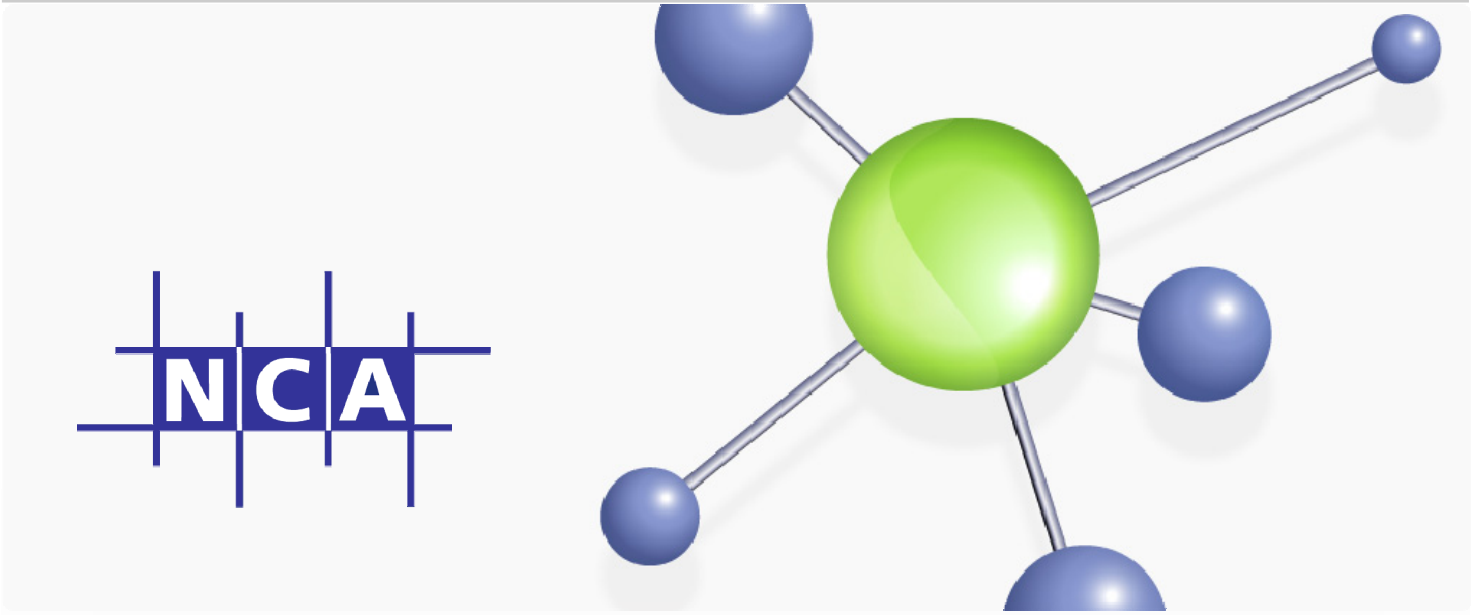
# Network Computing Architects Inc. (NCA)
# Network Operations Center (NOC) Services



**Network Computing Architects Inc. (NCA), Network Operations Center (NOC) Services** provides outsourced IT services by monitoring and managing clients' computing assets.

## Included Services:

For all systems covered under NOC Support, the following services are included:

**24 x 7 Monitoring and Remediation of covered systems:**
NOC staff will monitor covered client systems 24 hours a day, 7 days a week by utilizing the RMM (remote monitoring and management) platform.

**1 Hour Ticket Response Time:**
NOC staff will acknowledge / respond to new tickets within one hour. While all tickets are targeted to be resolved within 48 hours, the NOC makes no guarantee on resolution time.

**Automatic testing and deployment of Microsoft critical and security patches:**
Critical and Security updates for Microsoft products (Operating Systems (Windows XP and later), Office (2003 and later), Exchange Server (2003 and later), SQL Server (2005 and later), and ISA Server (2006 and later)). Critical and Security updates for Microsoft operating System features and add-ons are also included in automatic patching, including but not limited to .Net Framework (all versions), Windows SharePoint Services (2.0 and later), and Internet Explorer (6.0 and later). See Appendix C for more detail.

**Scheduled installation of Microsoft Service Packs:**
Service Packs for Microsoft products are not deployed automatically; rather they are scheduled for installation with each customer. See above for covered Microsoft products.

**Continual maintenance of monitoring templates:**
Monitoring templates are constantly evolving. As new monitoring and alerting conditions are identified for various products and environments, NOC staff will insure those additions are successfully applied across all customer client sites.

**Continual best practices recommendations for enhancing client infrastructure.**



330 120th Avenue NE Suite 210, Bellevue, WA 98005 Tel 800.604.6536

WWW.NCANET.COM

## Excluded Services:

The following services are excluded from normal NOC support:

**Work necessary to bring client site up to minimum baseline specs/health:**
Client networks must meet minimum specifications and health before being covered by NOC support. For more information on these minimums, refer to the Baseline Checklist in Appendix A.

**Installation/Upgrades/Uninstallation of client applications:**
The installation, upgrade or uninstallation of client applications falls outside the scope of NOC support services. Software deployment can be scheduled with the NOC at current service rates.

**Direct interaction with client and/or end-users via phone or email:**
The NOC staff does not engage end users or clients directly. If the NOC staff encounters a situation where the end user or client needs to be contacted, NOC staff will coordinate with the customer Point of Contact (POC). For customer sites that are covered by both NOC and Help Desk services, Help Desk staff will contact end users directly if necessary.

**Support of 3rd Party Applications:**
Due to the vast number of 3rd party applications (both desktop and server), NOC staff cannot support all 3rd party applications. NOC staff will ensure the network and underlying infrastructure is healthy and in proper working order for 3rd party applications, but the applications themselves will not be supported.

**Additions, migrations, re-architecture, or any other project related work beyond normal maintenance and administration of existing systems:**
Augmenting or adding new solutions to an existing network is excluded. For example, deploying Exchange server to an environment not currently running Exchange or upgrading from one version to the next is only supported under separate project and scope. These services can be delivered by and scheduled with NCA at current service rates.

## NOC Standard Ticket Handling Procedures:

The NOC Support Team's ticket handling procedures are driven by three key goals:

1. All service tickets are responded to within one hour.
2. Service tickets are only transferred to the customer POC if:
    a. The issue requires a technician be on-site to resolve
    b. The issue requires direct interaction with the end-user
    c. The issue requires 3rd Party Support
3. Full visibility/audit trail of ticket activities within NCA's service portal application whenever possible.

As part of the NOC setup process, NCA will assist the customer with configuring and training customer POC on use and administration of the NCA customer portal located at **https://connect.ncanet.com/support.** The portal is used for the customer POC or designated customer staff to enter requests for service. As part of our monitoring process, tickets are also automatically created in NCA's ticketing application. In both cases, the NOC team is immediately notified when a new ticket is created. The portal application allows the customer to easily see all open tickets being worked on by NOC staff.

## Ticket Lifetime Overview:

Below is a high-level outline of the NOC's ticket handling procedure:

1. New ticket is created in NOC monitored queue(s) and the application sends notification to NOC staff.
2. Within 1 hour of ticket creation, NOC staff member reviews and triages ticket to identify severity and priority of ticket.
3. If the NOC staff member is unable to start working ticket at time of triage, staff member will add a note to the ticket indicating the ticket has been "Accepted" and will provide an estimate on when work can begin. If ticket is for a client with Help Desk support as well, end-user will receive notification of ticket note.
4. NOC staff member begins working ticket, and adds note to ticket indicating work is starting.
5. When NOC staff member stops working ticket, they will complete a time entry on the ticket with summary notes of what work was performed, including troubleshooting, resolution, and testing.
6. If the ticket is not complete, NOC staff will repeat steps 4 and 5 as necessary until the ticket has been resolved. The NOC staff makes extensive use of ticket notes to provide detailed visibility of work performed, pending operations, and questions for customer staff. Whenever an individual has a question regarding the status of a ticket, or what work has been performed, the user should always consult the ticket notes first before contacting the NOC for clarification.



NETWORK COMPUTING ARCHITECTS, INC

330 120th Avenue NE Suite 210, Bellevue, WA 98005 Tel 800.604.6536

WWW.NCANET.COM

NCA adheres to the following procedure for ticket notes:

## CARRN

Cause: List the cause related to the ticket/alert
Action: List all actions you have taken. Make sure all steps are clear and concise, so others who are reading can understand your approach
Resolution: Provide detail on the outcome and/or status of the actions taken
Recommendations: List any recommendations as internal notes
Notes: List any additional Notes in the internal notes section

Each of these areas should appear in all tickets. While we may not have recommendations and notes for every ticket, we ensure that they are in the ticket and just say "None" (Example: Recommendations: None Notes: None).

**Ticket Statuses:**
Besides ticket notes, the NOC staff also utilizes ticket status to indicate the current status of a ticket. Users can quickly ascertain a basic progress on any ticket simply by making note of its status. Below is a list of the statuses employed by the NOC staff and their meaning:

- New - Ticket is newly created and has not yet been reviewed or triaged by NOC staff.
- Accepted - Ticket has been reviewed and triaged, but work has not yet started.
- In Progress - A technician is currently working on the ticket at this time.
- Complete - Ticket is complete/closed.
- Transferred to Tier II - NOC has transferred ticket to NCA Tier II resource.
- Transferred to NOC - Customer has transferred ticket to NOC for NOC staff to address.
- Waiting Customer - Ticket is waiting on response from client POC and/or end-user.
- Waiting Vendor - Ticket is waiting on response from 3rd party vendor.
- Waiting Tier II - Ticket is waiting on a response from Tier II resource.
- Waiting NOC - Ticket is waiting on response from NOC staff.
- % Complete: Multiple statuses (25%, 50%, 75%). Ticket is still open but idle. NOC will return to ticket. Often see these statuses when NOC staff needs to check back on a ticket – e.g. to verify running backup completes successfully, etc. The NOC only changes ticket status using two vehicles – ticket notes or time entries.
- Time entries will only ever change the ticket status to one of the following statuses:
- % Complete (25%, 50%, or 75%)
- Complete
- Waiting Customer
- Waiting Vendor

**Ticket notes will be used to change ticket status to one of the following statuses:**

- Accepted
- In Progress
- Transferred to NOC
- Transferred to Tier II
- Waiting NOC
- Waiting Tier II



NETWORK COMPUTING ARCHITECTS, INC

330 120th Avenue NE Suite 210, Bellevue, WA 98005 Tel 800.604.6536

WWW.NCANET.COM

## Detailed Ticket Handling:

**New ticket generation:**
The NOC staff will receive notification from the RMM application whenever a ticket is created that requires NOC attention. Workflow rules are set to notify NOC staff under the following conditions:
1. A new ticket is created in the NOC support queue.
2. A ticket is transferred to the NOC from the customer. This allows the NOC staff to receive notifications only for tickets that require the attention of the NOC staff.

**Triaging a New Ticket:**
After receiving notification of a new ticket, NOC staff will triage and respond to the ticket within one hour. NOC staff will review the ticket to determine the severity and priority of the issue and setting the ticket status to "Accepted".

**Starting Work on a Ticket:**
When a NOC technician starts to work on a ticket, they will change the ticket status to "In Progress."

**Entering Time on a Ticket:**
When a NOC technician stops working on a ticket, they will enter time worked on the ticket. The time entry will change the ticket status to an appropriate status (see Ticket Statuses above). Time entries will include a summary of work performed following the CARRN method. Time entries will always include NOC technician initials for reference in the internal notes section.

**Asking a question of customer staff:**
On occasion, NOC staff will have a question or require direction from the customer's staff. In these situations, NOC staff asks their question via a ticket note. This ticket note will change the ticket status to "Waiting Customer." Customer staff will be sent e-mail notification when the note is added. Note description will include NOC technician's initials for reference.

**Transferring ticket to customer:**
On occasion, the NOC staff will need to transfer a ticket to the customer for the customer's staff to complete. This normally only happens when on-site assistance is required, or direct interaction with the client / end-user is required when the client has not signed up for Help Desk support. In this scenario, NOC staff will add a ticket note that changes the status to "Transfer" whenever possible. Customer staff will receive e-mail notification when the note is added.

**Completing a Ticket:**
When the NOC staff completes a ticket, the ticket will be closed via a time entry. The time entry will set the ticket status to "Complete" and an email notification will be sent to the customer's staff.

**Duplicate Tickets:**
On occasion, multiple alerts and tickets may be generated for a single issue. In this scenario, the NOC staff will work from the first ticket created, and close the additional tickets as duplicates. To close the duplicate tickets, NOC staff will add a note to each ticket. This ticket note will change the ticket status to "Complete." The ticket description will indicate that the ticket is a duplicate, and reference the ticket number of the ticket that is being worked (the first ticket created for the issue). The ticket note will also include the NOC technician's initials for reference in the internal notes section.



NETWORK COMPUTING ARCHITECTS, INC

330 120th Avenue NE Suite 210, Bellevue, WA 98005 Tel 800.604.6536

WWW.NCANET.COM

# Network Computing Architects Inc. (NCA)
# Network Operations Center (NOC) Services

## Standard Operations Policies:

NCA has specified several basic standard operations policies for accessing client systems:

**Server Reboots:**
In order to provide efficient service, the NOC requests a standard reboot window be defined for each client's servers. For obvious reasons, this time window should fall when the client is not open for business and maintenance jobs (such as backups) will not be running. Obviously it may not be possible to provide a guaranteed reboot window for all clients. However, providing a guaranteed reboot window where NOC staff is free to reboot server(s) when necessary greatly increases the efficiency of NOC staff and reduces the amount of time tickets remain open.

**Workstation Access:**
When a ticket requires NOC staff to connect to a workstation, the primary goal of NOC staff is to avoid interrupting end users whenever possible. NOC staff will check to see if a user is logged in to the workstation. If so, NOC staff will try to ascertain if the user is active or if the session has been left idle, and what files are open. If the issue at hand is not critical, and we are unable to determine if the user can be safely logged off remotely, we will wait until the following day to connect to the PC. NOC staff will contact the customer's staff to coordinate having the user log off before they leave for the day.

**Passwords:**
Due to the nature of the services provided by NCA, we require that a separate admin account be created on each client domain the NOC will be supporting. Additionally, we specifically request that the built-in administrator credentials for each domain are not shared with NCA or any NOC staff member. We facilitate changing the password for our account at each client site whenever a staff change occurs. Whenever possible, NCA will notify the customer of an impending staff change on the NOC support team before it actually happens.

**Third Party Application Policy:**
There are large numbers of third party applications that are available for both Windows desktops and Windows servers. Since it is impossible for NOC staff to be well versed in all products we will encounter, the following guidelines for working with 3rd party applications were established:

- NOC staff will ensure client network and underlying infrastructure are of adequate health and stability to ensure proper functionality of 3rd party apps.
- New deployments/upgrades/uninstalls of any 3rd party application are not included under normal NOC services. Depending on the application at hand, NCA can provide a flat-fee quote for completing such new deployments. For 3rd party server applications, NOC staff will perform basic administration only if the customer provides detailed written instructions of how to perform the tasks requested. This policy is designed to insure the highest level of consistent service to all of our customers. As we are engaging more and more new customers, we are finding situations where two or more customers are using the same 3rd party application, but have vastly different procedures for administering and maintaining those solutions. As a result, we must have detailed written procedures from our customers regarding working with 3rd party applications. This is the only way to insure consistent, quality service for these applications for each customer.

**Supported Applications:**
The NOC staff is well versed in the following applications. As a result, these applications are not considered 3rd party, and are exempt from the 3rd party application policy:

- Microsoft Office (2003 and newer)
- Microsoft Exchange Server (2003 and newer)
- Microsoft SQL Server (2005 and newer)

*Microsoft desktop operating systems (Windows XP Professional and newer) and Microsoft server operating systems (Windows 2003 Server and newer) are naturally supported

*When supporting Microsoft SQL Server, NOC staff will not perform SQL actions that directly touch or manipulate contents of user databases. This primarily includes tasks such as running queries and/or scripts against user databases.

## APPENDIX A: New Site Baseline Specifications

In order to provide the highest level of service possible, NCA requires sites covered by NOC services meet minimum specifications and show general health.

**Minimum Specifications:**

All systems are running Windows 2003 or newer.
Any terminal server must be dedicated to only providing TS functions. NOC will not support terminal services on domain controllers, Exchange Servers, database servers, etc. or any other configuration not supported by Microsoft.
NCA will not support sites where end-users have domain administrator privileges. Obviously customers will often have their domain administrator password, and some sites will have a technical user who can accomplish basic tasks such as password resets, or a customer may have dedicated IT staff as well. Each of these scenarios is supported by NCA as long as users are using a separate admin level account to log in to the server to perform administrative tasks. We do not support sites where end-users' primary user accounts are members of the domain admins security group.
All systems must be protected by an up-to-date anti-virus solution. Symantec end-point protection is included with NOC service.

**Baseline Health Requirements:**

All systems must be free of any virus or malware before they can be supported by the NOC.
Active Directory must be healthy within a domain environment:
All domain controllers must be free of error events in the Directory Services event log.
All domain controllers must be free of error events in the File Replication Service event log.
All domain controllers must be free of error events in the DNS event log.
Primary systems and services must be in working order to be covered by NOC services. If a system is not functioning (e.g. Exchange) – NCA can evaluate the situation and potentially resolve the issue as a separate billable project. As long as key systems are functioning properly when NOC coverage begins, those systems will be covered under standard NOC support (subject to 3rd party application policy). NOC staff reviews each site and server configuration before activating NOC services. Due to the large number of possible configurations, NCA reserves the right to modify the minimum specifications and baseline health requirements outlined above at any time.

## APPENDIX B: Recommended Configurations

Appendix A outlines the minimum specifications and baseline health requirements for systems to be covered by NOC services. The following configurations are not required for NOC coverage, but are recommended to enable the NOC the ability to provide you with the highest service level possible.

**Hardware:**
All servers are running on server-class hardware including:
Redundant drive sub-system.
RAID controller with on-board battery to insure data writes complete successfully during power losses.
Battery backup units on all servers with associated software for clean shut-downs during power losses.
Key servers (domain controllers, Exchange servers, etc.) include a remote access card (DellDRAC, HP ILO or similar)
All new workstations deployed include Intel V-Pro technology.
Battery backup units with associated software connected to desktop machines whenever possible.
We strongly recommend that customers require all hardware to be covered by a manufacturer's warranty. (Optionally, NCA and client have agreed on a plan in writing to replace out-of-warranty machines.)

**User Environment:**
Standardize usernames and email aliases for individual client sites.
In domain environments, implement folder redirection to redirect My Documents, Desktop, &Application Data folders to a central server.
Implement an email archiving solution – either hosted (such as Reflexion's RADAR service) instead of having Outlook archive to pst files.
Remove local admin rights from all users on all client machines.
Standardize drive mappings so that drives mapped to the same share always use the same drive letter.

**Network:**
Standardize IP schemes across all sites. (e.g. .21-.30 is always for network devices, .31-.40 is always for peripherals, .41-.50 is always for network printers, etc.)
Use DHCP reservations instead of static IPs for network attached devices (switches, scanners, printers, etc.)
Whenever possible, utilize a small number of shared network printers instead of locally attached individual printers.
When using a network scanner and using scan-to-folder (SMB) functionality, create a separate domain user account solely for the scanner to authenticate with your file server. This new user account can be a standard user and only needs write access to the scan destination folders. We recommend not using existing domain administrator level accounts.
For customers with multiple locations connected via persistent router-based VPN connections, we recommend an additional domain controller be installed at each remote location with 5 or more users.

**Backup:**
Abandon tape-based technologies. Of the sites supported by the NOC, only about 10% are using tape based backups, and those 10% of sites generate more backup failures and backup related tickets than the other 90% of sites not using tape-based technologies.
Implement imaging of all machines on the network. In the event of a hardware failure, this allows you to have any machine back up and running with minimal downtime, assuming you have a user onsite that can follow instructions to assist with initiating the image restore.
Keep it simple – proportionally speaking, we see a much higher number of backup issues at sites using 3rd party file-level backup products like BackupExec. If the native NTBackup or SBS backupwill adequately back up the environment, use it. Otherwise, NCA offers managed backup solutions built specifically to allow us high levels of manageability and reliability.

**Automation:**
Whenever possible, use volume licensed software. Besides providing additional options for creating automated and standardized installations, depending on the application it provides down-grade rights so that you can keep your environment standardized.
Consolidate login scripts. More often than not, login items can be consolidated into a single script that utilizes tools such as IFMEMBER to perform different actions for different users.
Utilize a combination of group policy startup scripts, software installation policies & login scripts to automate as many software installation and system configuration tasks as possible.



NETWORK COMPUTING ARCHITECTS, INC

330 120th Avenue NE Suite 210, Bellevue, WA 98005 Tel 800.604.6536

WWW.NCANET.COM

**Documentation:**
As much as possible, provide detailed step-by-step checklists for common tasks:
New user additions
User termination
Adding new PC
Software installation checklist for 3rd party applications
ISP information for each physical location
Account information
Router make/model/serial number
Contact phone numbers/email addresses
IP block/gateway/subnet
LAN information
Firewall information
Device make/model/serial number
License keys (if applicable) LAN & WAN
IP info
Inbound & outbound access rules
Credentials
DNS & Web host information
3rd party software information
License info
Support information (including contacts)

## APPENDIX C: Patch Management Protocol

As part of the standard NOC Support services, the NOC support team provides patching of covered client systems. The protocol outlined in this document applies to all customers.

**Included Patches and Updates:**
By default, the NOC support team tests, approves, and installs only Critical and Security updates for specified Microsoft products. They will patch the following Microsoft products:

- **Microsoft Windows® Desktop Operating Systems**
  - ◊ Windows 7
  - ◊ Windows Vista
  - ◊ Windows XP
- **Microsoft Windows® Server Operating Systems:**
  - ◊ Windows Server 2008
  - ◊ Windows Server 2003 (including Small Business Server)
- **Microsoft Office:**
  - ◊ Microsoft Office 2010
  - ◊ Microsoft Office 2007
  - ◊ Microsoft Office 2003
- **Microsoft Server Applications:**
  - ◊ Microsoft Exchange Server (2007, 2003)
  - ◊ Microsoft ISA Server (2006)
  - ◊ Microsoft SQL Server (2005)
- **Components & Add-ons for Microsoft Operating Systems including (but not limited to):**
  - ◊ .Net Framework (all versions)
  - ◊ XML Core Services (all versions) Internet Explorer (6 and newer)
  - ◊ Windows SharePoint Services (2.0 and newer)

Service Packs for Microsoft Operating Systems, Office, and Server Applications are not deployed automatically. Service Packs for Operating System components (such as .Net framework) are deployed automatically according to the normal patch schedule. Testing provides basic testing of all Critical and Security updates before approving these updates for installation on client networks. Critical and Security updates are installed on our test servers after patch Tuesday. After critical and security updates have been installed in our test environment and run without issue for several days, critical and security updates are then installed on NCA's internal production network. If no issues are found on our internal production network, critical and security updates are installed on our production NOC systems (web and database servers). If the NOC identifies a critical or security update that we are not approving for installation, will provide detailed information to our customers about the uppate(s) not being approved and the issue encountered during testing.

**Installation Schedule:**
While NCA provides production testing of Critical and Security patches before approving for installation, it is impossible to test for every possible condition that may cause an issue. As a result, there is a possibility that a patch which performed flawlessly in testing may cause an issue with a specific client environment. Therefore, the NOC support team spreads patch installations over a one week (seven day) period. The patch installation schedule insures that each customer's client base is spread across all seven days – so in a worst case scenario, a patch will only cause an issue with a maximum of 1/7th of the customer's client sites maintained by the NOC. Microsoft releases Critical and Security updates on the second Tuesday of every month. These patches are tested for several days, and the NOC makes a preliminary recommendation of whether the current patches can safely be installed to production networks. Testing times can vary from month to month, but NCA targets making a formal recommendation by Thursday of the week following patch Tuesday. Patches will be approved for installation on client systems 48hrs after NCA makes a formal recommendation of patches to install. All patch installations will occur via the RMM platform. Individual client sites will automatically install updates on their designated night over the course of the next seven days. By default, NOC staff schedules patch installation to occur at 5am local time for all systems. If your environment requires patch installation to occur at an alternate time, please contact NCA to arrange the modification in the patch schedule.

**Service Packs:**
NCA does not include Service Packs as part of the routine patching schedule (except for Service Packs for components and add-ons to Microsoft Operating Systems as noted above). The NOC support team will install service packs for included Microsoft products listed above, but only on a scheduled basis. Customers are expected to request service packs be installed on a client system by creating an associated service desk ticket. NOC staff will not install service packs without a ticket requesting installation. Requests must be made at least 48 hours ahead of due date/time. NCA provides basic testing of Microsoft service packs. However, due to the wide variety of systems and environments across our entire customer base, we are unable to adequately test service packs for all possible situations. As a result, we strongly recommend customers perform their own testing of Microsoft Service Packs, and whenever possible install service packs to one or two machines initially to identify any issues.

## Appendix D: Response and Resolution Times

| Issue | Priority | Response time (in hours) | Type of Response | Resolution time (in hours) | Escalation threshold (in hours) |
|---|---|---|---|---|---|
| Network/Servers not available (all users and functions affected.) | 1 | Within 1 hour | NOC call to customer, ticket note and email notification | ASAP – Commercially Reasonable Effort | 1 hour |
| Significant degradation of network functionality (50% of users or any critical business functions affected.) | 2 | Within 1 hour | NOC call to Customer, ticket note and email notification | ASAP – Commercially Reasonable Effort | 1 hour |
| Limited degradation of network functionality (less than 25% of users or functions affected, business process can continue.) | 3 | Within 1 hour | Ticket note and email notification by NOC | ASAP – Commercially Reasonable Effort | 4 hours |
| Network/server degradation (business process can continue, one user affected.) | 4 | Within 1 hour | Ticket note and email notification by NOC | ASAP – Commercially Reasonable Effort | 8 hours |

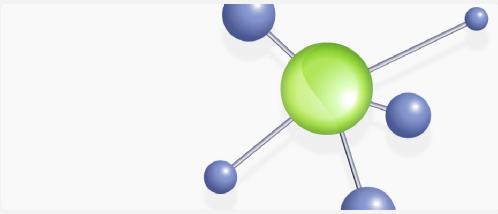
**Escalation Procedure**

1. Ticket is Created in ticketing system
2. Issue is Identified and documented in Ticket system via ticket notes
3. Issue is qualified to determine if it can be resolved through Tier 1 Support

| If issue can be resolved through Tier 1 Support: | If issue cannot be resolved through Tier 1 Support: |
|---|---|
| 4. Tier 1 NOC resolution - issue is worked to successful resolution. | 4. Issue is escalated to Tier 2 NOC support. |
| 5. Trouble Ticket is closed, after complete problem resolution details have been updated in Ticket system by NOC. | 5. Issue is qualified to determine if it can be resolved by Tier 2 NOC Support. |
| 6. Email notification is sent to customer contact with issue resolution details contained in notes by NOC. | |

| If issue can be resolved through Tier 2 Support: | If issue cannot be resolved through Tier 2 Support: |
|---|---|
| 4. Tier 2 Resolution - issue is worked to successful resolution by NOC. | 4. Issue is escalated to Tier 3 NOC Support. |
| 5. Trouble Ticket is closed, after complete problem resolution details have been updated in Ticket system by NOC. | 5. Issue is qualified to determine if it can be resolved through Tier 3 NOC Support. |
| 6. Email notification is sent to customer contact with issue resolution details contained in notes by NOC. | |

| **If issue can be resolved through Tier 3 Support:** | ***If issue cannot be resolved through Tier 3 Support:*** |
|---|---|
| 4. Tier 3 Resolution - issue is worked to successful resolution by NOC. | 4. Issue is escalated to vendor support or replacement is pursued. |
| 5. Trouble Ticket is closed, after complete problem resolution details have been updated in NOC Ticket system. | |
| 6. Email notification is sent to customer contact with issue resolution details contained in notes by NOC. | |



NCA is an ISO 27001 certified professional security services consultancy. That means we deliver world-class security solutions that both enable and protect your business.



NETWORK COMPUTING ARCHITECTS, INC

330 120th Avenue NE Suite 210, Bellevue, WA 98005 Tel 800.604.6536

WWW.NCANET.COM