FAQ

This FAQ is in response to questions regarding the RFP for IT services. Proposals are due to Domestic Abuse Intervention Services (DAIS) on April 28, 2025.

Q. What is the make and model of the Firewalls, Switches and Wireless Access Points?

A. Current Firewall = FortiGate-40F. Switches = HP 2920-48G, HP V1910-48G & Aruba 2530-48G (not including a temporary switch belonging to our current IT provider). Wireless Access Points = one is Honeywell 5800RP and three are Open-Mesh MR1750.

Q. Are the Firewalls, Switches and Wireless Access Points currently under maintenance and support from the manufacturer?

A. The Firewall is under warranty through 2026, though it will be replaced shortly. The rest of the devices are past warranty.

Q. What are the make and models of the 2 physical servers?

A. One physical server (HV HOST1) is a ProLiant DL380p Gen8. The second physical server (HV HOST2) is a loaner from our current IT provider and does not belong to DAIS.

Q. What are the server software license versions of the virtual servers?

A. Microsoft Windows Server 2019 Standard Version 10.0.17763 Build 17763

Q. **Can you provide an estimated number of labor hours for the break fix work needed monthly?**

A. We anticipate less than ten hours monthly.

Q. Is there an estimated timeframe for the Future Update- Cloud Services as listed on page 4?

A. We would like this project to be completed by the end of Q2, 2026.

Q. **Can you tell me what current security services are in place ie.) back-up, anti-virus, web filtering, anti-spam agent and any MFA in place?**

A. Back-Up = Acronis, web-filtering = Fortinet, anti-virus = Sentinel One, anti-spam agent = Mimecast, MFA in place on all accounts except for a couple of shared accounts.

Q. Do you have a SIEM in place?

A. We do not. We have been discussing Arctic Wolf with our current vendor.

Q. What are your expectations for camera system support (network support, camera support, DVR support)?

A. Our security company handles camera and DVR support needs. The only issues they cannot handle would be any support needed on our network.

Q. Are your current printers owned or leased?

A. Leased. There should be nearly zero support needed here, unless there are network changes that require us to re-add all printers. We manage most printer issues in-house, and our printing company handles support beyond our expertise & maintenance on printers.

Q. What is your approximate monthly IT support usage (hours per month)?

A. Average monthly hours are generally under ten.

Q. What percentage of your workstations are still running Windows 10?

A. ~9% - we have three laptops and one pc (used to run our security software) that are Windows 10.

Q. Are your workstations and laptops standardized, or do you use multiple brands?

A. We stay as standardized as we can. Our desktop PCs are all the same. Laptop groups vary depending on price at time of purchase and we have one iMac. We tend to stay with HP and Lenovo.

Q. What is your current experience with Microsoft Dynamics? Are you currently using it, or is it something you're considering moving towards?

A. We are not using Microsoft Dynamics and are unlikely to move in that direction.

Q. Are all employees using company-supplied DAIS equipment, or do you have some BYOD (Bring Your Own Device) users?

A. We have a mix of DAIS issues equipment (all desktops and several laptops) and BYOD (laptops or tablets). Many staff use an app on their personal cell phones that mimics our desk phone when out and about, and for completing MFA sign-ins. A few staff use their personal cell numbers.

Q. Would it be possible to conduct a site survey to get a better understanding of your overall IT environment?

A. We would be happy to set up a walk through, and show you our server room, pcs, Wi-Fi hubs, etc., but due to data confidentiality reasons, we don't allow non-vendors to run any type of software to gather data, etc.

Q. What Office 365 subscriptions do you currently have, and who manages them?

A. We have Microsoft 365 Business Premium, and the Operations Manager manages the licenses.

Q. Do you have specific requirements and/or expectations regarding the background screening process for staff assigned to your account?

A. While we will not run background checks for specific staff assigned to our account, we will require their names ahead of time to run through our database. We will also require certain conflict of interest and confidentiality agreements to be signed.

Q. What confidentiality requirements are necessary?

A. There are federal and state laws that DAIS must strictly follow to ensure the protection of the identifiable information of its clients. It is DAIS' policy that all DAIS staff, external visitors, and vendors coming on-site must sign a Confidentiality Agreement. The hired IT Company, as a whole, must also understand and formally agree that any employee who has access to client data will not disclose, reveal, or release personally identifying information or information collected in connection with services provided by DAIS. Data breaches are taken extremely seriously at DAIS due to the safety concerns they pose for survivors of domestic abuse in Dane County.

Q. Out of all your needs, what are your top three priorities that are vital to your organization right now.

A. Stability of our network, protection of our data, and cloud migration (including less physical equipment to manage on-site).

Q. What are your top three vendor capabilities that are vital to your organization right now.

A. 1. Quick responsiveness to outages, security concerns, or important technical issues due to the imperative continuity of our crisis support services. 2. Transparency, communication, and collaboration around planning for future needs for upgrades, services, or equipment. 3. Ability to facilitate a project plan and execution of Microsoft cloud migration,

Q. Is 24/7 onsite availability required? And if so, how regularly?

A. If our network is down or equipment malfunctions and we cannot resolve it through a phone call, then on-site support may be necessary (for example, on weekends). I don't expect this to be a frequent need.

Q. Your 'Financial Proposal Form' indicates hourly rates for service. Are you looking for an hourly aka time-and-materials agreement only or is it safe to assume you would also like pricing for per user / per device support services? Some of our services, specifically backup and security services, are priced on a per user / per device basis exclusively.

A. We are interested in both time/materials and pricing per user/per device.

Q. How regularly do you anticipate requiring after-hours remote support?

A. Very infrequent. We've used after-hours remote support in the past few years when our network is down, and we (DAIS & IT Vendor) can't identify or solve the issue remotely. Another after-hours remote support would also be needed for non-automated tasks, such an unexpected reboot of a server/firewall, which would need to be done when the least number of people are in the building (6pm or 7pm, for example).

Q. How do volunteers access the network? Are they treated as full users? How have you handled supporting volunteers in the past?

A. In our volunteer groups, we have two groups who access shared files. Each group has a DAIS controlled, shared login account, and that account only has access to the one folder on the shared drive that pertains to their work. Most of our volunteers do not access the network at all. They have been supported by Operations in the past and will continue that way.

Q. Do you have a vendor that you work with for your Camera System? Is the support expectation for the cameras or the network?

A. We do have a vendor for our security system, cameras and DVR. That vendor supports issues when we cannot solve them, which is rare. Support for the network would be needed (if it were down), but there should be nothing extra regarding the camera system.

Q. Crisis line / text line: How is this provided and what infrastructure is involved?

A. The Crisis Line is handled through our VOIP system vendor and is managed by our Operations Manager (with support from the vendor when needed). The Text Line is web-based and managed by the Operations Manager (with support from the vendor when

needed). Our IT provider may be involved if the internet & phones were down, or a switch or firewall is the problem. Reliable up-time is important.

Q. What compliance requirements are expected to be followed (e.g., HIPAA)? Please share an example.

A. We have no relevant compliance requirements outside of general data security.

Q. What resources are being accessed remotely? What VPN or remote desktop solutions are in use?

A. We currently use FortiClient VPN and Remote Desktop. Not all staff have access to work remotely. The VPN/RDS are used to access shared drives on the network, as well as the database software we must use for client data.

Q. What backup solution are you currently using for your servers? Are you backing up workstations?

A. We use Acronis for backups. We are not backing up workstations at this time, only servers (every evening). Backups are of the full server including files and the OS so it can be virtualized on a backup appliance or in the cloud if needed.

Q. Do you currently have cyber insurance? If not, are there plans to secure that in the future?

A. Yes, we do carry cyber insurance.

Q. How is Desktop Tier 1 support handled and how do you define Tier 2 support?

A. Tier 1 support is handled in-house by the Operations Manager and Operations Assistant. When we cannot solve an issue, we contact our Tier 2 support. We do not allow staff to contact the Tier 2 support desk without talking to the Operations Manager or Assistant first. Most calls coming in will be from the Operations Manager. We handle new staff set up and terminations, password issues, folder permissions, etc. Tier 2 support may also include new pc/laptop setup and more technical fixes that are needed.

Q. We do not have a SQL DBA. Is this a requirement?

A. No, it is not required.

Q. What type of Developer services are you requesting?

A. This is yet to be determined, but if requested, it would be basic developing skills.

Q. Do you have onsite SLA requirements?

A. On-site incident response for things that cannot be corrected remotely or through a phone call with our Operations staff would be as follows:

- *Critical Priority on-site w/in 2 hrs., issue resolution within 4 hrs.*
- *Moderate Priority on-site w/in 8 hrs., issue resolution within 24 hrs.*
- *Low Priority on-site w/in 24 hrs., issue resolution within 72 hrs.*
- *On-site visits may be necessary for hardware installations, maintenance, or repair but would typically be scheduled ahead of time.*