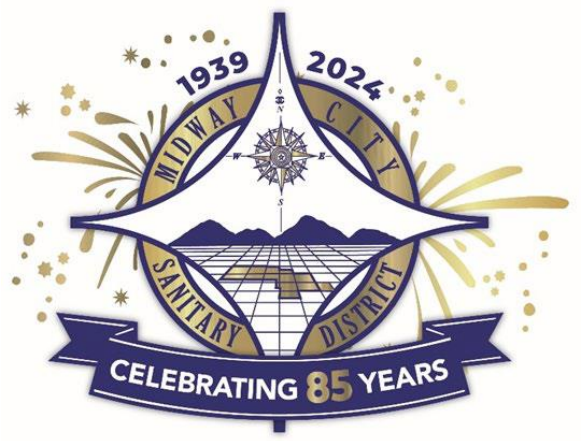
Response For:



Midway City Sanitary District

Request for Proposal for

IT Services

October 1, 2024

1301 Gervais Street,
Suite 1800, Columbia, SC 2920
(O) 803-733-7333
(TF) 800-787-1600
(F) 803-733-5888
VC3.com

Table of Contents

LETTER OF TRANSMITTAL

October 1, 2024
Shantae' Hansen
VC3, Inc.
1301 Gervais St., Suite 1800
Columbia, SC 29201

Response to: Request for Proposal For IT Services

Attention:
Robert Housley, General Manager
Midway City Sanitary District
14451 Cedarwood St.
Westminster, CA 92683

Dear Midway City Sanitary District:

VC3, Inc. respectfully submits the enclosed response for the Request for Proposal for Information Technology Managed Service Provider (MSP) and Cybersecurity Services. We certify that VC3 is authorized to operate contractually and sell within the State of California (Federal Tax ID: 57-0993240).

This response fully addresses the requirements of the District outlined in *Request for Proposal for Information Technology Managed Service Provider (MSP) and Cybersecurity Services*. This proposal and cost schedule shall be valid and binding for Ninety (90) days following the Request for Proposal due date and will become part of the contract that is negotiated with the District.

With over 29 years of IT experience and over 1,100 municipal government clients in 21 states, VC3 offers a longstanding history of combining stable day-to-day operations with forward-thinking IT leadership to establish a high-technology orientation for cities as they grow and evolve.

Our key contact for this proposal is:

Shantae' Hansen, Senior Account Executive
(909) 900-5694
Shantae.hansen@vc3.com

VC3 appreciates the opportunity to submit these qualifications.

Sincerely,

Ryan Vestby, CEO
(800) 787-1160
Ryan.Vestby@vc3.com

COMPANY PROFILE

Business Overview, Market Focus & Methodology

Since 1994 VC3 has intentionally focused on providing managed IT services to municipal government. Accordingly, VC3 has created service offerings to align with local government-specific needs including security & audit requirements, diverse technology needs across many municipal departments, IT budgeting, and financial models designed to contain costs and adapt to shifting priorities across fiscal years and administrations.

General Business Information

- Full legal company name: VC3, Inc.
- Total Full-Time Employees: 618
- Total Number of Clients: 1,800+
- Total Number of Municipal Clients: 1,100 +
- Location of office to service the account: Rancho Cucamonga, CA with staff in other metro regions across the state.
- Incorporated in 1994
- State of Incorporation: Delaware
- Federal Tax ID: 57-0993240
- Dun & Bradstreet Number: 926120601
- NAICS Code: 541512 - Computer Systems Design Services

VC3 Employee Background Checks

All VC3 employment offer letters are contingent upon completion of credit, criminal, and Department of Motor Vehicle (DMV) background checks.

Additional Office Locations

- 21820 Burbank Blvd Suite 220, Woodland Hills, CA 91367
- 10325 Younger Rd, Midland, TX 79706
- 333 Fayetteville Street, Suite 516, Raleigh, NC 27601
- 315 W Ponce De Leon Avenue, Suite 150, Decatur, GA, 30030
- 8000 Centerview Pkwy., Ste. 120 Memphis, TN 38018
- 5815 Clark Rd, Bath Twp, MI 48808
- 5614 Grand Ave, Duluth, MN 55807
- Suite 101, 15511 – 123 Avenue NW, Edmonton, Alberta T5V 0C3
- Suite 355, 3115 – 12 Street NE, Calgary, Alberta T2E 7J2

Financial and Audit Information

- **Financial Information**: Audited financials are available upon request.
- **SOC 2 Compliance:** VC3 maintains a SOC 2 certification, asserting that standards & controls are followed to keep client data secure, available, and confidential. SOC 2 is a

voluntary compliance standard and requires regular audits. SOC 2 compliance information is available upon request.

Municipal League/Association Endorsements and Partnerships

VC3 is proud to be endorsed by nine state leagues of municipalities who have chosen to partner with and/or endorse VC3:

- California Special District Association
- Tennessee Municipal League
- Maryland Municipal League
- North Carolina League of Municipalities
- Municipal Association of South Carolina
- Georgia Municipal Association
- Iowa League of Cities
- Connecticut Conference of Municipalities
- Kentucky League of Cities

REFERENCES

References were selected based on characteristics shared by Midway City Sanitary District, and its expressed goals. VC3 provides comprehensive IT support & management, cybersecurity, vendor management, network design, and strategic planning district-wide for all departments across these Districts.

Santa Ana Watershed Protection Agency

- **Contact:** John Leete, Director of IT: jleete@sawpa.gov, (951) 354-4228
- Client since 2008.

Upper San Gabriel Valley Municipal Water District

- **Contact:** Evelyn Rodriguez, CFO: evelyn@usgvmwd.org, (626) 443-2297
- Client since 2013.

Corning Healthcare District

- **Contact:** Tina Hale, District Manager: tehale@corninghealthcaredistrict.com, (530) 824-5451
- Client since 2023

STAFF RESOURCES

Midway City Sanitary District will be managed on a day-to-day basis by our local team supporting California clients but will have access to the entire VC3 engineering staff when needed.

Tentative Assigned Team Members (to be confirmed upon award):

- Erica Frye – Onboarding Project Manager
  - Main Point of Contact during onboarding process
- Vera Takakura – Strategic Advisor (SA)
  - Role explained below
- Chris Aalberg – Client Relationship Manager (CRM)
  - The Client Relationship Manager focuses on assisting our clients to navigate their service needs, ensuring proper escalations as required, and managing their technology needs and service expectations
- Johnny Olesh – Service Manager
  - Manager of Charlie Team
- Charlie Team
  - Team of Engineers that are assigned to support Midway City Sanitary District

Support Staff Categories and Domain Expertise

- Chief Technology Officer – 1
- Chief Information Security Officer – 1
- Strategic Advisors – 40+
- Service Delivery Managers – 10+
- Help Desk Engineers – 40+
- System Engineers – 100+
- Senior System Engineers – 10+
- Network Engineers – 5
- Architect & Escalation Engineers (domain experts) – 10+
- Client Relationship Managers – 25+
- Project Managers & Engineers – 25+
- Application Development Engineers – 20+

Total Engineering Resources – 300+

Certifications

- **CJIS:** As a condition of employment at VC3, all technical employees are required to maintain CJIS certification at federal and state levels:
- **FBI & NCIC Requirements**: VC3 has approximately 300+ engineers, Account Managers, Project Managers, and Virtual Chief Information Officers that:

  - Have completed the Criminal Justice Information System's (CJIS) Security and Awareness Training
  - Are certified as completing the Level 4 CJIS Security Training.
  - Are approved to access networks that connect to the Federal Bureau of Investigation's (FBI) National Crime Information Center (NCIC) Systems, therefore meeting the requirements needed for local law enforcement audits.

The following selected highlighted certifications below are held among VC3 engineers, managers, and support staff — including senior-level, long-term employees:

- Certified Information Security Systems Professional (CISSP)
- Certified Government Chief Information Officer (CGCIO)
- VMware:
  - VMware Certified Professional
  - Data Center Virtualization
  - VMware Sales Professional
  - Multiple years and versions of each across staff
- Microsoft:
  - Microsoft Certified Solutions Associate (MCSA)
  - Microsoft Certified Professional (MCP)
  - Microsoft Certified Systems Engineer (MCSE)
  - Microsoft Certified Technology Specialist (MCTS)
  - Microsoft Certified IT Professional (MCITP)
  - Microsoft Server (various years)
- Cisco:
  - Cisco Certified Entry Network Technician (CCENT)
  - Cisco Certified Network Associate (CCNA):
    - CCNA Routing & Switching
    - CCNA Security
  - Cisco Certified Network Professional (CCNP)
  - Cisco Certified Network Professional – Security (CCNP-S)
- Certified Wireless Network Administration (CWNA)
- Project Management Professional (PMP)
- Lean Six Sigma Yellow Belt
- Certified Business Continuity Professional
- Information Technology Information Library (ITIL) Certification
- CompTIA Security+

Solution Methodology for Midway City Sanitary District

- Your local VC3 team will be led by a highly skilled Strategic Advisor (SA) who understands your goals, advocates for your organization, and provides IT guidance. Additionally, an Account Manager, Service Manager, and engineers will provide you with a comprehensive IT service.
- A Strategic Advisor (SA) will be assigned to Midway City Sanitary District. The SA will work with the District to develop an annual technology budget for recurring expense items and new capital requirements in alignment with organizational goals. The SA will recommend technology and cyber security solutions as well as provide roadmaps that support key business processes to help the District leverage technology appropriately. The SA will work with the District as part of the annual planning process to understand the current business drivers and goals and make recommendations targeted toward maximizing the effectiveness of the customer's technology investment. The SA will also work with the District to create an IT Steering Committee to identify and facilitate all IT initiatives going forward.
- The SA will work with the VC3 team of engineering staff to review Midway City Sanitary District's existing IT infrastructure. The SA will also work with the Midway City Sanitary District management team to determine long and short-term goals for the District. These factors are taken into consideration when creating all IT proposals and plans for the client. As the normal part of IT strategy and management, all plans will be designed to preserve existing resources and expenditures when possible.
- With VC3's vast experience working with on-premises and cloud-based IT Managed Services, the importance of a robust, scalable, secure, and redundant IT environment is deeply embedded in our core philosophy and strategy. VC3 provides 7x24x365 management, monitoring and alerting, software patching and updates, and remote and onsite remediation for all server & infrastructure-related issues as necessary. VC3 ensures preventive maintenance for equipment is promptly performed and develops and tests backup and disaster recovery plans and procedural documentation. VC3 sets up new users and edits or removes existing users when requested to manage the computer network and associated hardware, software, communications, and operating system necessary for the quality, security, performance, availability, recoverability, and reliability of the system.
- As part of the proposed VC3 solution, VC3 will work with existing Midway City Sanitary District vendors to perform maintenance and updates. VC3 will deploy the VC3 Remote Support and antivirus agents to all applicable included devices. VC3 will monitor and maintain backups for included devices. VC3 will manage the inventory and configuration of all network devices to ensure that they provide the expected security for the District.
- VC3 will provide IT support for customer-licensed third-party applications. VC3 will recommend that support contracts be maintained as is appropriate with third-party vendors, and VC3 will manage these relationships for the District. For incidents requiring

support from third-party vendors, VC3 will act as the District's representative to facilitate the support from diverse vendors in a manner consistent with the District's best interests.

- VC3 will work with Midway City Sanitary District during the onboarding process to assess their current environment and make recommendations. These recommendations will focus on projects that will create a more stable, secure, and efficient IT environment for the District. These onboarding findings will also help build the District's IT Roadmap, which the SA will continue to focus on throughout the partnership with VC3.

VC3 PRESENTATION OF SERVICE

VC3's Managed-On Premises IT Solution with Protect Shield:

- Deploy VC3 RMM and network monitoring agent to all endpoints.
- Deploy base EDR agent and monitor with a 24x7x365 Security Operations Centre (SOC) to all endpoints (including workstations).
- Document the entire IT infrastructure and maintain documentation.
- Provide strategic recommendations to improve the overall IT environment in line with business objectives and IT best practices (SA- Strategic Advisor)
- Monitor and Manage all server and network endpoints 24x7x365.
- Respond to and resolve alerts generated through the monitoring of server and network endpoints.
- Patch Windows operating systems and approved third-party applications.
- Hardware, Software, Domain and License Procurement Help and Renewals
- Vendor Management to help with 3rd party applications.
- Virtual Chief Information Security Officer (VCISO Services) – optional
- Best Practices guided by the Information Technology Infrastructure Library (ITIL)
- Cybersecurity Solutions including web content filtering, advanced endpoint detections and response, dark web detection, email protection, cloud security event management, and end-user security awareness training.
- Microsoft Office 365 License Management.

VC3 Manage – On-Premises

A. Discovery & Deployment

1. Set up the Client System for management and provide training to help the Client get the most out of the services. This includes:
    i. Deployment of the Company monitoring and management platform.

ii. Deployment of the Company Endpoint Protection software.
iii. Full documentation and inventory of your network
iv. Best-practice configuration of the network for monitoring and management
v. Orientation and training for your staff
vi. MacOS Note: If the Client is utilizing Mac OS, the Company will provide documentation to end users on how to install the Company's monitoring and management platform. MacOS does not allow a remote deployment of standard Company tools.
    1. Should Mac OS users require onsite assistance to install VC3's monitoring and management platform, support will be provided on a Time and Materials basis at the rates detailed within the Client's Master Agreement.

2. Implement performance monitoring of the client's network prior to and during implementation.

B. 24x7 Monitoring and Incident Response Services

1. Provide 24X7 Incident response services for all included users, servers, and network devices.
2. Provide phone, remote, and onsite support to authorized users for all included devices.
3. Track all incidents through an ITIL (Information Technology Infrastructure Library) based Service Desk system. All requests will be prioritized and processed per the 'Priority' guidelines listed in Addendum A.
4. Provide 24x7 collection of performance data for the client's included server and network devices per the Company's best practices.
5. Utilize industry best practices for remote access, control, and management of all devices.
6. Patching: Deploy, manage, and monitor the installation of approved service packs, security updates, and firmware updates as deemed necessary on all

applicable devices. Some devices such as tablets and cell phones may not be compatible with included patching methodologies.

7. Resolution of monitoring alerts.
8. Resolution of performance issues.
9. Resolution of availability issues.
10. Resolution of end-user-reported problems.
11. Routine additions, deletions, and changes to included devices and users.

C. Application Support

1. Provide support for client licensed 3rd party applications. If it is determined from the initial discovery and/or from third-party application vendors that an application requires additional servers, licensing or support resources, additional monthly costs may be required before the application can be supported.
2. Microsoft Applications
    i. Includes Microsoft Office and Office 365 core applications. This is limited to Microsoft Access, Excel, OneDrive for Business, OneNote, Outlook, PowerPoint, SharePoint, Teams, and Word.
    ii. Application installs, synchronization issues, permission management, and general troubleshooting are all within the scope for these applications.

D. **Strategic IT Planning**

Provide the client with a named Strategic resource to assist the Client with the following:

1. **Budgeting**: Work with the client to develop an annual technology budget for recurring expense items and new capital requirements in alignment with organizational goals.
2. **Strategic Planning**: Recommend technology solutions as well as provide roadmaps that support key business processes in order to help the client leverage technology appropriately. The Company will work with the client as part of the annual planning process to understand the current business drivers

and goals and make recommendations targeted toward maximizing the effectiveness of the client's technology investment.

3. **Analyze IT Health data**: Perform a periodic analysis of the data collected by the Company's monitoring systems to proactively resolve issues and assess potential risks within the environment. The Company will make this analysis available to key stakeholders and provide direction on business decisions regarding the level of investment.

E. Endpoint Detection and Response

1. Deployment of Company Endpoint Detection and Response (EDR) agents to all applicable included devices.
2. Monitoring of EDR agents by 24x7x365 Partner Security Operations Center (SOC).
3. Provide 24x7 Incident response services for all security events and incidents generated by the EDR tool for applicable devices. All events and incidents will be prioritized and processed per the 'Priority' guidelines listed in Addendum A.

F. IT Asset Administration

1. Hardware and software asset and warranty expiration tracking
2. Domain name expiration tracking
3. Hardware and software purchase specification
4. Web portal access for ticket creation and management
5. Maintaining network documentation and secure password storage
6. Interfacing with vendors such as internet service providers (ISPs)

G. Procurement

1. Server, Networking, and Power equipment.
2. Desktops, laptops, tablets.
3. Peripherals, including Printers.
4. Software, including subscription-based services.
5. Domain names and security certificates.

H. Cloud Data Recovery:

1. Deployment & Implementation Services

i. Configure backups for all accounts licensed with appropriate Microsoft 365 and/or G Suite licenses.
ii. Backup the following items within the Client Microsoft 365 environment:
    1. SharePoint
    2. Teams
    3. OneDrive
    4. Exchange Online
iii. Backup the following items within the client's G Suite environment:
    1. Google Drive
    2. Google Calendar
    3. Gmail
    4. Google Shared Drives
iv. Configure infinite backup data retention.
v. Configure backups to occur 3 times a day.

2. General Managed Backup Services
    i. Monitor and maintain backups for the applicable devices and accounts protected.
    ii. Perform periodic updates to the backup software such as patches, and updates.
    iii. Perform data recovery actions at the request of Client in line with priorities outlined in Addendum A.

I. **Cyber Security – Cloud Protect**

1. Deployment & Migration Services

i. Provision **Cloud Protect** – Cloud Platform Security Event and Incident Reporting platform.
    1. Authentication with Client Microsoft 365 and/or G Suite tenant.
    2. Alerting threshold tuned to meet industry best practices.

2. General Managed Security Services

i. **Cloud Protect**. Includes cloud security event and incident monitoring and reporting for productivity suites for Microsoft 365, &/or G Suite cloud platforms.

ii. **Security Monitoring Center**. Includes:

1. 24x7 third party security monitoring of the solution.
2. Monitoring of any account with an active sign on to the Microsoft 365 and/or G Suite environment.
3. Security Information and Event Management of the Cloud Productivity suite.
4. Critical system log capture and retention.
5. 24x7 third party monitoring of Microsoft 365 and/or G Suite security logs.
6. Escalation to Company of any detected security incidents requiring remediation.

1. General Managed Security Services

i. ***24x7 Monitoring and Incident Response Services***:

1. Provide 24X7 Incident response services for all included deployed services.
2. Track all incidents through an ITIL (Information Technology Infrastructure Library) based Service Desk system. All requests will be prioritized and processed per the 'Priority' guidelines listed in Addendum A.
3. Provide 24x7 Partner Security Operations Centre (SOC) monitoring for all endpoints with Endpoint Protect deployed.
4. 24X7 response to critical event-driven Incidents.
5. Utilize industry best practices for remote access, control, and management of all devices.

2. ***Quarterly Security Summary***. Includes a report of the activities that have taken place under this Order.

B. **Cyber Security – Cloud Protect**

1. Deployment & Migration Services

i. Provision **Cloud Protect** – Cloud Platform Security Event and Incident Reporting platform. Includes deployment of the cloud monitoring services to the Clients' Microsoft 365, or G Suite tenant.

2. **General Managed Security Services**
    i. **Cloud Protect**. Includes cloud security event and incident monitoring and reporting for productivity suites for Microsoft 365, &/or G Suite cloud platforms.
    ii. **Security Monitoring Center**. Includes:
        1. 24x7 third-party security monitoring of the solution.
        2. Security Information and Event Management of the Cloud Productivity suite.
        3. Critical system log capture and retention.
        4. 24x7 third-party monitoring of Microsoft 365 security logs.
        5. Escalation to the Company of any detected security incidents requiring remediation.

A. VC3 Protect – Server Data Recovery Backups

1. Could not quote based on limited information. If awarded VC3 will provide an updated path to achieve Data recovery backups.

B. 24x7 Monitoring and Incident Response Services

1. Provide 24X7 Incident response services for all included backup devices.
2. Provide phone, remote, and onsite support to authorized users for all included devices.
3. Track all incidents through an ITIL (Information Technology Infrastructure Library) based Service Desk system. All requests will be prioritized and processed per the 'Priority' guidelines listed in Addendum A.
4. Provide 24x7 collection of performance data for the client's included server and network devices per the Company's best practices.
5. Utilize industry best practices for remote access, control, and management of all devices.
6. Patching: Deploy, manage, and monitor the installation of approved service packs, security updates, and firmware updates as deemed necessary on all

applicable devices. Some devices such as tablets and cell phones may not be compatible with included patching methodologies.

7. Resolution of monitoring alerts.
8. Resolution of performance issues.
9. Resolution of availability issues.
10. Resolution of end-user-reported problems.
11. Routine additions, deletions, and changes to included devices and users.

VC3 Protect – Shield (Cyber Security)

A. VC3 Protect - Shield

1. Deployment & Implementation Services

i. Provision **Dark Web Protect** -Dark web monitoring platform, including provisioning Client's domain(s), reviewing existing data with Client point of contact, and configuring real-time alerting:
   1. Configure monitoring service to monitor corporate domains in scope.
   2. Configure up to five (5) personal email addresses to be monitored.
   3. In scope domain and email addresses are listed in Addendum C.

ii. Provision **Cyber Aware** – Cyber Security Training platform. Includes synchronizing employees between the Client's domain and training platform. The company will configure initial and ongoing testing and training at a frequency determined by Client.
   1. Whitelisting emails from the Cyber Aware server to maximize delivery rates.
   2. Maintaining an active user list within the platform.
   3. Creating phishing campaigns targeting users on the Client domain.
   4. Management of phishing campaigns monthly.
   5. Creating training campaigns and educating users on the Client domain.
   6. Management of training campaigns monthly.
   7. Providing phishing/training reports to Client.

iii. Configure **Endpoint Protect** – Advanced threat hunting for endpoints.
   1. Deploy Endpoint Protect agent to all devices with Company RMM deployed.
   2. Configure initial policy settings for application whitelisting.
   3. Deploy monitoring of agents from the 24x7x365 Security Operations Centre (SOC)

iv. Deploy **Web Protect** – Advanced DNS/Web protection platform. Filters content accessible by employees when connected to the corporate network or using corporate devices:
    1. Deployment of agent to all devices with Company RMM deployed.
    2. Initial configuration of web and content filtering policy within the solution.
v. Provision **Email Protect** – Advanced Email Threat Protection platform.
    1. Deploy Email protection to Client Microsoft 365 environment.
    2. Updating MX Records.
    3. Customizing Spam settings.
    4. Creating filter policies and approve/block sensor list items.
vi. Provision **Cloud Protect** – Cloud Platform Security Event and Incident Reporting platform.
    1. Authentication with Client Microsoft 365 tenant.

Alerting threshold tuned to meet industry best practices.

HELPDESK SUPPORT AND ON-SITE SUPPORT

All documented District computer users will have direct and unlimited access to VC3's helpdesk, and VC3 will provide a centrally managed ticketing system. Service will be provided by VC3's California Service Delivery Team. The Service Delivery Team is trained to follow regimented processes that ensure optimal response times, high levels of client satisfaction, and prompt escalation to an advanced engineer (within 15 minutes) if a support request is beyond the initial receiving engineer's level of skill or expertise.

Every end-user support interaction is documented, and District staff will receive regular status updates and ongoing communication regarding support issues.

As a condition of employment, all VC3 technical staff are required to pass criminal background checks and maintain Level 4 CJIS certification to comply with federal CJIS and NCIC requirements.

During onboarding, the dedicated Project Manager will ensure that District IT users are trained on the four methods available to obtain support from VC3's helpdesk: phone, email, chat, and via the VC3 logo icon in the System Tray on District workstations (installed during implementation).

Users will be instructed that High priority issues must be placed via phone to ensure the timeliest response. Summarily, troubleshooting activities will begin immediately.

District technology users will be encouraged to make VC3 the first call for all IT-related issues. VC3's helpdesk will provide:

- Application and Operating System helpdesk services

- Guidance and user support pertaining to proper use of District applications and systems.
- Guidance and user support pertaining to proper response to security concerns such as websites, emails, and application behavior.

VC3 will maintain a knowledge base of support resolutions and instruction on best practices for quickly resolving District support needs to be tailored to the District's environment on VC3's documentation management system. An export of District-specific content can be provided at the District's request.

All support requests will flow through VC3, and VC3 will assign tickets to the appropriate resource (VC3 or District staff) based on need. VC3's helpdesk is staffed by direct employees of VC3 on all three shifts daily to provide 24x7x365 support for District staff. All requests for assistance will be logged and tracked in a central ticketing system and VC3 will operate from that same system managed by VC3.

Support requests will first be addressed remotely. If unable to be resolved remotely, VC3 will dispatch resources on-site or with direct assistance from the District's local IT resource.

Proactive alerts from all monitoring systems will be reviewed and triaged by the helpdesk to help prevent potential outages before they become an issue.

VC3 will work with all third-party IT vendors on behalf of the District.

VC3 will provide record-keeping and administration for maintenance and support contracts for server and network-related software. This will include timely notification of pending contracts and/or license renewals.

The District's SA will provide monthly service desk reports on problems, issues, affected users, and problem categories.

SERVER MANAGEMENT

Using the same Remote Monitoring and Management (RMM) tool mentioned above, VC3 will provide 24x7x365 support for the District's servers (remote and onsite). VC3 will manage, monitor, and track the performance of the District's server infrastructure. Management will be administered by a longstanding team of network engineers with certifications in Microsoft Server and VMware (see list of highlighted certifications on page 5).

VC3 will utilize its RMM tool to provide the following:

- Inventory Control & Reporting
- Warranty Management
- Asset Tracking
- Patching and compliance for Operating Systems and Installed Applications
- Antivirus & Antimalware management and remediation

- Endpoint Detection and Response
- Security Policy Management
- Remote Monitoring of hardware and software for errors, warnings, or non-compliance
- Daily backup verification provided.
- Management of Offsite Backup storage and Disaster Recovery of District's data and applications
- Management of District's Virtual Servers
- Monitoring of SNMP-enabled devices such as UPS's and Server Hardware.
- Monitoring and Maintenance of the District's Server Backups.

VC3 will manage endpoint encryption for offsite servers. VC3 will also assume management of third-party vendors and interface with them to provide support for their hardware and services.

VC3 will also maintain ongoing reports of server health performance via the District's SA. The SA will keep the District up to date with reporting on server health and coordinate with internal staff to guide needed projects and upgrades.

Support SLA's and Ticket Priorities

Call Priority	Initial Client Contact Guidelines	Initial Client Contact Percentages
1	1 Hour	90%
2	2 Hours	90%
3	4 business hours	90%
4	8 business hours	90%
5	N/A	N/A

A. **Priority 1:**
   - System/device/application down causing work to cease and critical impact to the entire organization, a whole department, or a C-level executive or VIP user; no interim solution available; Client is in danger of or is experiencing a financial loss or the ability to make strategic business decisions is impaired.
   - **24x7 Support:** Priority 1 incidents will be addressed on a 24 hours a day, 7 days a week basis including holidays.

B. **Priority 2:**
   - System/device/application down causing work to cease and potential business impact for up to 5 users, a C-level executive, or a VIP user; no interim solution available.
   - **24x7 Support:** Priority 2 incidents will be addressed on a 24 hours a day, 7 days a week basis including holidays.

C. **Priority 3:**
   - Level of service degraded causing impact to an individual user; no interim solution available. Operational impact to the organization or a whole department though work continues as a result of implementing an interim solution or use of other system/device/service.
   - **Business Hours Support:** Priority 3 incidents will be addressed during normal business hours Monday-Friday, 8:00am to 5:00pm excluding holidays.

D. **Priority 4:**
   - Minor inconvenience to a department or user exists though work continues as a result of implementing an interim solution or use of another system/device/service.
   - **Business Hours Support:** Priority 4 incidents will be addressed during normal business hours Monday-Friday, 8:00am to 5:00pm excluding holidays.

E. **Priority 5:**
   - Maintenance tasks, audits, or alignment work that is not requested by the client.
   - **Business Hours Support:** Priority 5 incidents will be addressed during normal business hours Monday-Friday, 8:00am to 5:00pm excluding holidays.

NETWORK MAINTENANCE AND MANAGEMENT

The District's SA and a VC3 networking specialist engineer will evaluate the District's use of its network and wireless technologies, create thorough documentation, and provide recommendations to enhance network resiliency and reliability when necessary.

VC3 will monitor, maintain, and manage the District's network across all its locations 24x7x365. Along with its RMM tool, VC3 will utilize Professional Services Automation and monitoring software PRTG to monitor and track the performance of the District's infrastructure.

A 30-minute response time SLA for all network outages, 24x7x365, will be provided by VC3.

VC3 will maintain expertise in network maintenance and management that includes senior-level, long-term employees with advanced skill sets and specialties including Cisco CCENT, Cisco CCNA, and CWNA certifications (see list of highlighted certifications on page 6).

VC3 will use PRTG in conjunction with customized power shell scripts and software to capture both the up/down status of all District network components and to capture data points around the utilization of these resources. With this data, VC3 can forecast and predict future performance issues.

VC3 will be able to monitor hundreds of services running on the District's infrastructure and will automatically trigger failed services to restart and minimize user downtime without the need for the user to create a ticket.

When services are restarted, VC3 captures these events in the ticketing system to identify trends & patterns and resolve root causes of failure. This minimizes the likelihood and impact of future failures and downtime.

PRTG can be configured to check the status of network assets as often as every 60 seconds. For any critical services, this in turn will automatically alert VC3's service desk so immediate action can be taken to remediate the failed service.

As part of on-boarding, VC3 will deploy and configure the above tools.

VC3 will provide regular reviews of the network for security updates to firmware and configuration.

Additionally, VC3 will provide the following for network maintenance and management via its RMM tool:

- Inventory Control & Reporting
- Warranty Management
- Asset Tracking
- Patching and compliance for Operating Systems, appliance upgrades, and all network equipment including firewalls, switching, routing, and wireless infrastructure.
- Security Policy Management

VC3 will utilize the SA (Strategic Advisors) and Service Delivery Team to ensure Change Management is being handled to the standards of ITIL (IT Infrastructure Library).SA's and the Service Delivery Team are trained in the ITIL Change Management Methodology which is the IT Standard for Business Change Management.

The SA and a dedicated account manager will drive and coordinate regular management update meetings to deliver reports on monthly and yearly accomplishments, needs, and trends. These

meetings will occur at an interval agreed upon by District staff and VC3 based on the needs of the District.

VENDOR MANAGEMENT

VC3 will manage relationships with third-party vendors who provide services and/or software to the District. To ensure reliable operation of District applications, VC3 will maintain subject matter expertise on managing systems for optimal use of District applications (requirements for hosting, configurations, etc.). VC3 will coordinate with vendors and District staff on appropriate timing to apply updates to the District's software.

If services stop working or troubleshooting is necessary, VC3 will initiate contact with vendors and provide support to resume services. VC3 will also assist in the management of vendor contracts and new purchases.

VC3 will maintain a knowledge base of vendors, applications, services, and instructions for best practices to quickly resolve District support needs. An export of district-specific content can be provided at the District's request.

NETWORK ARCHITECTURE AND DESIGN

As part of the IT roadmap created by the SA, network architecture and design will be addressed to advance the District's ability to achieve objectives and long-term goals. VC3 will review all aspects of the District's IT environment during the initial onboarding assessment, and provide recommendations driven by best practices for a municipality its size.

VC3 will work with the District's management and IT Steering Committee to establish priorities and provide appropriate budget estimates for necessary changes so that the District will maintain:

- A functional, resilient, and modern network topology
- Critical government operations in the event of natural disasters, technological, biological, or nuclear attacks – or other situations that would require extended periods of time during which District facilities are offline or disconnected from the main network.

The SA will provide guidance on strategic improvements regarding the District's use of hosting, services, data storage, security issues, and other Disaster Recovery issues discussed above.

The SA will lead the District in regular, planned evaluation and testing of DR (Disaster Recover) operations and strategies.

VC3 will stay ahead of District needs, providing ongoing guidance as technology evolves, and proactively advising improvements that the District should consider implementing. These

recommendations will be provided on a hierarchical basis, segmenting critical issues from long-range and non-urgent recommendations.

ADDITIONAL SERVICES

Additional Services

- **Managed VOIP Phone Systems:** Designed for organizations needing cost-effective, fully supported, and modernized phone systems.
- **Application Development:** VC3 can take your business process and automate it through the development of custom software that meets your specific business needs.
- **Web Design & Hosting:** We provide a modern, custom-designed website that looks good and delivers the information your residents need.
- **Power BI:** Track and evaluate your metrics against benchmarks, spot areas of strength and opportunities for improvement, combine data from multiple systems into a single dashboard, and spend more time making impactful decisions.
- **SharePoint Consulting & Records Management:** Centralize documents, retain records, and streamline workflows—with VC3 as your guide.

Pricing and comments:

PRODUCTS & SERVICES	QUANTITY	UNIT PRICE	PRICE
VC3 Manage - Full User 24x7x365 Remote & Onsite Support: Users, Servers, Network Foundational Protection Components: EDR Including 24x7x365 SOC, M365 Protection & Backups Proactive Monitoring, Maintenance & Patching: Workstations, Servers, Network Strategic IT Planning: Alignment with IT Best Practices, IT Budgeting, Technology Roadmap M365 License Management Vendor Co-Ordination Hardware, Software, Domain and License Procurement / Renewals	15	$150.00 / month	$2,193.75 / month after 2.5% discount for 3 years

PRODUCTS & SERVICES	QUANTITY	UNIT PRICE	PR
VC3 Manage - Email Only User Support for email only users includes troubleshooting send/ receive issues and access issue to email platform. M365 & Email Protection & Backups Included	13	$25.00 / month	$316.87 / month after 2.5% discount for 3 years
Protect Shield (Add On) Cyber Aware Complete - Cyber Security Training & Simulated Phishing Tests Dark Web Credential Monitoring Web Protection & Content Filtering Email Protection & Spam Filtering VC3 Security Team	15	$21.99 / month	$254.85 / month after $75.00 discount for 3 years
Protect Shield M365 Only User Cyber Aware Complete - Cyber Security Training & Simulated Phishing Tests Dark Web Credential Monitoring Email Protection & Spam Filtering M365 Monitoring & Protection VC3 Security Team	13	$10.50 / month	$104.00 / month after $32.50 discount for 3 years
Protect Shield Email Protect Archiving Upgrade Email Archiving for up to 10 years.	28	$2.00 / month	$56.00 / month for 3 years
M365 Business Standard NCE Annual Subscription	15	$12.50 / month	$187.50 / month for 1 year
Exchange Online (Plan 1) NCE Annual Subscription	13	$4.00 / month	$52.00 / month for 1 year

PRODUCTS & SERVICES	QUANTITY	UNIT PRICE	PR
CSDA Member Benefit Cyber Aware Complete - Cyber Security Awareness Training and Simulated Phishing Attacks Dark Web Protect - Dark Web Credential Monitoring Self Service Password Reset	1	$5.00 / month	$0.00 / month after 100% discount for 3 years
VC3 Managed Services Onboarding	1	$3,097.35	$3,097.35
SUMMARY			
Monthly subtotal			$3,164.97 after $176.88 discount
One-time subtotal			$3,097.35

Comments

Prices shown above are valid for 30 days from date of Order.

This work order is provided with the following acknowledgements and assumptions:

- No discovery was performed prior to work order creation. Numbers presented are an estimation based on client provided documents. If onboarding discovery presents different findings, monthly costs will be adjusted accordingly.
- Printers will be supported as best effort. Extensive printer support will be provided through a separate third-party printer support contract which VC3 will manage through vendor management.
- Client is currently performing full backups of all servers in line with industry standards.
- Client currently has active support contract with backup software vendor.
- As client backup solution is not a VC3 offered backup solution, VC3 will support current backup solution as best effort through active support contact.

This Order is entered into as of October 1, 2024 between VC3 Inc., a Delaware corporation ("Company") and Midway City Sanitary District ("Client")

Order Governed by the Master Agreement

This Order is subject to and governed by Company's Master Agreement in effect on the date this Order is entered into between Company and Client. The Master Agreement is available at https://www.vc3.com/terms-of-service/ and is incorporated in full into and made a part of this Order by this reference. The Client may also request a copy of the Master Agreement by submitting an email request to betterit@vc3.com identifying the Client and the applicable Orders. Company's entering into this Order is conditioned on Client's agreement to the Master Agreement, and by entering into this Order with Company, Client accepts and agrees to the Master Agreement.

Deliverables & Services

Discovery & Deployment
Setup the Client System for management and provide training to help the Client get the most out of the services. This includes:

1. Deployment of all services listed above.
2. Full documentation and inventory of your network
3. Best-practice configuration of the network for monitoring and management
4. Orientation and training for your staff
5. MacOS Note: If Client is utilizing Mac OS, Company will provide documentation to end users on how to install Company's monitoring and management platform. MacOS does not allow a remote deployment of standard Company tools.
   Should Mac OS users require onsite assistance to install VC3's monitoring and management platform, support will be provided on a Time and Materials basis at the rates detailed within Client Master Agreement.
6. Implement performance monitoring of client's network prior to and during implementation.

24x7 Monitoring and Incident Response Services

1. Provide 24X7 Incident response services for all included user, server, and network devices.
2. Provide phone, remote and onsite support to authorized users for all included devices.
3. Track all incidents through an ITIL (Information Technology Infrastructure Library) based Service Desk system. All requests will be prioritized and processed per the 'Priority' guidelines listed in Addendum A.

4. Provide 24x7 collection of performance data for the client's included server and network devices per Company's best practices.
5. Utilize industry best practices for remote access, control, and management of all devices.
6. Patching: Deploy, manage, and monitor the installation of approved service packs, security updates and firmware updates as deemed necessary on all applicable devices. Some devices such as tablets and cell phones may not be compatible with included patching methodologies.
7. Resolution of monitoring alerts.
8. Resolution of performance issues.
9. Resolution of availability issues.
10. Resolution of end-user reported problems.
11. Routine additions, deletions, and changes to included devices and users.

Foundational Protection

1. Deploy Endpoint Detection and Response (EDR) to all workstations and servers with Company RMM deployed.
2. Monitor workstations and servers with EDR installed via 24x7x365 partner SOC.
3. Deploy M365 Monitoring and Backup Solutions to Client M365 Tenant.
4. Continually monitor M365 tenancy.
5. Backup M365 (SharePoint, OneDrive, Teams & Exchange Online) 3 times a day.
6. Configure infinite retention on M365 backups.
7. Respond to incidents and service requests. All requests will be prioritized and processed per the 'Priority' guidelines listed in Addendum A.

Application Support

1. Provide support for client licensed 3rd party applications. If it is determined from the initial discovery and/or from third-party application vendors that an application requires additional servers, licensing or support resources, additional monthly costs may be required before the application can be supported.
2. Microsoft Applications:

a. Includes Microsoft Office and Office 365 core applications. This is limited to Microsoft Access, Excel, OneDrive for Business, OneNote, Outlook, PowerPoint, SharePoint, Teams and Word.

b. Application installs, synchronization issues, permission management and general troubleshooting are all within scope for these applications.

Strategic IT Planning

Provide the client with a named Strategic resource to assist Client with the following:

1. **Budgeting**: Work with the client to develop an annual technology budget for recurring expense items and new capital requirements in alignment with organizational goals.
2. **Strategic Planning**: Recommend technology solutions as well as provide roadmaps that support key business processes in order to help the client leverage technology appropriately. The Company will work with the client as part of the annual planning process to understand the current business drivers and goals and make recommendations targeted toward maximizing the effectiveness of the client's technology investment.
3. **Analyze IT Health data**: Perform a periodic analysis of the data collected by Company's monitoring systems to proactively resolve issues and assess potential risks within the environment. The Company will make this analysis available to key stakeholders and provide direction on business decisions regarding the level of investment.

IT Asset Administration

1. Hardware and software asset and warranty expiration tracking
2. Domain name expiration tracking
3. Hardware and software purchase specification
4. Web portal access for ticket creation and management
5. Maintaining network documentation and secure password storage
6. Interfacing with vendors such as internet service providers (ISPs)

Procurement

1. Server, Networking, and Power equipment.
2. Desktops, laptops, tablets.
3. Peripherals, including Printers.
4. Software, including subscription-based services.

5. Domain names and security certificates.

Protect Shield

1. **Deployment & Implementation Services:**
    a. Provision **Dark Web Protect** -Dark web monitoring platform, including provisioning Client's domain(s), reviewing existing data with Client point of contact, and configuring real time alerting:
        i. Configure monitoring service to monitor corporate domains in scope.
        ii. Configure up to five (5) personal email addresses to be monitored.
    b. Provision **Cyber Aware** – Cyber Security Training platform. Includes synchronizing employees between Client's domain and training platform. Company will configure initial and ongoing testing and training at a frequency determined by Client.
        i. Whitelisting emails from the Cyber Aware server to maximize delivery rates.
        ii. Maintaining active user list within the platform.
        iii. Creating phishing campaigns targeting users on Client domain.
        iv. Management of phishing campaigns monthly.
        v. Creating training campaigns, educating users on Client domain.
        vi. Management of training campaigns monthly.
        vii. Providing phishing / training reports to Client.
    c. Provision **Email Protect** – Advanced Email Threat Protection platform.
        i. Deploy Email protect to Client Microsoft 365 environment.
        ii. Updating MX Records.
        iii. Customizing Spam settings.
        iv. Creating filter policies and approve/block sensor list items.
    d. Provision **Web Protect -** Advanced DNS/Web protection platform. Filters content accessible by employees when connected to the corporate network or using corporate devices:

1. Deployment of agent to all devices with Company RMM deployed.
2. Initial configuration of web and content filtering policy within the solution.

2. **General Managed Security Services**

1. ***24x7 Monitoring and Incident Response Services***:

1. Provide 24X7 Incident response services for all included deployed services.

2. Track all incidents through an ITIL (Information Technology Infrastructure Library) based Service Desk system. All requests will be prioritized and processed per the 'Priority' guidelines listed in Addendum A.

3. Provide 24x7 Partner Security Operations Centre (SOC) monitoring for all endpoints with Endpoint Protect deployed.

4. 24X7 response to critical event driven Incidents.

5. Utilize industry best practices for remote access, control and management of all devices.

3. ***Quarterly Security Summary***. Includes a report of the activities that have taken place under this Order.

CSDA Member Benefits

1. Provision **Cyber Aware** – Cyber Security Training platform. Includes synchronizing employees between Client's domain and training platform. Company will configure initial and ongoing testing and training at a frequency determined by Client.
    1. Whitelisting emails from the Cyber Aware server to maximize delivery rates.
    2. Maintaining active user list within the platform. Creating phishing campaigns targeting users on Client domain.
    3. Management of phishing campaigns monthly. Creating training campaigns, educating users on Client domain.
    4. Management of training campaigns monthly. Providing phishing / training reports to Client.
2. Provision **Dark Web Protect** -Dark web monitoring platform, including provisioning Client's domain(s), reviewing existing data with Client point of contact, and configuring real time alerting:
    1. Configure monitoring service to monitor corporate domains in scope.
    2. Configure up to five (5) personal email addresses to be monitored
3. Provision **Self Service Password Reset Tool**
    1. Deploy Self Service Password Reset Tool to be used by Client users within Client Active Directory.

2. Provide training to Client users on how to use tool.

Exclusions

Items other than those included above are expressly excluded from the Services provided within this Order. The following exclusions and clarifications are intended to clarify the scope of services for this order:

1. Excluded services are those related to functionality upgrades, such as those required to evaluate, specify, purchase, and implement client system or server upgrades such as operating systems, Microsoft Office suite software unless included with a specific Company product, third party software deployments or upgrades, or equipment related to these services whose scope exceeds that defined above. Company will provide these services to the client on a Time & Materials Order basis at the rates outlined in the Master Agreement. If modification or replacement of a hardware device or component is required, client is responsible for all hardware and hardware vendor services costs, excluding Company owned hardware explicitly provided through this Order.
2. Software development, training and project work, including client-owned PC upgrades and non-patch upgrades of software, are not included.
3. When client requests services by Company not explicitly included in this agreement, they are agreeing to invoicing of said services per the terms outlined in the Master Agreement. For all services which incur additional hourly fees, Company will notify the client that these services are outside the scope of this work order and will receive approval from client prior to rendering these additional services.
4. Software and licensing purchased by the client directly from a third-party vendor are not included as a part of services to be supported.
5. Architectural changes, mass deployment, database management, data visualization and business process automation / troubleshooting are considered excluded from this Order.
6. Cybersecurity event or incident response activities or remediation efforts exceeding eight (8) hours of technician, engineer or project management time.
7. Should deficiencies, malware infections, or critical vulnerabilities be discovered during the deployment of services, Company will bring to Client attention and discuss the

impact of the deficiencies on Company's ability to provision the Services and provide client with options to correct the deficiencies. Initial remediation hours will be billed outside of this Order unless otherwise explicitly stated in this Order.

8. Company is authorized to obtain any documentation or information regarding any and all accounts at all locations the Client may have with any telecommunications vendor. Company also has the authority to be added as an account contact and speak on behalf of the Client in negotiating services, billing, credits and/or connectivity of this Client's services with the Telecommunications company and/or vendor with the proviso that only the Client has authority to enter into contracts with any vendor or supplier.
9. Throughout the relationship between Company and Client, the Company will also make extensive use of Remote Management software. This software is used across all clients to monitor workstations and servers in real time. Company will also use this software to remotely connect and assist the Client's users when they have a technological problem if the user has an internet connection. In addition, endpoint protection software, ticketing, and asset management are managed through this software.

Assumptions

1. The Order will not become effective unless and until it is agreed upon and signed by the Client and Company.
2. If Company is providing or managing Client 's Microsoft Licenses, then Client agrees to the Microsoft terms and conditions as stated in the Microsoft Customer Agreement found here: https://www.microsoft.com/licensing/docs/customeragreement
3. Company reserves the right, at its discretion, to pass onto the client any changes to obligations, such as terms or pricing imposed on Company by a given vendor, for an offering that is currently resold to the client at any time during the current agreement term.
4. Company will make reasonable efforts to resolve all issues remotely prior to dispatching an engineer onsite. Travel hours incurred will be invoiced according to the Master Agreement.
5. Microsoft NCE licenses and subscriptions run on an annual basis and cannot be terminated nor altered mid-term.
6. If client Microsoft licenses are under a current annual NCE subscription, Company assumes they will migrate to become under Company's management at the point of renewal.

7. The items defined in this Order are designed to enhance the security of the customer environment. There is no guarantee that any security measure will prevent a data breach, infection, or other cyber security incident.

Client Responsibilities

1. Client will provide a primary point of contact for Company to work with on all services provided in this Order.
2. Client is responsible for authorizing access for Company to sites that are owned / controlled by third parties.
3. Client is responsible for proper disposal of client-owned devices.
4. Client will make a best effort to maintain the minimum infrastructure requirements as defined by Company.
5. Client will maintain both hardware and software maintenance agreements with the source Vendor whenever possible to allow for ongoing access to security updates and to provide quick replacement of non-functioning components.
6. Client must assign Company as their Microsoft Partner of record.
7. Client is responsible for procurement and ownership of all licenses, maintenance, and vendor support agreements required for support of their third-party applications, excluding the Microsoft licensing explicitly included in the per seat packages identified in Products & Services section.
8. Third party tool licensing may be required for additional cost.
9. Client will be financially responsible for any remaining or ongoing charges from Microsoft. Microsoft subscriptions can each have their own terms and renewal dates. It is the client's responsibility to engage Company to adjust Microsoft subscription counts and terminations prior to 12 months from the original work order or subsequent change order purchase date.

Invoicing

Recurring services, if included, shall be provided for term indicated in Products & Services, starting from the date of the first recurring invoice (Effective Services Start Date), unless terminated in accordance with the terms of this Order or the Master Agreement.

Company will invoice the Client a pro-rated monthly fee based on any partial month of service plus the first full month of service on the Effective Services Start Date. All subsequent service months will be invoiced at the start of the month in which services are to be rendered. Services

activated after the first of month may be invoiced on a pro rata basis the following month. All One-Time Fees will be invoiced to Client upon signature of this Order.

Any taxes related to services purchased or licensed pursuant to this Order shall be paid by Client or Client shall present an exemption certificate acceptable to the taxing authorities. Applicable taxes and freight charges shall be billed as a separate item on the invoice.

Unit rates will automatically increase annually on the anniversary of the Effective Services Start Date equivalent to the CPI change for All Urban Consumers or by 4.00%, whichever is higher.

The terms of this Order will automatically renew for an additional term of equivalent length to the current active term unless notice of termination is provided by either party no fewer than 90 calendar days prior to expiration of the current active term.

Company will audit the Client's usage of the quantity of Services on a monthly basis; for each quantity of Services found in excess of the amount stated in this Order above, Company will increase the monthly service fee amount by the corresponding unit price stated above.

At no time during the term of this Order will the fees payable under this Order (i.e. the monthly subtotal amount) drop below seventy-five percent (75%) of the initially agreed upon monthly subtotal stated above.

In the event of the early termination of the Agreement in accordance with Section 3.3 of the Master Agreement, Client agrees that the initially agreed upon monthly subtotal stated above shall be used for calculating fees due for the remaining term of the Agreement.

Additional services may be added at any time during the life of this Order at the unit price listed above.

Addendum A – Service Desk Priorities

Incidents and Service Requests are triaged and prioritized to effectively resolve the most important issues in a timely manner. Company utilizes the following priorities, criteria and response metrics:

- **Priority 1:**
    - System/device/application down causing work to cease and critical impact to the entire organization, a whole department, or a C-level executive or VIP user; no interim solution available; Client is in danger of or is experiencing a financial loss or the ability to make strategic business decisions is impaired.
    - **24x7 Support:** Priority 1 incidents will be addressed on a 24 hours a day, 7 days a week basis including holidays.
- **Priority 2:**
    - System/device/application down causing work to cease and potential business impact for up to 5 users, a C-level executive, or a VIP user; no interim solution available.
    - **24x7 Support:** Priority 2 incidents will be addressed on a 24 hours a day, 7 days a week basis including holidays.
- **Priority 3:**
    - Level of service degraded causing impact to an individual user; no interim solution available. Operational impact to the organization or a whole department though work continues as a result of implementing an interim solution or use of other system/device/service.
    - **Business Hours Support:** Priority 3 incidents will be addressed during normal business hours Monday-Friday, 8:00am to 5:00pm excluding holidays.
- **Priority 4:**
    - Minor inconvenience to a department or user exists though work continues as a result of implementing an interim solution or use of another system/device/service.
    - **Business Hours Support:** Priority 4 incidents will be addressed during normal business hours Monday-Friday, 8:00am to 5:00pm excluding holidays.
- **Priority 5:**
    - Maintenance tasks, audits, or alignment work that is not requested by the client.
    - **Business Hours Support:** Priority 5 incidents will be addressed during normal business hours Monday-Friday, 8:00am to 5:00pm excluding holidays.

Addendum B - Maintenance Windows

All work performed within Company's Hosting or Client Infrastructure is a form of maintenance. Such work may or may not result in a disruption of service depending on the scope of the activity.

1. **Scheduled Maintenance**: All planned work performed on Company's Hosting or Client Infrastructure by Company engineers, or staff is defined as "Scheduled Maintenance". During Scheduled Maintenance, some or all of Company's Hosting or Client Infrastructure may be out of service and therefore may not be accessible to users. Regularly Scheduled Maintenance will occur between 2 AM and 6 AM in the local time zone for which the Client Infrastructure being maintained resides. Downtime to perform changes is expected during this window. If Client has a business need to avoid said downtime, they must provide their request via the Company Service Desk ten business days in advance.
    a. **Notification**: Client will be notified via email should Scheduled Maintenance be required to take place outside of the windows specified above.
2. **Emergency Maintenance**: All work performed in response to a disruption or a threat to the availability of a component of Company's Hosting or Client Infrastructure within the control of Company is defined as "Emergency Maintenance".
   Emergency Maintenance will be conducted based upon the timeframe that the emergency exists. Normal business hours will see an immediate response. For issues that occur during non-business hours, the impact of the event will be evaluated as soon as possible, and appropriate measures taken to return the system to normal availability.
    a. **Notification**: Client will be notified via email should Emergency Maintenance be necessary. Commercially reasonable efforts will be made to notify Client prior to emergency maintenance. Company reserves the right to complete Emergency Maintenance without prior notification to Client if necessary to mitigate risks posed by the need for Emergency Maintenance in a timely manner.