MANAGED IT SERVICES (MSP) RFP QUESTION RESPONSE

The following document represents the answers to RFP questions proposed through the official process. The questions will be responded to in the order they were received. Due to the repetitive nature of questions received, the question may be higher or lower in the list.

Answers to questions will be identified in red.

Answers to Questions

Response to question set from 3/26

- Can we get a full list of existing licensing for Microsoft 365?
    - 3x exchange online (plan 1)
    - 63x Microsoft 365 Business Basic
    - 32x Microsoft 365 Business Standard
    - 1x Microsoft Entra ID P2
    - 1xMicrosoft Teams Rooms Basic
- Would you be open to recommendations or changes for Microsoft 365 licenses?
    - Yes. One of the things we are looking to do is merge all licenses to "Business Standard", or equivalent, to eliminate old/outdated volume licensed versions of Outlook.
- What is the total count of workstations (desktops, laptops, etc.) that are in the environment?
    - ~55-60
- How many physical hosts and virtual servers?
    - 10 Physical (including Hypervisors)
    - 15 Virtual
- What is the total used space on the servers that will need to be backed up?
    - Same question but total 365 data size
    - 6TB from onsite systems
    - Microsoft 365:
        - Exchange: 500GB
        - OneDrive: 363GB
- How many firewalls are in the environment?
    - 1
- What is the use case for DUO MFA?
    - Secured 2FA for all endpoint computers of users with remote access or access to sensitive information. Additionally, provides 2FA for RDP access to servers and VPN.
- Are there any thin clients in the environment?
    - No
- Number of Active Directory users?

- o 138 (This count may represent inactive accounts. FTE approximate is 70-100 depending on season)

Response to question set from 3/27

- A. On-Site IT vs. MSP Responsibilities
  - o Circuit Ownership & Support
    - In the event of a circuit outage (e.g., internet or WAN carrier failure), should the MSP engage the ISP directly, or is that the responsibility of your on-site IT staff?
      - Onsite IT monitors and will typically engage ISP, however depending on severity it may be escalated to involve MSP assistance
    - Are the MSP and internal IT both authorized to work with the internet provider(s), or will escalation routes need to go through QCAA personnel?
      - Currently internal, however depending on agreement reached MSP could be added as a support contact.
- Boundary of Responsibility
  - o Could you define the lines of responsibility between the internal IT Manager and the MSP? For example, if a workstation issue is found to originate from the core switch or firewall, should the MSP step in immediately or await escalation from internal IT?
    - Varies depending on severity. It is currently a very fluid relationship with active communication back and forth to address issues depending on source. Some simple things like port chances and triage are dealt with internally however depending on the severity of an issue such as routing, VLAN issue, or otherwise, the MSP is engaged from internal IT.
  - o Are all buildings and facilities outside the passenger terminal within the scope of the RFP?
    - Yes. All within MAA direct control. Some spaces are leased to tenants in which case their own equipment is their responsibility, however the MAA has a presence in all spaces.
- Ticket Triage
  - o Will all user issues and infrastructure alerts be routed through the MSP, or does the internal IT manager plan to triage and escalate only select cases? If hybrid, what's the preferred escalation workflow?
    - Presently it's triaged internally and escalated, however depending on capabilities of helpdesk platform and internal IT accessibility of said platform, a hybrid workflow can be established.
- B. Network, System, and Power Redundancy
  - o Redundant Internet Circuits
    - Does the airport currently have more than one active internet connection or cellular backup in place? If not, is redundancy something you would like included as part of our infrastructure recommendations?
      - Yes. Airport is currently configured in an SD-WAN setup with dual internet connections.
- Redundancy of Core Systems
  - o Are there currently any known single points of failure (e.g., only one core switch, firewall, or hypervisor) in the environment? Should redundancy planning be

included in our proposal, and if so, are there current constraints (e.g., rack space, budget, vendor lock-in) we should be aware of?

- There are a couple known single points such as firewall and fiber switch locations that are planned for expansion to HA capacity, planning for budget expense to add in FY26 is expected.

- Power Infrastructure
  - Is there UPS and/or generator backup in place for critical IT infrastructure (servers, switches, wireless controllers)? If so, are these components monitored today, and would you like the MSP to include that monitoring in our scope?
    - Yes. UPS backups are in place at key server/network core locations and handles fluidity between the Airport's two power sources. Monitoring can be added to scope if current UPS' are capable of monitoring.
- C. Support Expectations – Business and After-Hours
  - Definition of After-Hours
    - Is "after-hours" defined as any time outside Monday–Friday, 6 AM–6 PM CST? Are weekends and holidays included under that definition, or do they have separate expectations?
      - Yes. Based on operating personnel hours, that time range is satisfactory. Typical airport shifts are within the 7AM to 4:30PM range for direct-hire employees. There are after hours/overnight shifts on staff however we have not seen any substantial need after hours.
    - Critical After-Hours Scenarios
      - Which types of incidents would you classify as requiring urgent response during after-hours periods (e.g., firewall outage, email failure, airline communications disruption)?
        - Primarily firewall/network outage, interruption of a critical system in the Airport Police/Fire division, or cybersecurity incident.
      - Conversely, which types of issues (e.g., individual user desktop problems) would typically be deferred to regular business hours?
        - Typical incidents revolve around issues with exchange/365 platform or server based services such as Print/File Shares. Workstation issues beyond internal triage availability are also escalated.
  - Critical Operating Hours
    - Are there specific hours or days considered "mission-critical" for airport operations, such as early morning flight windows or holiday travel peaks? Should service prioritization be adjusted based on flight volume or staffing?
      - The airport has primary working shifts for teams within the 7A-430P range. Flight volume/staffing typically doesn't impact prioritization of services as airlines have their own IT systems that are independent of airport owned systems.
- D. Help Desk and End-User Support
  - Role of On-Site IT Manager
    - Will the on-site IT Manager continue to handle routine desktop support and internal triage, or is the MSP expected to provide regular user support (either remote or on-site) during business hours?

3

- - - • Based on current issue quantity/occurrence, the onsite IT will likely continue with internal initial triage during business hours.
  - Help Desk Add-On Scope
    - If 24x7 Help Desk support is purchased later as an add-on, would this be for all QCAA employees, or are there subsets of users (e.g., operations staff, tenant businesses, TSA teams) who would be included or excluded?
      - Primarily for direct employees of the MAA. The airport does not support any tenant businesses, TSA, or Airlines beyond control of Fiber Optic pathways.
  - Does the Help Desk need to be US based?
    - Preferred.
- E. Physical Access & Security Zones
  - Server and Network Room Access
    - What are the requirements for MSP personnel to gain physical access to secure IT areas (e.g., background checks, badges, escort requirements)?
      - MSP personnel onsite are required to obtain a background check and fingerprinting prior to access to a secured area. Video-based training is also required.
    - Will MSP staff be permitted to access those areas independently once cleared, or will they always need to be accompanied by airport personnel?
      - Once cleared, badged personnel may move unaccompanied and also escort employees that are not badged.
  - Access Hours and Restrictions
    - Are there any restrictions on when the MSP can access network/server rooms (e.g., during normal business hours only)? What is the emergency access procedure if immediate intervention is needed outside those hours?
      - No. Procedure can be determined between onsite IT and MSP, however it can be expected that immediate access to site can be attained in conjunction with a notification to onsite IT.
- F. Compliance and Cybersecurity Governance (CISA / TSA)
  - Regulatory Frameworks in Use
    - The RFP references TSA, NIST, and CISA requirements. Could you specify which cybersecurity compliance frameworks (e.g., TSA SD 1580/82-2022-01, NIST 800-171, CISA Cross-Sector Cybersecurity Performance Goals) QCAA is currently aligned with or planning to implement?
      - The airport most closely aligns with the CISA Cross-Sector goals. Employing best practices, and zero trust protocols such as automated firewall rules to isolate services to those only with need. We strive to take the necessary approach to isolate critical operational systems and open only as necessary.
  - Attestation vs. Third-Party Validation
    - Is QCAA currently pursuing a self-attestation model for cybersecurity compliance, or is there a mandate for third-party audits or certifications from external firms?

4

- Combination of both. Self-attestation for standard practices throughout regular operations. However external third-party testing to identify any holes is expected.
  - If third-party validation is expected, are there preferred assessment vendors, audit standards, or certification types the airport must comply with?
    - None known
  - o Incident Reporting Protocol
    - In the event of a security incident, what is the protocol for notification, documentation, and recovery reporting to the airport? Are there TSA or CISA-mandated forms or procedures the MSP must follow?
      - MAA maintains a cybersecurity incident workflow which dictates the process for notification of required parties.
  - o OT (Operational Technology) Support
    - Are any systems considered OT (e.g., badge access, surveillance, airfield lighting control) part of the MSP's monitoring or security responsibilities? Should these be integrated into the security roadmap or vendor coordination?
      - Yes. Any computers accessible from internal networks are considered part of scope. Badging and surveillance are currently accessible. Airfield lighting control is isolated and not connected in any way.
    - Does any of the compliance require FedRAMP certified services and/or services that are only on US soil?
      - Non presently. Best effort should be exerted to ensure cloud services are not housed offshore, but the airport isn't held to the same federal regulations.
- G. Vendor Coordination and Software Oversight
  - o Third-Party Vendor Expectations
    - Does QCAA expect the MSP to coordinate directly with third-party vendors (e.g., access control, baggage handling systems, airline interfaces) for troubleshooting and integration, or will that be handled by internal personnel?
      - Internal
  - o Licensing Oversight
    - Beyond the Microsoft 365 and Cisco Duo licenses mentioned, will a full software and licensing inventory be provided? Should the MSP assume responsibility for managing licensing renewals and compliance?
      - No. Specialty software licensed outside of MSP provided software will be handled internally.

Response to questions set 1 from 3/28

- **General Clarification Questions**
- Can you clarify any specific expectations around collaboration between the onsite IT Manager and the MSP?
  - o The airport maintains a very dynamic and open-communication relationship currently between the IT manager and MSP. Back/forth discussions over certain areas frequently occur over Teams. The IT Manager conducts a lot of the day-to-day needs as well as overall program direction, with the MSP serving at a

higher level for system/network engineering, helpdesk escalation, and other requests as they occur.

- Are there any preferred platforms or tools currently in use for network monitoring, cybersecurity, or endpoint management?
  - A lot of the monitoring tools in use are MSP maintained such as N-Able and Sentinel One. However the onsite IT personal also maintain their own suite for monitoring and log collection such as LibreNMS, Graylog, and other tools to help supplement.
- Will the MAA be open to recommendations for alternative tools or software that could optimize operations?
  - Yes
- **Compliance and Security**
- What are the primary pain points in maintaining TSA and CISA cybersecurity compliance?
  - The biggest thing is the ever evolving landscape. There are continuous changes in attack methods and vectors which TSA and CISA frequently send out notices for. Staying on top of system integrity, network segmentation, and policies, both proactively and reactively are critical.
- Can you provide details about the most recent cybersecurity assessment findings or audits?
  - If the MSP is selected these would be able to be shared. Due to the nature of the information falling into Sensitive Security Information (SSI), we are unable to directly share those.
- What level of access will the MSP have to existing compliance reports, network diagrams, and incident response plans?
  - MSP would have access to available information.
- **Technical and Operational**
- How are current infrastructure and network management services being handled? Are there areas where the MAA seeks improvement?
  - Overall infrastructure and network management is kept up-to-date by MSP with patches and policies rolled out both at regular intervals by MSP and at the direction of the onsite IT based on needs/changes.
- What specific metrics or key performance indicators (KPIs) will be used to evaluate MSP performance?
  - The following information are some examples of what will be used:
    - Uptime/downtime of critical platforms
    - Mean time to respond/resolve incident
    - SLA Adherence
    - Breach Count or SLA that could lead to breach
    - Backup Test Success Rate
    - Internal Team Satisfaction
    - Server/Network Latency
    - Satisfaction of relationship between internal stakeholders
- Is there a current disaster recovery and business continuity plan in place? How frequently is it tested?
  - Yes. It is expected that the MSP would test BDR annually. Additionally, recurrent test of backups for resiliency is requested.
- **Onsite and Remote Support**
- What is the average number of critical incidents requiring onsite support per month?

- o It's dynamic, there could be nothing in a given month or two, and then 5 the following.
- Are there existing escalation procedures that the MSP should follow during incident response?
  - o The main escalation centers around communication and relationship with onsite IT. Incident response will be coordinated and needed parties outside of IT notified from there.
- Can you clarify the expectations for the 24/7 Security Operations Center (SOC) response times in comparison to the proposed SLAs?
  - o The biggest thing is analyzing and reacting to detected threats. For example in a lateral movement detection: actively isolating affected devices, notifying critical parties, and removing/reverting breaches and investigating source. In these cases they often require an immediate response to stop it from becoming a severe event which a standard helpdesk SLA may not meet.
- Is the MAA open to creative pricing models, such as bundled service options or value-based pricing?
  - o Absolutely.
- Are there preferred terms for contract length and opportunities for performance-based renewals or bonuses?
  - o Typically the airport would prefer a 1 year initial. However up to 3 to start may be considered for preferential pricing. Early renewals based on performance are certainly up for discussion.
- Would the MAA consider separate pricing for proactive security enhancements or additional cybersecurity services not outlined in the base proposal?
  - o Sure. Part of this proposal process is so that the MAA can identify the budged needed for the FY26 and allocate accordingly.
- What factors are most important to the MAA when evaluating proposals beyond cost (e.g., innovation, past experience, compliance expertise)?
  - o All of the above with ability for the MSP to closest meet the requested needs of the RFP outline in a cost efficient manner. The airport values the relationship with the MSP and having the ability to demonstrate the experience, provide development ideas, and recognize compliance requirements are crucial.
- How would you describe an ideal MSP partner in terms of communication, responsiveness, and collaborative problem-solving?
  - o An ideal partner is one who has a close relationship with onsite IT. Back and forth open collaboration through IM/email is vital to ensuring needs are met, identifying changes, and further progressing the airports IT mission.

Response to question set 2 from 3/28

- Can you elaborate on the current pain points and challenges in airport operations, such as security screening, baggage handling, and airfield management?
  - o The airport is unable to comment on security screening or baggage handling due to SSI restrictions. However for the most part the IT operations at the airport center around the physical property and it's direct-hire employees. The airport does not control airline, TSA, or other tenant IT systems.
- How do you envision the ideal airport operations workflow, and what role can technology play in streamlining these processes?

- o There's a close relationship between all stakeholders at the airport. Technology plays an increasing role in everyday lives and frequent meeting with all airport personnel to collaborate and bring technologies to the floor is key.
- What are the key performance indicators (KPIs) for airport operations, and how can we measure the success of our solution in addressing these metrics?
  - o See prior KPI question.
- Are there any specific regulatory or compliance requirements that our solution must adhere to, such as TSA or FAA regulations?
  - o There are many. The biggest control centers around separation of OT (Operational Technology – card access, automation, etc) and IT (Information Technology – email, workstation, etc) are the main touch-points.
- How can we ensure that our solution is scalable and flexible to accommodate future growth and changes in airport operations?
  - o The best solution is one that closely meets the requirements of the RFP and maintains an open relationship with the airport, it's IT staff, and other personnel.
- Can you describe the ideal passenger experience at Quad Cities International Airport (QC Airport), from curb to gate, and what role can technology play in enhancing this experience?
  - o Technology is an ever-advancing role and there's many things that are often considered bleeding-edge, and cutting-edge. What works best is a plan that best supports the passengers at the airport in a reliable and verifiable manner. That being said, the airport IT operation, aside from a public WiFi and Flight Status displays, do not have a direct impact on passenger experience.
- How can we personalize the passenger experience, and what data sources can we leverage to inform these efforts?
  - o The airport IT operation, aside from a public WiFi and Flight Status displays, do not have a direct connection with passenger experience.
- What are the key touchpoints and pain points in the passenger journey, and how can we address these through our solution?
  - o The airport IT operation, aside from a public WiFi and Flight Status displays, do not interact with passenger journeys currently. Support of devices and networking to minimize interruption of security services that, when down, may inhibit certain functions are key.
- Are there any specific accessibility or inclusivity requirements that our solution must address, such as accommodations for passengers with disabilities?
  - o To maintain anonymity on the process, we are unable to directly answer based on the solution specifics. ADA compliances typically center around some of our public facing web pages which we are currently in compliance with.
- How can we ensure that our solution is intuitive and user-friendly for passengers of all ages and technical abilities?
  - o Current RFP request does not have a passenger facing component aside from a publicly accessible WiFI.
- **Sustainability and Environment:**
- Can you elaborate on QC Airport's sustainability goals and objectives, and how our solution can support these efforts?
  - o To maintain anonymity on the process, we are unable to directly answer based on your solution specifics. The airport maintains a goal of looking at what is best to improve airport business operations. Being a steward towards sustainability

includes finding more energy efficient technologies and equipment for all aspects.

- What specific environmental initiatives or programs are QC Airport currently undertaking, and how can our solution integrate with or support these efforts?
  - The airport maintains a strong approach and adheres with all regulations towards technology. Environmental initiatives include HVAC system tuning to best economize and minimize waste, automation of lighting systems to minimize usage and lower energy costs.
- How can we reduce energy consumption and greenhouse gas emissions through our solution, and what technologies or strategies can we leverage to achieve these goals?
  - To maintain anonymity on the process, we are unable to directly answer based on your solution specifics. The biggest thing around IT at the airport is identifying energy efficient technology systems through planned upgrades and replacements.
- Are there any specific waste management or recycling programs that our solution must integrate with or support?
  - To maintain anonymity on the process, we are unable to directly answer based on your solution specifics. The airport however maintains an active e-waste recycling plan to ensure sustainable recycling of retired IT materials.
- How can we ensure that our solution is designed with sustainability and environmental responsibility in mind and that it aligns with QC Airport's overall sustainability vision?
  - To maintain anonymity on the process, we are unable to directly answer based on your solution specifics. The airport however has a desire for sustainability in its aspects as it pertains to technology.
- **Technology and Innovation:**
- Can you describe the current technology infrastructure at QC Airport, including any existing systems or platforms that our solution must integrate with?
  - To maintain anonymity on the process, we are unable to directly answer based on your solution specifics. The airport however has a series of interconnected system between HVAC, Security, and corporate networks. All of this operates on a site-wide fiber backbone which services the airport and its tenants.
- What emerging technologies or innovations is QC Airport interested in exploring or leveraging, such as biometrics, blockchain, or the Internet of Things (IoT)?
  - We find an increasing use in IoT devices for things such as wireless temperature/occupancy sensors, biometrics for authentication, and more. Conferences are frequently attended to identify emerging technologies and see what best fits in the need of the airport.
- How can we ensure that our solution is scalable and flexible to accommodate future technological advancements or changes in airport operations?
  - To maintain anonymity on the process, we are unable to directly answer based on your solution specifics. The airport expects a close relationship with the selected MSP to identify future technological advancements and develop a path forward.
- Are there any specific cybersecurity or data protection requirements that our solution must address, such as protecting passenger data or preventing cyber threats?
  - To maintain anonymity on the process, we are unable to directly answer based on your solution specifics. The biggest need centers around ensuring cyber resiliency against outside and internal threats.

- How can we foster a culture of innovation and experimentation at QC Airport, and what role can our solution play in supporting these efforts?
  - To maintain anonymity on the process, we are unable to directly answer based on your solution specifics. The airport values a dynamic and open relationship with the selected MSP and desires an environment for a collaborative and progressive path forward.
- **Cybersecurity:**
- **Vulnerability Management:** What tools or processes do you currently have in place for vulnerability scanning and patch management?
  - We currently have the tools that the current MSP provides for scanning with center around N-Able and Sentinel One.
- **Endpoint Detection and Response (EDR):** What solution are you currently using for Endpoint Detection and Response (EDR)?
  - N-Able and Sentinel One are the main tools however there are also more sets involved.
- **Penetration Testing:** What level(s) of penetration testing are expected (e.g., internal, external, application, network)? Is there an existing testing schedule, or should the vendor propose one?
  - It is the desire of the airport that the vendor provide a plan for internal/external testing. We strive for an annual approach to a full-scale test, however recurrent audits are done frequently to ensure current configurations meet expectations.
- **IT Asset Management:** What tools or processes are currently in place to provide visibility into and manage your IT assets?
  - There is a combination of MSP maintained and internal IT tools to support the assets. MSP has their own suite of tools that is self contained and the internal IT tools consist of monitoring and logging platforms such as LibreNMS and Graylog.
- **Cloud SaaS Management:** What are the critical SaaS applications that require protection? What solution(s) are you currently using for Cloud SaaS security?
  - The primary SaaS application the airport uses is Microsoft 365. Cloud security centers currently around Barracuda for inbound email threat management combined with Defender on the Microsoft side.
- **Mobile Security:** How many mobile devices require security coverage? What mobile security solution(s) are currently in place?
  - None presently. Employee provided mobile devices serve primarily for communication via email/phone and do not interact with systems aside for specific cases.
- **Incident Response:** Do you have a formal Incident Response Program in place? How do you currently evaluate the effectiveness of your Incident Response Program?
  - Yes. The airport, by TSA mandate, has a recurrent annual test to ensure the program is where it needs to be.
- **Security Awareness Training:** What platform or approach are you currently using for security awareness training? What has been your experience with phishing simulations, and how do you measure success?
  - The airport has a phishing email testing platform to continuously test employees with false positives. Success is measured in the amount employees that fall for the test.
- **DNS Security:** Are you currently utilizing a DNS security solution? If so, which one?
  - Yes. Cloudflare

- **Email Security:** What measures are currently in place to protect email communications? Have you experienced notable issues with phishing or other email-based threats?
    - The airport uses the Barracuda cloud platform to screen inbound emails. There has been an uptick lately however employees have been responsive to those and there are currently no known failures.
- **Technical Clarification Questions:**
- Can you please clarify total counts of
- User?
    - 70-100 depending on the season
- Workstation/Laptop Device?
    - 55-60
- Network Switches?
    - 25
- Firewalls?
    - 1
- **Partnerships and Collaboration:**
- Can you describe the current partnerships and collaborations between QC Airport and other stakeholders, such as airlines, ground handlers, and concessionaires?
    - The airport has an open relationship between all aspects of the airport, regular meetings for news and information are held between all stakeholders to ensure all are informed.
- How can we foster stronger partnerships and collaboration between these stakeholders to enhance the passenger experience and improve operational efficiency?
    - The selected MSP will be the one that best meets the airports needs. This selection will aid the airport in ensuring an optimal technical operation to ensure no interruptions of various internal departments.
- What role can our solution play in supporting these partnerships and collaborations, such as through data sharing or integration with existing systems?
    - To maintain anonymity on the process, we are unable to directly answer based on your solution specifics.
- Are there any specific industry associations or advocacy groups that QC Airport is involved with, and how can our solution align with or support these efforts?
    - To maintain anonymity on the process, we are unable to directly answer based on your solution specifics. There are no known industry or advocacy groups that would be correlated with a MSP at the airport.
- How can we ensure that our solution is designed with the needs and priorities of all airport stakeholders in mind, including passengers, airlines, and concessionaires?
    - To maintain anonymity on the process, we are unable to directly answer based on your solution specifics. The MSP that best aligns with the Airport plan is one that meets the needs as outlined in the RFP, maintains an open relationship with internal IT and other stakeholders, and meets all highlighted needs in the RFP.