

Cistel IT Services

Scheduled On-site Support Service Desk On-call On-site Support

Our technical support staff is here to help you when you need it most: We'll be there before IT problems occur in order to prevent them, but we'll also help you after problems have manifested themselves in order to fix them ASAP.

Our support services are geared to End Users (First Level of Support) and IT Staff alike (Second Level of Support). Every incident that we work on is managed via our web-accessible ticket management system.

Scheduled On-site Support is our proactive IT support service designed to reduce the amount of downtime associated with failures in your IT infrastructure. The objective of Scheduled On-site Support is to prevent IT issues wherever and whenever possible BEFORE they occur. On-site Support is scheduled at a mutually convenient time, as chosen by the Client and by the Cistel Service Delivery Manager.

On-call Service Desk is your new IT Help Desk. Cistel maintains a staff of IT professionals that you can access 24 hours per day, 7 days per week, with a 1-hour response time during business hours. The objective of the On-call Service Desk is to help your staff solve their IT issues as quickly as possible and get back to productivity in as short a time as possible. We can be reached by telephone at **613.723.1723** or via email at servicedesk@cistel.com. Our technicians will help your staff remotely, or if required, a team member will be dispatched to correct the problem on-site (at Cistel's discretion).

On-call On-site Support is for those occasions when you decide that you need to have a technician come to your site to do the work. This could include physical maintenance of equipment, network issues, installations, etc. With one phone call to the Service Desk, our technicians will be dispatched at the agreed-to time and work until the problem is solved.

These service offerings include:

- Desktop service requests
- Common application requests
- Emergency response
- Further administrative attention based on items discovered during proactive package operations
- Managing third party contracts

IT Management

Supporting your IT is more than just fixing problems and assembling the right components.

At Cistel, we believe in building networks for the long-term. Therefore, we have an IT Management offering where our team of senior technicians and in-house managers work with you to build the right plan for your organization.

This offering Includes:

- Strategic management of the technical requirements incorporating capacity management, problem management, and availability management
- Development of client-centric processes for IT management based on industry standards and best practices (ITIL)
- Assumed IT governance over internal infrastructure and service delivery
- Representation at regular IT meetings

- Direct reporting to Executive level
- Input into the development of a business continuity plan with respect to the IT infrastructure
- IT reviews
- Reporting
- Initial Review & Documentation
- Align with Business Objectives
- Plan and Budget
- Implement
- Manage, Review and Document

Proactive Operational Management

Our Proactive Infrastructure Maintenance services are provided either on-site or remotely, as determined by Service Delivery Manager.

Services include:

- Patch Management
- Core Server Management
- System Health Monitoring
- Managed anti-virus
- Backup & Recovery Management
- Scheduled Maintenance
- Incident management

Patch Management

The Patch Management service offering entails the monitoring and application of patches pertaining to the operating system and any included components thereof. For example, Internet Explorer would be considered an included component of the Windows Operating Systems. This service does not include applications running over and above the operating system itself (Microsoft Office, SQL, Exchange etc.). This service may be applied either to Microsoft Windows and/or Linux based operating systems.

Cistel tracks vendor released security hot fixes, patches and related system updates. When an update becomes available Cistel’s standardized response procedure includes an evaluation of the update whereby we assess the level of urgency for implementation, perform internal testing, plan and perform the deployment of the patch. Cistel categorizes level(s) of urgency based on the potential and impact for system compromise. The following table outlines these levels and their associated response measures:

Severity Level	Measure
Critical	Patches will be deployed to customer site(s) within 48 hours.
Important	Patches will be deployed to customer site(s) within 7 (seven) days.
Moderate	Patches will be deployed to customer site(s) within 14 (fourteen) days.
Low	Patches will be deployed to customer site(s) within one month.

Table 1: Patch Implementation

In the interest of proactive system management and protection Cistel also monitors industry sources for vulnerability advisories and will perform necessary defensive measures where applicable, regardless of whether or not the vendor has released an update at that time.

In the event a deployed patch is detected as not being properly installed on a target system Cistel will spend up to 15 minutes working to resolve the issue. Resolution efforts above and beyond this 15 minute window will be deducted from the On Call Service Desk (OSD) block of time in 15 minute increments.

Core Server Management

Core Server Management is the Cistel service offering designed to cover the configuration and maintenance of the elemental system services ensuring the smooth operation of your IT infrastructure.

Cistel technicians will perform consistent assessment(s) of these services within your organization, tuning and adjusting them as required.

These include any of the following items:

- Configuring operating system for security/performance
- Job scheduling/monitoring
- DHCP, WINS and DNS administration and monitoring
- Domain and group policies implementation and management
- User and group account management

Server Health Monitoring

The Cistel Remote Monitoring service offers to our clients a manner through which to have professional technical personnel more readily aware of and able to respond to system/service outages within your technical environment.

Through an automated monitoring process via the Internet Cistel technicians will be promptly alerted in the event one of your servers or an application hosted on that system should fail.

Once a failure alert is received a Cistel technician will follow a standardized approach to addressing and resolving the issue, sometimes before the client even realizes there has been an issue!

The methodology followed for a system outage is as follows:

- Create a communication relay to the client either directly or through other Cistel personnel
- Work to resolve the issue as quickly as possible
- Follow up with the client as to the cause and resolution of the outage

This package allows for the monitoring of servers and/or applications and services hosted from these servers. Cistel technicians will work with you to arrange a monitoring solution best suited to your environment, and our standardized approach follows the same escalation structure as our support level agreement.

This service offering encompasses the management and initial discovery of items requiring further technical intervention only. The time needed to implement the resolution for these issues will be billed to the client as per the service agreement.

Cistel technicians not only resolve the current issue, but work to ensure any future similar situation is avoided wherever possible.

Managed Anti-virus

The Cistel Managed Anti Virus service offering is a multi functional package leveraging industry proven tactics to help prevent the intrusion and impact of unsolicited programs. Our solution provides clients with a solid approach to managing virus threats.

As part of the setup process Cistel's professional technicians will work with the client to design a personalized architecture and the supporting policies to ensure a custom fit malware prevention and security solution. Our technical staff is able to make use of your existing technology and/or provide recommendations for the most suitable solution to fit your needs.

Further augmenting this solution Cistel also provides the following key services as part of this package:

- **Implementation:** Once you have decided on the approach you wish to take Cistel will distribute the solution into your environment as seamlessly and non-intrusively as possible.
- **Management:** Your anti virus solution is administered remotely from the Cistel Service Center via the Internet. The management console and/or other reporting tools are used daily to monitor the activity occurring within your organization. Our professional staff is prepared to react to any emergencies involving virus intrusion, and have experience dealing with industry leaders in virus awareness while managing an “outbreak”.
- **Definition Updates:** Virus prevention software is only as strong as the algorithms and definitions it has to identify potential issues. Cistel will ensure your anti virus solution is kept up to date with the latest virus definitions providing a more solid operating environment.
- **Moves/Changes:** As your business grows and changes, so should your protection. Cistel will offer to you solutions and advice on the impacts of changes you request always bearing in mind the need to provide a sense of security and protection of your data and operating environment.

Backup and Recovery Management

Every organization has the need to preserve part of the electronic framework they operate within.

Cistel’s Backup and Recovery Management offering is designed to provide a reliable solution whereby you can be sure your systems configuration and data is properly archived and readily serviceable should it ever be needed.

As part of the setup process/fees Cistel technicians will analyze your environment, software and archival methodology.

Using this information we will assist you in the design and implementation of a dependable solution geared to the needs of your organization.

Once this has been implemented a technician will perform a check following every backup interval to confirm the successful completion of backup jobs being performed.

Should the need for modifications to the engineered solution arise, whether through growth or change within the client’s environment, Cistel will ensure the design continues to provide the utmost in dependency available.

The backup is only as useful as the ability to restore the data.

As part of this service offering Cistel will perform a monthly rotational trial restore to verify the recoverability of the data being stored on your backup media.

As part of the trial restore process Cistel will also perform a cleaning operation on the backup hardware should the necessary apparatus be available (cleaning tape, CD cleaner etc.).

In the event an error is detected in the backup log/report requiring further investigation Cistel will spend up to 15 minutes working to resolve the issue. Resolution efforts above and beyond this 15 minute window will be deducted from the On Call Service Desk (OSD) block of time in 15 minute increments.

Incident Management

Every incident or service request our technicians work on, is tracked.

You and/or your staff can check on the status of any incident they've reported to Service Desk through our web based Client Management Portal. This gives you direct visibility into our Incident Management System in real time allowing you to review current service requests, and previously resolved service requests. For your convenience, you will also have the ability to create your own tickets via the portal through a simple form based page. A technician will be immediately alerted to the creation of this ticket and we begin the process to respond to and resolve your request as quickly as possible.

IT Projects

In this fast-paced world of IT, the only constant is change. Implementing these changes with a minimum of disruption to your IT infrastructure and with the lowest cost to your organization is everyone's aspiration. Cistel can help you make that a reality.

As a Microsoft Certified Partner, Cistel has experience in designing and implementing Networking Infrastructure Solutions, Advanced Infrastructure Solutions, Security Solutions, and Integrated E-Business Solutions. Our IT Project service includes:

- Project and special engineering delivery management
- Design and testing
- Implementation
- Management, review and documentation

Networking Infrastructure Solutions: Includes implementing technology solutions based on Microsoft Windows 2000 Server and Windows Server 2003 operating system technology, with a particular focus on Microsoft Small Business Server 2000 or Windows Small Business Server 2003.

Advanced Infrastructure Solutions: We can craft high-availability infrastructure solutions that include one or more of the following:

- Design and deployment of the Windows Active Directory service
- Microsoft Identity Integration Server implementation
- Microsoft Exchange Server migration or deployment
- Data management migration and server consolidation
- Storage solutions design and deployment
- Systems management design and deployment
- Hosting services

Security Solutions: Cistel builds the most advanced Microsoft security solutions to protect the customer's information assets. This includes:

- Security management and operations
- Secure wireless VPN and perimeter
- Identity and access management

Integrated E-Business Solutions: Cistel deploys internet-based business solutions and infrastructure, including:

- Internet Business
- Extranets and Web hosting
- Web application and portal development
- Web-based workflow and orchestration solutions

Delivery Agreement and Escalation Procedure

Cistel provides the following as part of their on-going contract.

- **Monthly time usage reports** of On-site and Remote interventions, as part of the monthly invoice;
- Access to an **Incident Tracking system** to manage and track all outstanding issues and support requests;
- A **process for submitting service requests** with specified response times and Cistel internal escalation procedures.

There are 3 different levels of service issues as identified by the Cistel support staff upon analyzing the impact of the issue. The following defines the issue types and response times based on the issue priority.

A “response” is defined as a Cistel representative contacting the user by phone. A response does NOT mean that the problem has been corrected, but only that contact has been established with the end-user and that the problem has been logged in our Incident Tracking system.

Definitions

- **Urgent:** Service/system down emergencies: a response within 1 hour. A service/system down emergency is defined as total service disruption or inability of the user to perform their duties.
- **Attention:** Service impacting: a response during the next site visit. Any emergencies where some service is still available but performance is degraded or partial service is unavailable.
- **Normal:** Non-service impacting or regular change requests: a response will be provided as priorities dictate. General support questions dealing with issues where no service disruption is occurring.

Response times

- **Urgent:** When an URGENT service request is received Cistel will respond to the request within 1 business hour. This does not mean the problem will be solved within the 1 business hour, but it will be addressed and a relevant update will be provided within that timeframe.
- **Attention:** When a service request marked ATTENTION is received, Cistel will respond to the request during the next site visit. This does not mean the problem will be solved during the next site visit, but it will be addressed and a relevant update will be provided within that timeframe.
- **Normal:** When a non-critical, service or user impacting service request is received Cistel will respond to the request as priorities dictate. This means the request will be queued and addressed based on existing priorities or new impacting issues.

Notification procedures

When submitting IT service support requests, the following are the notification procedures for each of the three priority level issues:

- **Urgent:** Log an URGENT issue by calling the Cistel Service Desk at **613.723.1727**.
- **Attention:** Log an ATTENTION issue either by calling the Cistel Service Desk at **613.723.1727** or by emailing **servicedesk@cistel.com**.
- **Normal:** Log a NORMAL issue either by calling the Cistel Service Desk at **613.723.1727** or by emailing **servicedesk@cistel.com**.

Call escalation within the Service Desk

All issues logged with Service Desk will follow the escalation procedure below during the resolution process:

Responding to calls

- Within 1 business hour, if an issue is not responded to, then it is escalated to the Service Delivery Manager
- Within 2 business hours with no response, it will be escalated to the Manager, IT Solutions Group.

Problem resolution

- Within 2 business hours, if no progress has been made on an issue, it is escalated to a senior technician
- Within 4 business hours, if no progress has been made on an issue, it is escalated to the Manager, IT Solutions Group

Cistel Contacts

Cistel Technology Inc. 210 Colonnade Road, Suite 200 Ottawa (Ontario) K2E 7L5 www.cistel.com		Telephone: 613.723.0023 Toll-free: 866-9-CISTEL Facsimile: 613.274.2804
Service Desk 613.723.1723 servicedesk@cistel.com	Incident Management Client login at portal.cistel.com	