CISPOINT
MSSP Focused on Rightsizing Your IT

OUR COMPREHENSIVE SERVICE OFFERINGS

User Support

1. Onboarding new employees.
2. Offboarding exiting employees.
3. Password resets.
4. Troubleshooting user login issues.
5. Resolving email configuration issues.
6. Assisting with software installations.
7. Setting up multi-factor authentication (MFA).
8. Providing remote desktop assistance.
9. Creating and managing user accounts.
10. Addressing printer and scanner issues.
11. Troubleshooting internet connectivity issues.
12. Resolving VoIP phone issues.
13. Assisting with video conferencing tools.
14. Managing mobile device setups.
15. Setting up and managing VPN access.
16. Handling application crashes.
17. Managing email distribution lists.
18. Educating users on cybersecurity best practices.
19. Resolving browser performance issues.
20. Managing shared file permissions.

Server Management

21. Monitoring server performance.
22. Patching and updating server operating systems.
23. Managing Active Directory.
24. Setting up and managing virtual machines.
25. Configuring and managing server backups.
26. Addressing disk space issues on servers.
27. Resolving server crash incidents.
28. Updating server hardware drivers.
29. Migrating servers to new platforms.
30. Troubleshooting group policy issues.

Network Management

31. Monitoring network performance.
32. Configuring firewalls.
33. Setting up and managing VLANs.
34. Troubleshooting network latency issues.
35. Managing wireless access points.
36. Updating firmware on network devices.
37. Managing DNS and DHCP services.
38. Configuring network security policies.
39. Installing and managing network switches.
40. Conducting network performance assessments.

Cybersecurity

51. Installing and managing antivirus software.
52. Conducting phishing simulations.
53. Setting up intrusion detection systems.
54. Implementing endpoint protection.
55. Monitoring security alerts.
56. Conducting vulnerability scans.
57. Managing encryption for sensitive data.
58. Responding to potential data breaches.
59. Managing user roles and access controls.
60. Educating clients on cybersecurity best practices.

Backup & Recovery

41. Configuring backup solutions.
42. Testing backup restoration processes.
43. Monitoring backup jobs.
44. Resolving backup job failures.
45. Managing offsite backup storage.
46. Implementing disaster recovery solutions.
47. Performing data recovery in emergencies.
48. Updating backup retention policies.
49. Documenting recovery procedures.
50. Assisting with cloud backup solutions.

Cloud Services

61. Managing Microsoft 365 tenants.
62. Setting up cloud storage solutions.
63. Migrating workloads to the cloud.
64. Managing Azure or AWS environments.
65. Configuring cloud application permissions.
66. Monitoring cloud service performance.
67. Resolving cloud service outages.
68. Configuring SaaS applications.
69. Managing SharePoint permissions.
70. Implementing cloud cost management solutions.

Device Management

71. Managing desktop and laptop provisioning.
72. Configuring device security policies.
73. Monitoring device health and performance.
74. Deploying software updates.
75. Troubleshooting hardware issues.
76. Managing device warranties and replacements.
78. Resolving issues with peripheral devices.
79. Setting up new workstations.
80. Conducting device lifecycle planning.

Software Management

81. Installing software updates and patches.
82. Configuring licenses for applications.
83. Troubleshooting software compatibility issues.
84. Managing software renewal reminders.
85. Conducting software audits.
86. Managing third-party integrations.
87. Providing application training.
88. Testing new software before deployment.
89. Setting up custom application configurations.
90. Managing ERP/CRM software.

Proactive Monitoring

91. Monitoring uptime for critical systems.
92. Setting up automated alerts for anomalies.
93. Conducting quarterly system health checks.
94. Implementing predictive analytics tools.
95. Proactively resolving disk space issues.
96. Identifying network bottlenecks.
97. Addressing recurring issues through root cause analysis.
98. Monitoring end-user device performance.
99. Setting up monitoring dashboards.
100. Scheduling regular system maintenance.

Policy & Compliance

101. Auditing IT compliance with standards (e.g., CMMC, HIPAA, PCI-DSS).
102. Implementing data retention policies.
103. Documenting IT policies for clients.
104. Setting up secure file-sharing policies.
105. Assisting with IT compliance reporting.
106. Ensuring regular patch management.
107. Conducting regular security assessments.
108. Managing privileged account access.
109. Assisting with audits and certifications.
110. Establishing acceptable use policies.

Strategic Planning

111. Developing IT roadmaps for clients.
112. Conducting quarterly business reviews (QBRs).
113. Recommending hardware and software upgrades.
114. Planning cloud migrations.
115. Aligning IT with business goals.
116. Preparing budgets for IT expenditures.
117. Providing strategic consulting.
118. Implementing scalable IT solutions.
119. Planning for end-of-life (EOL) systems.
120. Designing business continuity plans.

Incident Management

121. Logging and tracking incidents.
122. Responding to critical outages.
123. Coordinating with third-party vendors.
124. Providing 24/7 emergency support.
125. Root cause analysis after incidents.
126. Documenting incident resolution procedures.
127. Escalating complex issues to senior engineers.
128. Addressing DDoS attacks.
129. Prioritizing tasks based on SLAs.
130. Maintaining a knowledge base of solutions.

Hardware Management

131. Installing and configuring servers.
132. Managing UPS systems.
133. Conducting hardware diagnostics.
134. Setting up storage arrays.
135. Installing cabling for new networks.
136. Coordinating hardware repairs.
137. Recycling or disposing of old hardware.
138. Conducting hardware inventory audits.
139. Troubleshooting RAID configurations.
140. Managing IoT device setups.

Client Communication & Documentation

141. Preparing monthly performance reports.
142. Providing updates on ongoing projects.
143. Educating clients about emerging technologies.
144. Maintaining detailed documentation for systems.
145. Sharing updates on system outages or maintenance.
146. Setting up client portals for support tickets.
147. Offering training sessions for client staff.
148. Maintaining contracts and SLAs.
149. Providing regular IT health summaries.
150. Soliciting feedback to improve services.