Support team will perform maintenance activities on a scheduled basis as follows:

- Windows patch management – security and critical patches will be automatically deployed and applied for supported Microsoft operating systems to Rydal's pre-defined schedule.
- Apple Mac patch management - security and critical patches will be deployed to Rydal's pre-defined schedule.
- Anti-virus/Anti-malware updates – definition updates for supported anti-virus and anti-malware products.

Maintenance Schedule

Maintenance Activity	Schedule	Details
Windows patch management	Monthly	Microsoft critical and security patches will be approved automatically and installed during the agreed scheduled maintenance window. A workstation reeboot will be intiated if required.
Apple Mac patch management	Monthly	Critical and security patches will be installed during the agreed scheduled amaintenance window. A workstation reboot will be initiated if required.
Anti-virus/Anti-malware***	Daily	all definition and signature updated are performed on a daily or as needed basis

* Corrective action will be taken to fix a failed patch and any consequential issues within the standard SLA and if required, this may be escalated back to the Client for assistance and/or further action.
** In the case of application or definition update corruption, the Rydal IT Team will remediate the issue and any consequential issues within the standard SLA. Alternatively, the Client can request the scheduling of an issue remediation task out of office hours to avoid disruption to the Client. Where anti-virus/anti-malware software licensing has expired, the Rydal IT Support team will escalate to the Client for further action.

Anything not listed here or within Supported Items and Services is considered out of scope

4.2. Workstation

Alerts received will be analysed, prioritised and corrective action taken. Patching, anti-virus/anti- malware definition updates and other maintenance activities will be carried out on a scheduled basis.
Package includes: Monitoring and notification, remote remediation, preventive maintenance services and vendor management for monitored Microsoft Windows and Apple Macintosh workstations.
Root Cause Analysis (RCA) services and service requests are not included.
The Inbay NOC team will monitor and take corrective action based on the notifications received. The following standard monitors will be configured.

- CPU
- Memory
- Disk space
- Anti-virus and anti-malware status

The standard polling level for workstations is every 4 hours.

* In order to regulate alert frequency within acceptable parameters, the Rydal IT Support team will configure an appropriate delay trigger for certain monitored services.

Preventive maintenance

The Rydal IT Support team will perform maintenance activities on a scheduled basis as follows:
• Windows patch management – security and critical patches will be automatically deployed and applied for supported Microsoft operating systems to Rydal's pre-defined schedule.
• Apple Mac patch management - security and critical patches will be deployed to Rydal's pre-defined schedule.
• Anti-virus/Anti-malware updates – definition updates for supported anti-virus and anti-malware products.
• Disk clean-up & temporary file deletion (Microsoft Windows only).
• Disk health check. (Microsoft Windows only).

Maintenance Schedule

Maintenance Activity	Schedule	Details
Windows patch management	Monthly	Microsoft critical and security patches will be approved automatically and installed during the agreed scheduled maintenance window. A workstation reeboot will be intiated if required.
Apple Mac patch management	Monthly	Critical and security patches will be installed during the agreed scheduled amaintenance window. A workstation reboot will be initiated if required.
Anti-virus/Anti-malware***	Daily	all definition and signature updated are performed on a daily or as needed basis
Disk cleanup***	Monthly	Temporary files are removed
Disk health- check	Monthly	Disk issues are identified and flagged as appropriate

* Corrective action will be taken to fix a failed patch and any consequential issues within the standard SLA and if required, this may be escalated back to the Client for assistance and/or further action.
** In the case of application or definition update corruption, the Rydal IT Support team will remediate the issue and any consequential issues within the standard SLA. Alternatively, the Client can request the scheduling of an issue remediation task out of office hours to avoid disruption to the Client Customers. Where anti-virus/anti-malware software licensing has expired, the Rydal IT Support team will escalate to the Client for further action.
*** If execution of the temporary file removal process causes a related system issue, the Rydal IT Support team will remediate the issue and any consequential issues, within the standard SLA.

Anything not listed here or within Supported Items and Services is considered out of scope.

Service Requests
Out-of-scope services (Service Requests) for workstations can be carried out for monitored devices if the Client has a valid Service Desk Services contract in place for the relevant Client Customer(s). Such requests will be undertaken by the Inbay Service Desk.
Examples of Service Requests include (but are not limited to);

- Email account configuration
- Application installation and troubleshooting
- User password resets

4.3. Server
Alerts received will be analysed, prioritised and failed alerts will be triaged back to the Client for remediation.
The Rydal IT Support team will monitor the following standard services and any additional services agreed during on-boarding for failures and triage alerts based on severity. Standard monitoring includes:

- Heartbeat
- Critical Windows or Linux daemon(s) availability
- CPU, Memory, Paging/Swap file & Disk space
- HTTP/HTTPS
- Anti-virus/Anti-malware
- Backup

Preventive maintenance, remediation, Add-On's, vendor management and Root Cause Analysis (RCA) services are not included.
Anything not listed here is considered out of scope.

Alerts received will be analysed, prioritised and corrective action taken. Windows patching, anti- virus/anti-malware definition updates and other maintenance activities will be carried out on a scheduled basis.
Package includes: Monitoring and analysis of failed alerts, preventative maintenance, remediation, , vendor management and root cause analysis (RCA)

Monitoring & notification
The Rydal IT Support team will monitor the following critical services and any additional services agreed during on-boarding for failures and triage alerts based on severity. The monitoring includes:

- Heartbeat
- Critical Windows or Linux daemon(s) availability
- CPU, Memory, Disk space
- Anti-virus/Anti-malware
- Backup*

*The Rydal IT Support team will monitor for backup job failure and take corrective action to remediate the issue. All media unavailable, tape cleaning or backup hardware issues will be escalated back to the Client.

Remote Remediation and Root Cause Analysis (RCA)
The Rydal IT Support team will carry out remediation work on the notifications received. Root Cause Analysis (RCA) will be carried out by the Rydal IT Support team for unexpected server shutdown or re- boots only.
The RCA process will commence once the server is back online and the following activities will be carried out to determine the root cause:
• Analysis of the event logs
• Analysis of the memory dump file
• Review of hardware diagnostic logs

An RCA report will be produced and shared with the Client. This will give an overview of the incident, the corrective action(s) taken and list any recommendations to prevent future occurrence.

Preventive maintenance
The Rydal IT Support team will perform maintenance activities on a scheduled basis as follows.
• Windows patch management – security and critical patches will be automatically deployed and applied for supported Microsoft operating systems to Rydal's pre-defined schedule.
• Anti-virus/Anti-malware updates – definition updates for supported anti-virus and anti-malware products.
• Disk clean-up & temporary file deletion.

Maintenance Schedule

Maintenance Activity	Schedule	Details
Windows patch management	Monthly	Microsoft critical and security patches will be approved automatically and installed during the agreed scheduled maintenance window. A workstation reeboot will be intiated if required.
Apple Mac patch management	Monthly	Critical and security patches will be installed during the agreed scheduled amaintenance window. A workstation reboot will be initiated if required.
Anti-virus/Anti-malware***	Daily	all definition and signature updated are performed on a daily or as needed basis
Disk cleanup***	Monthly	Temporary files are removed

* If execution of the patching process causes a related system issue, the Inbay NOC team will remediate within the standard SLA.
** In the case of application or definition update corruption, the Inbay NOC team will remediate the issue and any consequential issues within the standard SLA. Alternatively, the Client can request the scheduling of an issue remediation task out of office hours to avoid disruption to the Client Customers. Where anti-virus/anti-malware software licensing has expired, the Inbay NOC team will escalate to the Client for further action. If the Anti-virus/ Anti- malware update event(s) failed during the scheduled time, the Inbay NOC team will investigate the issue(s). If two consecutive scheduled events have failed and/or if the latest definition versions have not updated within 48 hours, then the Inbay NOC team will remedy the issue within the standard SLA.
*** If execution of the temporary file removal process causes a related system issue, the Inbay NOC team will remediate the issue (along with any consequential issues) within the standard SLA. Alternatively, the Client can request the scheduling of an issue remediation task out of office hours to avoid disruption to their Client Customers.

Sanity check Process
The Rydal IT Support team will carry out sanity checks after patch installation and upon rebooting to:

• Check the monitored Windows services for any failures and remediate issues.
• Check the server heartbeat and escalate back to the Client if the server is down within the standard SLA.
The services will be carried on an automated basis via the RMM.

Service Requests
Any pre-approved service requests by the client can be carried out for supported devices. Examples of Service Requests include (but are not limited to);

• Group Policy Object management
• Microsoft Exchange Email Connector configuration
• Security Certificate installation

Suitable for managed and unmanaged devices.

All alerts received will be analysed, prioritised and triaged back to the Client for remediation work.

Package includes monitoring and notification of critical alerts.

The Rydal IT Support team will monitor the following standard services and any agreed additional services (where the facility exists) for failures and triage alerts based on severity. Standard monitoring includes:

• Device heartbeat
• CPU, Memory, Utilisation
• Interface status
• Interface Traffic Utilisation
• System Temperature
• Fan Status

Only devices that support SNMP can be monitored.

Preventive maintenance, remediation, Add-On, vendor management and Root Cause Analysis (RCA) services are not included.

Suitable for managed devices only.

Only devices that support SNMP can be monitored.

Preventive maintenance, remediation, Add-On, vendor management and Root Cause Analysis (RCA) services are not included.

Suitable for managed devices only.

Alerts received will be analysed, prioritised and corrective action taken. Preventive maintenance (back-up of network device configuration only). Remediation, Add-On and vendor management are included.
Root Cause Analysis (RCA) services are not included.

Package includes: Monitoring and notification, remediation and preventive maintenance services.

The Rydal IT Support team will monitor the following standard services and any agreed additional services (where the facility exists) for failures and triage alerts based on severity. Standard monitoring includes:

- Device heartbeat
- CPU, Memory, Utilisation
- Interface status
- Interface Traffic Utilisation
- System Temperature
- Fan Status

Only devices that support SNMP can be monitored.

Remote Remediation
Alerts received will be analysed, prioritised and remediated within the standard SLA.

Preventive Maintenance
Where the facility exists, the Inbay NOC team will administer the automated back-up of the network device configuration for each supported network device on a monthly basis Back-ups will be stored on a shared drive on the Client and/or Client Customer's specified local server. Where automated back-up of a network device is not available, the Inbay NOC will not administer the back-up of that device

Maintenance Schedule

Endpoint Computer
Monitoring & Notification
Automation Service
Remote Remediation
Windows patch management
Antivirus/Antimalware updates
Automated disk clean-up & health check services
24/7 coverage (If Applicable within Contract)

Servers
Monitoring & Notification services
Automation
Remediation and RCA services
Patch management
Service requests
Vendor management
24/7 or in-hours or OOH coverage (If Applicable within Contract)

Servers
Monitoring & Notification services
Remediation and RCA services
Vendor management
Service requests
24/7 or in-hours or OOH coverage (If Applicable within Contract)

5. EXCLUSIONS FROM IT SUPPORT SERVICES

Any services or items not explicitly covered within this IT Support Charter are considered out of scope.

a) problems occurring with unsupported software applications or devices.

b) onsite support.

c) SharePoint set-up or administration.

d) network device firmware updates.

e) Application of software updates and patches for third party applications other than as specified in Supported Items and Services. Any requirement for the application of unsupported updates and patches will be escalated back to the Client or the Client's nominated technical contact for review and at the Client's request can be treated as a project-based task as outlined in paragraph (s) below.

f) where any software or services are being used illegally or with expired, invalid or discontinued licenses.

g) dealing with any inappropriate materials, content or software, including those that infringe any applicable laws, regulations or third-party rights (including material which is obscene, indecent, pornographic, seditious, offensive, defamatory, threatening, liable to incite racial hatred, menacing, blasphemous or in breach of any third party's rights);

h) any software or services used for gambling, online trading, commodities exchanges or any other real-time financial data application.

i) any software or services which conduct or facilitate illegal or objectionable activity, such as (but not limited to) unsolicited bulk email, email harvesting, unlawful MP3 content collection and distribution.

j) systems or software that may be prejudicial or damaging to the software and services used by Rydal and its other clients, including (but not limited to) malware and viruses.

k) project-based tasks, being any remediation or support work that sits outside of the scope of the IT Support Services as detailed above, including (but not limited to) migration of data; server consolidation; server rebuilds, major system configuration changes and operating systems upgrades, re-installation or re-imaging; mass installation or re-installation of software; set-up or relocation of device(s); creation and application of customised scripts and automation policies.

l) any services required to bring the Client's or the Client Customers' IT systems and/or network environments up to the required standards for the receipt of the Rydal IT Support Services, which will be regarded as a project-based task, as detailed above;

m) any software programming or systems design services including modification of source or object code or any software maintenance.

n) any training, consulting, design or implementation services.

o) where the Client has its own Remote Monitoring and Management (RMM) software and/or host systems, Rydal IT Support Services excludes management and maintenance of the software and host system(s) themselves.

p) If the Client has made unauthorised changes to the configuration or set up of equipment,software or services, this Agreement may not apply.

q) If the Client had prevented the Supplier from performing required maintenance and updates, there may be a delay in resolving IT System issues.

This Agreement does not apply to circumstances that could reasonably be said to be beyond the
Supplier's control. For instance: floods, war, acts of God, virus outbreaks, quarantines and so on.

This Agreement also does not apply if the Client fails to pay agreed supplier invoices on time.

The Supplier reserves the right to halt all services including support should the Client be provably holding back payments without explanation or reasonable expected timeframes.

The Supplier will always aim to be helpful and reasonable and accommodate requests where possible for the mutual benefit of both parties.

6. STANDARD SERVICE LEVEL AGREEMENT (SLA)

Our service is delivered on best endeavours. We aim to resolve all IT issues as swiftly as we can, and as a result the SLAs above should only be used as a rough indicator. The vast majority of calls are resolved VERY quickly, however, it must be noted that the above SLA times in no way relate to a guaranteed fix time. If this is required, we are happy to provide an alternative IT support agreement which can include this feature.

For the purposes of the IT Support Services, Rydal adopts the following priority categories:

• P1 Critical Priority: incident affects more than 75%business-critical functions in one area.
• P2 High Priority: incident affects multiple machines/users and several business-critical functions in one area.
• P3 Medium Priority: one device/user is affected moderately and there is some productivity loss or multiple machines/users are affected with only minor loss of productivity.
• P4 Low Priority: one device/user is affected. The issue relates to only a minor enhancement. There is no productivity loss.

For service requests the target resolution time is 48 hours.

The following table shows the target response times for each priority level along with the target resolution time for Service request requests.

All IT support is provided as per our charter and delivered in accordance with the priority-based system detailed below:

Category P1	**-1hr Response**	**-IT failure across the entire company or major security risk**
Category P2	**- 2hr Response**	**- IT issue stopping multiple users or a VIP from operating**
Category P3	**- 4hr Response**	**- IT issue stopping a single user from operating normally**
Category P4	**- 8hr Response**	**- IT issue inconveniencing a single or multiple user(s)**

* Rydal IT Support Service fault reporting is automatically identified by Rydal via the Client's or Rydal Remote Monitoring and Management Software or is reported by the Client via email or telephone.

First response time shall be calculated from the time that Rydal identifies the fault after initially reviewing the alert or when the Client reports the issue to Rydal Communications and Rydal has acknowledged receipt.

• The Rydal IT Support Services shall be provided to the Client by all or any of the following means as detailed, and during the times referred to, in the relevant order:
o email via a designated email address.
o telephone via a designated telephone number.

• All SLA times shown are target times, which are for guidance purposes only and time shall not be of the essence.

6.1. SLA Responsibilities

• The Client shall ensure that support requests are made via the appropriate support channels, by authorised users of the Service.

• The Client must supply (and not unreasonably withhold) important or accurate information at the outset or when requested subsequently by Inbay.

• The Client and any related third party must respond to or act upon Rydal's reasonable instructions and/or requests for assistance in a timely manner.

• Rydal can provide the Client with a monthly report detailing its performance in respect of the SLA.

• Rydal and the Client shall monitor and review SLA performance and the provision of the Services at meetings wherever felt necessary (not more than once a month).

• Prior to any meeting, each party shall notify the other of any problems relating to the provision of the Services for discussion at the meeting. At the meeting, the parties shall agree a plan to address such problems.

• Rydal shall not be deemed to be in breach of the SLA in the event that a crucial element of the relevant IT system is not available to Rydal to permit it to provide the Services, including (but not limited) to the Client's or Rydal's Remote Monitoring and Management (RMM) software and/or host systems, Professional Services Application (PSA) systems, lack of internet connectivity at the Client Customer or Client's location(s) or in any other circumstances outside of Rydal's reasonable.

• control such as (but not limited to) reliance on a third-party vendor or service provider for relevant information, timely action or response, or in any other circumstances that would amount to a Force Majeure Event.

SENSITIVE REQUESTS

When making a request which has potential security ramifications, it is important for both parties to be clear on the action to be taken. Please ensure that in every correspondence with our helpdesk you are specific about the item you are referring to, and we in turn will endeavour to seek clarification on requests which may be open to misinterpretation. An example of this, may be requesting security permissions to a mailbox rather than to a specific folder, we encourage all requests of this nature to be discussed verbally and followed up via email. Please bear with us if you feel we are being excessive with emails seeking to quote and clarify requests, it is in everyone's best interest.

NETWORK BREACHES

In the event of a user believing they may have been misled by any party via email or phone, it is imperative we are contacted immediately, and asked to perform a full malware scan on the presumed affected hardware/software. We ask that the end user be very specific and honest about the interaction they may have had and the links or attachments they have opened.

CYBER THREATS

Although we take every precaution to protect our users from malicious cyber-attacks, it is still the case that over 90% of all network compromises start with email. It is the responsibility of end users to be vigilant when using email, and to not open attachments or links without being 100% certain of their validity. Regardless of the technology, Rydal Communications Ltd cannot accept any responsibility for end user errors or lapses in judgement which may compromise a network, this extends to but is not limited to any incidental impact including financial loss.

PROJECT WORK

Please be aware that this charter defines our obligation to you in relation to any work to be carried out on your IT. The details outlined do not extend to project work, which are defined as "anything to be implemented in the network that did not exist previously" or "anything that requires significant alteration following its previous completion". Examples may include, the installation of a new PC or printer, or the relocation of software from one server to another, which may take significant time and planning to complete. Any downtime or interference caused by a 3rd party or their product that requires our involvement to correct (PCI Compliance / 3rd Party testing etc) will be charged at the development rate.

NETWORK ACCESS

It is of paramount importance that in-house testing (by you) and general checks be undertaken to ascertain whether your staff are being granted the correct access rights. This includes user offboarding processes and making sure access to sensitive information is regularly reviewed.

One provider, no stress, save money.

rydal™ Infotech

Making IT work seamlessly

Rydal Group, Elwes House, 19 Church Walk, Peterborough, PE1 2TP

RydalGroup.co.uk