



Technology Master Plan

A Framework for Implementing Technology
at the Santa Clara Valley Open Space Authority



REVISION HISTORY

Revision Number	Revision Date	Nature of Revisions
0	09/15/2020	Original
1	04/28/2021	Updated exhibits; added estimated implementation timeline.
2		
3		

CONTENTS

Introduction	1
Current Environment	2
Network Services and Hardware	2
Internet Connectivity	2
Firewall.....	2
Switches	3
Server	4
Avaya Private Branch Exchange (PBX)	5
Management Console	5
Uninterrupted Power Supplies	6
End-User Devices and Software.....	6
General Overview	6
Workstations.....	6
Mobile Devices.....	7
Other Computer Peripherals.....	7
Software.....	7
Policies	9
Electronic Records and Communications	9
Prohibited Uses of Electronic Tools	9
Network Security	10
Remote Access Policy.....	10
Information Technology Operations.....	11
Ideology.....	11
Recurring Maintenance.....	11
Recurring Security Audits.....	12
Backup Plan.....	12
Support Tools	13

Exhibit D

RMM	13
TeamViewer	13
MSP360 (formerly Cloudberry Lab)	13
Strategic Planning 2020 – 2025	14
Goals and Objectives.....	14
Reliability.....	14
Innovation	16
Security	17
Estimated Implementation Timeline	19
Approval of Projects.....	19
Glossary.....	20
Exhibit A	22
Exhibit B	23
Exhibit C	25
Exhibit D	26
Exhibit E.....	27
Exhibit F.....	28

INTRODUCTION

The Santa Clara Valley Open Space Authority (Authority) is a public, independent special district created by the California state legislature in 1993 at the urging of community leaders who saw the importance of maintaining the ecological integrity of the region.

The Authority conserves the natural environment, supports agriculture, and connects people to nature, by protecting open spaces, natural areas, and working farms and ranches for future generations. The Authority envisions the Santa Clara Valley and its surrounding hillsides as a beautiful place where a vibrant network of interconnected open spaces, trails, wildlife habitats, and thriving agricultural lands enrich the region's cities and make it an exceptional and healthy place to live, work, learn, and play.

To effectively execute the agency's vision, the Authority understands the importance of ensuring reliable productivity and collaboration technologies are available to staff so that they may perform their roles and responsibilities efficiently.

The Authority's IT team currently consists of two members: the IT Technician responsible for day-to-day technical support and maintenance of the agency's network and systems, and the Accounting and Financial Analyst, who supervises the IT Technician and provides support to special projects. The agency also has an on-call contract with Veltec Networks, an IT service vendor, to augment the IT Technician's part-time hours (30 hours a week).

The purpose of the Technology Master Plan is to document the existing technological environment and evaluate the agency's needs over the next five years. The resulting assessment will help IT staff plan for scalability and guide future IT projects and standards, such as establishing minimum requirements for new system deployments, informing future hardware procurements, promoting best practices, and acknowledging limitations of IT staff and resources.

CURRENT ENVIRONMENT

Network Services and Hardware

INTERNET CONNECTIVITY

The Authority signed a five-year master agreement with Comcast in May 2017 to secure dedicated internet access for the office building (symmetrical bandwidth of 50 Mbps). The fiber connection originates from the office building's telephone room and routes into a secured server room. Comcast provides internet access through a Ciena fiber optic switch. The telecommunications provider also supplies an ADTRAN unit, a device that allows the Authority to handle incoming and outgoing calls. The ADTRAN is configured with a full Primary Rate Interface (PRI) line, allowing staff to make and receive up to 23 simultaneous calls over the internet. The equipment is mounted to a plywood backboard and connected to the agency's network devices, which all reside in an industry-standard four-post 42 rack unit server. Please see [Exhibit A](#) for a diagram of the Authority's server rack.

In addition to providing internet connectivity and telephony equipment, Comcast also provides two different internet protocol (IP) blocks to the Authority:

- A point-to-point (P2P) block which is associated with the Ciena switch. This block of addresses contains the WAN IP address, which is the address given to the router/firewall that is connected to the internet. This block of addresses is public-facing and can be seen by others on the World Wide Web.
- Six (6) customer routable blocks which can be assigned to different local network devices. Each block of 256 IP addresses are available for the network administrator to assign to Authority devices.

Wired internet access is available in individual offices, conference rooms, cubicle workstations, and the Board Room. The Authority has also configured a mesh wireless network by installing twelve (12) strategically-placed Ubiquity Unify AP-AC Pro access points throughout the office building, as indicated in [Exhibit B](#). For security purposes, wireless communications for guests run through a different virtual local area network (VLAN) to prevent unauthorized access to network resources and data on the file server. Additional technical specifications for the wireless access points can be found in [Exhibit C](#).

FIREWALL

A firewall is a network security device that monitors incoming and outgoing network traffic and allows or blocks data packets based on a set of security rules. Its purpose is to establish a barrier between the internal network and incoming traffic from external sources (such as the internet) in order to block malicious traffic like viruses and hackers.

In 2017, the Authority procured a Dell SonicWall Network Security Appliance (NSA 2600). The NSA Series firewalls have been acclaimed for its world-class security and performance, ease of use, and cost-effectiveness. SonicOS, SonicWall's operating system, provides features such as real-time visualization, intrusion prevention system (IPS), high-speed virtual private networking (VPN), and other security features. The Authority maintains an annual renewal of the comprehensive gateway intrusion services.

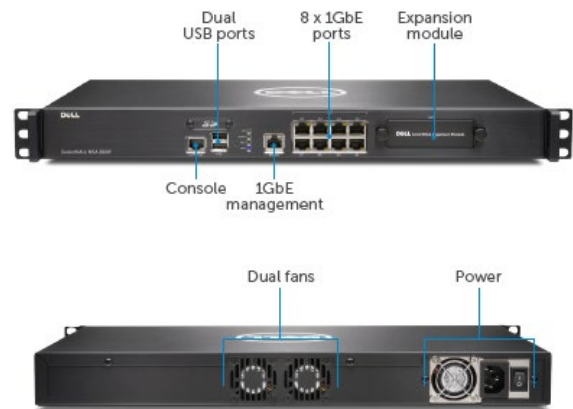
Technical Specifications ([Exhibit D](#))

Firewall Inspection Throughput	1.9 Gps
IPS Throughput	700 Mbs
VPN Throughput	1.1 Gps
Connections per Second	15,000/sec
Maximum Connections	500,000

Licensed Security Features

- Content Filtering
- Gateway AV/Anti-Spyware/Intrusion Prevention
- Capture Advanced Threat Protection
- Global VPN Client – 54 of 60 client licenses used

Network Security Appliance 2600



SWITCHES

Switches connect multiple network devices to the Authority's Local Area Network (LAN) within a building. A switch enables connected devices to share information and talk to each other.

The Authority uses two (2) Netgear ProSafe 48-Port Stackable Smart Switch with Power Over Ethernet (PoE). These switches provide scalability, reliability, and performance for small to medium-sized growing organizations. An advantage for procuring stackable switches is that additional switches can be added to provide resiliency and scalability at a later time without disrupting the network. The stack creates a virtual chassis for easy management under a single IP address. PoE ports supply power through the network cable which optimizes the installation and management of network devices such as Voice Over Internet Protocol (VoIP) phones and wireless access points (WAPs).

Technical Specifications ([Exhibit E](#))

Network Latency	Less than 20 ms
Bandwidth per unit	104 Gbps
Stacking bandwidth	5 Gbps
PoE+	384 Watts
Number of VLANs	256
Number of Routed VLANs	15

As of September 2020, 94 of the 96 available ports are in use (72 data, 13 WAPs, 6 IP phones, 1 firewall connection, 2 management ports).

SERVER

One of the most important components of an entire network infrastructure is the server. A server is a powerful computer that provides various shared resources to workstations and other servers on a network. The shared resources can include disk space and access to other networked peripherals.

Most of the Authority's working files and official records are stored on the server. Using an PERC H730P controller card to manage the RAID (Redundant Array of Independent Disks) configuration, the agency's data is protected and can be accessed should a hard drive disk fail.

The agency's server, recently procured in late 2020, is built on Dell's hardware and utilizes the Windows Server 2019 operating system to manage its business services, as summarized below.

Technical Specifications

Model	Dell R640
CPU	Dual Intel Xeon 2.30Ghz
RAM	97 GB DDR4
Storage	2.6 TB SSD (RAID 10)
System Type	64-bit, x64-based

Windows Server Roles

- **Domain Name Service (DNS)** – Websites are accessed online through common domain names, like www.openspaceauthority.org, but web browsers interact through Internet Protocol (IP) addresses. A Domain Name System (DNS) translates domain names to IP addresses so browsers can load Internet resources. Without DNS, other server roles will not function properly.
- **Dynamic Host Configuration Protocol (DHCP)** – a DHCP server dynamically assigns an IP address and other network configuration parameters to each device on the network, so they can communicate with other devices. A DHCP server enables computers to request IP addresses and networking parameters automatically from the Internet service provider (ISP), reducing the need for a network administrator or a user to manually assign IP addresses to all network devices.
- **Active Directory** – a directory service developed by Microsoft for Windows domain networks. A directory service is a hierarchical arrangement of objects which are structured in a way that makes access easy. However, functioning as a locator service is not AD's exclusive purpose. The service is used to manage computers and other devices on a network, authenticates and authorizes all users and computers in a Windows domain type network, assigns and enforces security policies for all computers, and installs or updates software.
- **File and Storage Services** – includes technologies that help you set up and manage one or more file servers, which are servers that provide central locations on the network where files can be stored and shared with users.

- **Synchronization Service Manager** - Windows Server's Synchronization Service Manager connects to the Authority's Azure Active Directory, providing Single Sign On (SSO) capabilities to Office 365 for Authority staff. SSO minimizes password reuse, streamlines the user experience, and reduces IT helpdesk support for forgotten passwords.

AVAYA PRIVATE BRANCH EXCHANGE (PBX)

Avaya's PBX system provides telephone and voicemail features for the Authority's voice over internet protocol (VoIP) phone system. Avaya's IP 500 V2 Private Branch Exchange (PBX) hardware system with a DIG ADPx16 RJ45B—1 expansion module is currently used as the core infrastructure for voice services, allowing up to forty (40) Avaya digital phones and five (5) IP phones to be connected to the system.

Avaya handsets and conference phone models compatible with the Authority's system include: 9508 digital phones, 9608 IP phones, and B179 SIP conference phones.

The Authority purchased and installed the PBX system in January 2014. At that time, the agency had more than one office location. IP phones allowed staff in satellite offices to connect to the central PBX system. While the IP phones are still compatible with the system and continue to be used at the office headquarters, subsequent phones added to the PBX system must be digital phones. The agency currently contracts with ConvergeOne, a leading IT services provider specializing in Avaya phone systems, to offer annual maintenance and support of the system. The agreement provides the Authority with system updates and up to eight (8) hours of support.

Current License Count

Essential Edition	255
Power User	6
Office Worker	10
Avaya IP endpoints	5
Avaya SIP Softphone	6
R8+ Preferred Edition	1

MANAGEMENT CONSOLE

A Windows 10 workstation is configured as a management console for IT staff to monitor the Authority's network activities, manage system settings, and ensure systems are running optimally.

Technical Specifications

Motherboard	Dell 0XJ8C4
CPU	Intel Core i5-6600k 3.50Ghz
RAM	32 GB DDR4
Storage	2 TB
Graphics	NVIDIA GeForce GTX 745
System Type	64-bit, x64-based

- **SonicWall Universal Management Suite** helps establish comprehensive security management and analytic reporting for the Authority's firewall.
- **UniFi's Network Management Controller** is used to manage the Authority's wireless access points.
- **IP Office Manager** is used to manage the Authority's Avaya private branch exchange (PBX) phone system.

UNINTERRUPTED POWER SUPPLIES

The Authority currently uses an APC Smart-uninterrupted power supply (UPS) 1500 system with two batteries connected in series to provide temporary power to critical equipment in the event of a power outage or brownouts. The batteries may continue to provide temporary power up to approximately 30 minutes based on the current number of equipment connected to the UPS system.

Technical Specifications



Output Voltage	120.2 VAC @ 60.0Hz
Load Current	2.9 Amps
Output VA	24.0 %
Output Watts	29.9%
Output Efficiency	96.0 %
Output Energy Usage	6288.61 kWh

The PowerChute Network Shutdown App is installed on the server which sends a shutdown command so that the server has sufficient time to properly end its services and avoid data loss or corruption. The shutdown command is set up to run approximately ten (10) minutes after a detected outage to ensure the systems are properly shut down before the batteries deplete fully.

End-User Devices and Software

GENERAL OVERVIEW

IT currently manages an array of electronic devices which include desktops, laptops, tablets, and mobile devices. A current breakdown of the device types is summarized in the table below.

			
7	55	16	26

WORKSTATIONS

Workstations (desktops and laptops) are the productive heart of the Authority. The Authority's preferred hardware manufacturers include Lenovo and Dell. Each workstation runs on a 64-bit Windows 10 operating system and is preconfigured with general use applications such as Microsoft 365 suite, Adobe Acrobat Reader, Webroot Antivirus, SonicWall's Global VPN client, and Backblaze, a cloud backup application. Minimum requirements for workstations can be broken down into two categories listed below:

Basic User – these users utilize their workstation for general administrative tasks such as document editing and web browsing. Minimum requirements include an Intel i5 processor and 8GB of RAM.

Power User – these users need more processing power to handle applications such as photo and video editing software, geographic information system (GIS), and computer-aided design (CAD) rendering software. Minimum requirements include an Intel i7 processor, 16GB of RAM, and a dedicated video card.

MOBILE DEVICES

The Authority assigns mobile devices to all field personnel, as well as additional personnel based on the need and requirements of their role. Staff may be assigned a device from either Apple (iOS operating system) or Samsung (Android operating system).

The agency has an enterprise cellular plan with AT&T to provide unlimited talk and text, along with 60GB* of shared data. The shared data allows staff to check emails, upload files, and utilize GPS for navigation and safety purposes.

**Due to the COVID-19 pandemic, the Authority has procured unlimited data plans for certain lines for specialized purposes of streaming live events, hosting virtual outreach events, and providing Wi-Fi hotspot coverage.*

OTHER COMPUTER PERIPHERALS

The Authority recognizes that staff needs the proper tools and an ergonomic work environment to best perform in their roles. For staff using laptops, Authority provides docking stations to provide connectivity to monitor displays, wired Ethernet connection, and extra USB ports. At staff's request, ergonomic fittings and equipment such as keyboards and mice are provided.

IT also provides support for twelve (12) onsite printers: two (2) Konica Minolta industrial office printers, two (2) HP plotter printers, seven (7) HP office printers, and one (1) Canon office printer.

Type of Printer	Quantity	Usage
Industrial office printers	2	Workloads that require hundreds of pages
Plotter printers	2	Topographical maps
Regular office printers	8	General office usage

The IT team is responsible for providing said tools and ensuring any computer peripherals are compatible with the agency's network or workstations.

SOFTWARE

Out-of-the-Box Consumer Software

The following list of common software applications are approved for use and supported by the IT team.

Name	Description
Adobe Acrobat Reader or Pro	PDF viewing and editing software
Adobe Creative Suite	Video and image editing software
ArcGIS Desktop	Geographical Information System (GIS) tools used for spatial analysis
ArcGIS Pro	GIS cloud tools used to create interactive online maps
Backblaze Backup	Cloud backup solution
Google Chrome	Web browser
Google Earth Pro	Digital land surveying tool
Microsoft 365 Apps	Productivity software
Webroot Anti-Virus	Antivirus software

The IT team has configured and deployed several applications within the Microsoft Office 365 suite for Authority staff use. Microsoft Outlook, Word, Excel, PowerPoint, and OneNote are the default productivity apps. Microsoft Teams is the default messaging and video/audio conferencing application. Staff is also allocated 1TB of cloud storage on OneDrive for file-sharing and collaboration purposes. Additional apps, such as Microsoft Forms and Power Automate, are also available to staff through the online portal, but IT does not locally install these apps by default.

Based on their role and responsibilities, staff may also request licenses for Microsoft Visio and Microsoft Project.

Cloud-based Enterprise Software Systems

The Authority contracts with several software consultants to host, support, and maintain cloud-based enterprise software systems configured for specific purposes. IT staff does not provide support for the following software systems:

Name	Description
Acumatica	Accounting and time tracking system
Hubspot	Customer relationship management system
ArcGIS Pro	Geographical information system
PrimeGov	Electronic agenda management & governance system

The responsible program manager or department is directly involved in the maintenance and administration of the software systems. Occasionally, IT staff is requested to provide input with regards to compatibilities to the agency's network infrastructure and/or configurations.

POLICIES

The goal of IT policies is to ensure the proper use of electronic media for communication and research purposes for the benefit of the Authority and the public. Furthermore, due to the reliance of computer-based technology and information systems, policies are established and enforced to protect the Authority's technology assets from threats associated with unauthorized access, inappropriate use, information leakage, and data integrity.

The following section summarizes the policies currently in effect at the Authority.

Electronic Records and Communications

All electronic communications, systems and media, including computer files, hardware, software, and email and Internet access are the property of the Authority, regardless of their physical location or the form in which they are maintained. Furthermore, all data, pictures, files, folders, graphics or other material stored on the server or individual computer workstations is the property of the Authority.

Prohibited Uses of Electronic Tools

The following are prohibited Internet/Electronic Communication/Social Uses of Authority computers and electronic devices and tools. This description of prohibited uses is not exhaustive, and it is within the discretion of the Authority to determine if there has been a violation of this policy:

- Use or transmission of material or usage in a manner, which constitutes harassment or disparagement of others or is threatening, defamatory, obscene or sexually explicit;
- Download and/or installation of software onto Authority equipment without the authorization of the Authority's Network Administrator;
- Use in a manner that constitutes copyright or trademark infringement;
- Use in a manner that violates software-licensing rules;
- Use in any manner that is illegal or contrary to the goals of the Authority;
- Transmission of messages that disclose personal information without authorization;
- Disclosure or discussion of confidential information;
- The use of aliases - This includes the use of "anonymous", alias, message board postings, or re-mailing services to protect or hide individual identity;
- Unauthorized access to other employees' files;
- Any use which results in private gain for the employee, soliciting others for private commercial ventures, religious or political causes, outside agencies, or any other non-Authority related matters;
- The display of any kind of sexually explicit multimedia content, message, or document on any Authority computer;
- Unauthorized use of social media on behalf of the Authority

Network Security

To protect the Authority's privacy interests in its official business messages and assure the security of the electronic mail systems, IT requires all employees to change their password every 180 days.

Passwords must contain a minimum of eight (8) characters, including one special character, and previous passwords may not be reused.

Remote Access Policy

The Authority provides remote access through a Virtual Private Network (VPN) to Authority employees, as approved by management. A completed VPN/RDP Request and Authorization Form is required for each individual requesting access to maintain network security and compliance. The use of the VPN connection is available to staff with more than six (6) months of tenure and is for agency-related business only.

VPN account holders agree to the following:

- Has read, understood and will abide by the Authority's Internet/Email and Network Security policy as stated in the Employee Handbook.
- Will only access systems and resources that the account holder is authorized to access.
- Will notify itsupport@openspaceauthority.org immediately if they believe their VPN account is compromised or misused.

Note: The six-month waiting period for VPN access has be waived for the duration of the shelter-at-home orders from Governor Gavin Newsom and the Santa Clara County Health Officer.

INFORMATION TECHNOLOGY OPERATIONS

Ideology

The Authority's IT team focuses on maintenance that is proactively performed with the goal of mitigating the likelihood of network and equipment failure, reducing unexpected downtime, and prolonging the useful life of its equipment.

IT employs a combination of time-based and usage-based preventative maintenance.

Time-based preventative maintenance – routine inspection of critical infrastructure equipment to minimize impacts to user productivity in the event of a breakdown; deploy updates to patch security vulnerabilities and software glitches on a regular schedule

Usage-based preventative maintenance – IT equipment is cyclically replaced after a certain period to ensure up-to-date hardware is capable of handling evolving technology. Laptops are purchased with a minimum three-year warranty and are assessed every 3-4 years for replacement. Network infrastructure is assessed every five years. Equipment is typically replaced if it has reached the end-of-life support as determined by the manufacturer or is no longer operative, whichever is sooner.

Recurring Maintenance

IT has devised a recurring maintenance schedule that involves performing routine tasks at varying set intervals in the following areas:

Active Directory – IT checks and updates group policies, file shares permissions, admin passwords, inactive devices, and security groups.

Hardware – IT performs visual and hardware checks on critical infrastructure equipment such as the server, switches, firewall, backup power supply, and server room air conditioning.

Network – IT reviews logs for critical warnings and firmware/software updates within SonicWall's global management suite and Ubiquity's wireless controller software.

Office 365 – IT checks for severity issues reported by Microsoft, mailbox access by non-owners, malware detections report, Exchange and OneDrive statistics.

Security – IT checks its anti-virus admin console for updates and SonicWall's security suite logs.

Server – IT reviews server logs, backups, Domain Name Service (DNS), Redundant Array of Disks logs, and updates.

Software – IT performs pending and available updates, which include applications, operating system, and hardware firmware updates for mobile phones, tablets, and laptops.

Recurring Security Audits

Beginning in July 2021, vulnerability scans and penetration tests will be performed to check the Authority's networks and systems. Conducting a security audit is an important step toward protecting the agency against data breaches and other cybersecurity threats.

Vulnerability assessments can uncover flaws in security procedures, design, implementation or internal controls. During a vulnerability test, staff will examine and determine which system flaws are in danger of being exploited. Staff may run specific software to scan for vulnerabilities, test from inside the network or use approved remote access to determine what needs to be corrected to meet security standards. These assessments will be performed on a continuous, but no less than quarterly, basis.

Penetration testing has the same goal of identifying and evaluating security weaknesses, but is a more involved process which includes manual probing and exploitation by a security professional to simulate what a real attacker would do. This type of security audit leads to insight about potential loopholes in infrastructure. Penetration testers use the latest hacking methods to expose weak points in cloud technology, mobile platforms and operating systems. These tests will be performed semi-annually.

Backup Plan

The Authority's IT Team employs the 3-2-1 backup strategy ([Exhibit F](#)) to ensure that data is adequately protected. In essence, this backup strategy means:

- (3) having at least three copies of the data;
- (2) storing two of those copies on two different types of storage media; and
- (1) sending at least one copy of the data offsite.

The 3-2-1 backup strategy is recognized as one of the best practices for data security by information security professionals and government authorities. While the strategy does not guarantee data will never be compromised or lost, as there is no such thing as a perfect backup system, the 3-2-1 approach is a simple but effective mitigation against data loss.

Backup schedule for files on the server

Twice a day, shadow copies (Microsoft's operating system version history technology) of staff's files on the file server are made. Windows Server Backup Utility and FileSync Protocol manage the daily incremental backups of the entire file server, which occur each evening. These onsite backup copies are saved on an external hard drive and on the management PC console.

Every Saturday, a full backup of the server is created. Backups are kept on Amazon Web Services for thirty days.

Backup schedule for files on individual workstations

Staff's files stored on individual laptops are continuously uploaded to a cloud server via Backblaze. Staff also has 1TB of online cloud storage to OneDrive for Business under the Authority's Office 365 subscription.

Support Tools

To manage the volume of routine maintenance tasks and helpdesk support issues, IT mainly uses several tools on a daily basis.

RMM

Remote monitoring management (RMM) is a type of platform designed to help IT remotely and proactively monitor client endpoints such as laptops and desktops. This tool provides IT with the ability to easily maintain and update machines with the latest security patches to prevent issues from occurring.

TEAMVIEWER

TeamViewer is a remote desktop manager that allows IT to connect to computers remotely to perform maintenance or provide technical support. For example, when users need administrative permission for program installations or system updates, TeamViewer allows IT to quickly access the workstation.

MSP360 (FORMERLY CLOUDBERRY LAB)

MSP360 Explorer for Amazon S3 provides a user interface to Amazon S3 accounts allowing to access, move and manage files in the agency's cloud storage, Amazon Web Services (AWS).

STRATEGIC PLANNING 2020 – 2025

Goals and Objectives

The agency's strategic goals and objectives for technology are identified in this section of the Technology Master Plan. These goals and objectives are grouped into three categories:

RELIABILITY Provide high quality IT products and services to Authority stakeholders	INNOVATION Explore and invest in innovative ideas to help Authority staff to work efficiently and effectively	SECURITY Protect and safeguard the Authority's data and infrastructure
1. Upgrade and scale network infrastructure as necessary	1. Pilot new collaboration tools	1. Improve awareness and understanding of cybersecurity
2. Streamline daily helpdesk operations	2. Design and document IT norms	2. Enhance cybersecurity controls and tools
3. Plan for IT business continuity	3. Explore and test automation tools	3. Research and implement security best practices and policies

Within each category, the agency has identified a few potential projects (bold-faced) that will contribute to achieving the goals and objectives.

RELIABILITY

Upgrade and scale network infrastructure

The Authority's IT team understands that technology changes often. Outdated applications and equipment create network vulnerabilities that could damage or bring down office networks and operating systems.

In the next five years, IT staff plans to **upgrade a number of network equipment**:

Network Equipment	End-of-Life Date	Estimated Replacement Timeframe
UPS batteries	n/a	Dec 2022
Switches	01/18/2021	Dec 2024
Firewall	03/08/2024	Dec 2024
Management PC	n/a	Dec 2025
VoIP system	n/a	Dec 2025

UPS batteries typically last for 3-5 years, depending on several factors. One of the major factors affecting battery life is that battery can only undergo so many discharge/recharge cycles before it reaches the end of its usable life and must be replaced. The Authority does not experience a large volume of power interruptions and can attempt to maximize the useful life of the UPS batteries before procuring replacement units in 2022.

While network equipment, such as switches and firewalls, may often last up to ten years, manufacturers typically retire firmware updates and support around five years after the model is released. Therefore, it is a best practice to replace it before waiting on its failure. Planning to replace it between 5-8 years after an equipment is procured is ideal.

Additionally, IT staff must ensure that the agency's network infrastructure is scalable to accommodate staffing requirements. Based on the agency's strategic staffing forecast and resource needs assessment conducted as part of the Office Space and Resource Planning project, IT staff must be prepared to **plan a move to hosted virtualization or an expansion of the server room to scale capacity**. There is currently limited capacity to add new network devices to the network due to a minimal number of available ports on the switches. An increase in headcount may also require more phones but the current VoIP system does not have the capacity to add more handset devices, unless either an expansion module is added to the base unit or the agency considers moving to a hosted VoIP solution. Procurement of an additional switch and a VoIP expansion module may require procurement of an additional 42U rack, as there is limited rack space to mount new equipment. Depending on the staff positions hired, the current infrastructure may accommodate no more than five new personnel before the agency needs to redesign the server room configurations. IT staff will work with the Office and HR Administrator to continuously evaluate the agency's needs over the next five years.

In the absence of a current staffing forecast and resource needs assessment, all procurements, beginning with the server, will be designed and configured for with an assumption of up to 65 staff personnel.

Streamline daily helpdesk operations

To further ensure the IT team has the capacity to service up to 65 staff personnel, the IT team will be assessing processes related to technical support, routine maintenance tasks, and management of hardware and software.

Currently, staff emails the IT team for technical support and the IT team enters the ticket information and manages the status in an Excel document. This current process has several issues: (1) some emailed issues are never logged into the spreadsheet, (2) an Excel spreadsheet does not provide a way to store screenshots or conversations, and (3) solutions are not recorded afterwards. The IT team will research potential ideas, **deploy a helpdesk tracking solution**, and train staff on how to report issues.

A valuable resource will be created as a result of the helpdesk tracking solution – **a knowledgebase**. An IT knowledgebase will become a self-serve online library of information about common issues and possible solutions, all collected from the tickets created in the helpdesk tracking solution.

IT also plans to research and implement solution(s) to help streamline or **automate routine maintenance tasks**. Finally, to help the IT team better manage the ever increasing list of hardware and

software the agency procures, **a database will be created to record software subscription dates** to prevent lapses or unintended auto-renewals and hardware technical specifications, as well as the purchase, warranty, and end-of-life dates, to help establish a rotation schedule to replace obsolete hardware.

Plan for IT business continuity

An **IT business continuity/disaster recovery plan** is a documented step-by-step procedure to continue operations, and recover and protect IT infrastructure and data due to an unforeseen event. This includes conducting a thorough analysis of the existing digital setup, which includes networks, servers, desktops, laptops, wireless devices, data, and connectivity, creating a recovery team, designating a recovery location where critical backup systems can be assessed by employees, identifying IT resources required to support time-sensitive business functions and processes, and conducting a test of the plan on a regular basis.

While the high availability of network equipment and internet connectivity is important, recovered access to the agency's data is also critical. Currently, the agency has a reliable, redundant data backup plan, as previously described. But IT staff intends to research viable **failover solutions**, which involve having standby systems and networks that the agency can easily switch to if the primary infrastructures fail or is unexpectedly terminated, thereby meeting defined recovery time objectives (RTO) and minimizing downtime.

Finally, the agency currently lacks **a cloud archive of its data**. Based on the backup schedule, if a file is deleted, it will be permanently deleted from the server and the backups after thirty days. Establishing a process to archiving the agency's data will help reduce the volume of data on the file server, ensure important historical data is permanently protected, and streamline the backup process.

INNOVATION

Pilot new collaboration tools

Over the past few years, the agency's projects and initiatives have increasingly required cross-departmental collaboration. In December 2018, the Authority migrated to Microsoft Office 365, a cloud-based subscription of office productivity applications to help staff work together on documents and spreadsheets, share files, and reserve conference rooms and resources. In March 2020, the Authority launched Microsoft Teams, a chat-based collaboration platform with audio and video conferencing capabilities, to allow staff to communicate despite everyone working remotely due to the COVID-19 pandemic.

By the end of 2021, the IT team plans to **pilot SharePoint**, a web-based application included in the Office 365 subscription. The collaborative platform serves as an intranet, which is simply the agency's internal website for information sharing, task scheduling, contacts, and much more. Advantages of SharePoint

include opportunities to streamline and automate key processes, track information, manage documents, and work on group projects. Sites can be built to streamline project processes, simplifying day-to-day activities and keeping a central location for content.

For administrators, sites can be easily customized and access to the sites can be assigned to users based on different permission levels. Should the pilot's feedback be satisfactory, the IT team will proceed to produce how-to documentation, document norms, host training sessions, and create sites for the agency's departments and projects.

Design and document IT norms

As staff continues to collaborate with each other and data is created, shared, and stored, it is important for the Authority to establish an **agency-wide file naming protocol** rather than maintaining siloed naming conventions that could only be understood by departments or divisions. Being consistent with file names will allow the Authority's data to be easily managed and accessible.

In addition to file naming protocols, the IT team will **create file management protocols** compliant with the agency's records retention policy to help minimize multiple copies of draft and final versions of documents on the file server. Best practices on how to manage multiple versions of a document, as well as how to prevent editing or deletion of the final version of a document, will be provided to staff. Advocacy for storing only a single copy of a document will reduce storage costs, increase server performance, and streamline backup processes.

Explore and test automation tools

Available as part of the agency's Office 365 subscription, Power Automate is an automation software that can create time-saving workflows. **Process automation** could automate repetitive manual tasks simply by recording mouse clicks, keystrokes and copy paste steps tasks, thereby optimizing operations.

The IT team will be available as a thought partner to staff, reviewing current processes to identify bottlenecks and repetitive tasks, brainstorming improvements to the processes by incorporating the use of automation, and providing technical support in developing the workflows using Power Automate or other technologies. Potential areas for improvements include but are not limited to volunteer recruitment and event registration process, daily activity log data entry, petty cash reimbursement forms, employee onboarding, and wildlife camera photo organization.

SECURITY

Improve awareness and understanding of cybersecurity

Despite the fact that, as a public agency, most of the Authority's documents and files can be made available to the public upon request, cybersecurity still cannot be ignored or neglected. Cybersecurity risk is increasing, driven by higher usage of cloud services and reliance on technology.

The IT team proactively monitors the agency's networks and systems, but Authority staff is the true last line of defense. While the IT team has already presented for various IT topics, they intend to continue launching **a series of training sessions focused on topics related to cybersecurity**. End users will be informed about best practices, tips and tricks, and examples of common scams. IT team will also continue to publish its newsletter, TechTuesdays, on a quarterly basis to keep staff informed about the latest technological trends and threats.

The IT team believes the most relevant cybersecurity awareness training topics for staff include:

Phishing attacks	Public Wi-Fi
Removable media	Cloud Security
Passwords and Authentication	Social Media Use
Physical security	Internet and Email Use
Mobile Device Security	Social Engineering
Working Remotely	Security at Home

Enhance cybersecurity controls and tools

In addition to providing staff with the education about cybersecurity, the IT team will research and introduce controls and tools to enhance the safeguarding of the Authority's networks and data.

Password security best practices dictate that different passwords are used for different accounts, and each password at the minimum should be complex with a combination of letters, numbers, and symbols. However, this best practice is often neglected because it is difficult to remember a string of random alphanumeric characters for numerous accounts created online. The IT team plans to introduce **the use of a password manager**, a program that generates secure credentials for any site and remembers the password. End users will only have to memorize a master password, thus minimizing the number of multiple compromised accounts due to a shared passwords.

Research and implement security best practices and policies

Ransomware attacks on state and local governments are on the rise. Ransomware is a form of malicious code (or malware) that can take control and prevent access to systems or data. In 2019, at least 948 government agencies, educational establishments and healthcare providers in the United States were impacted by ransomware attacks. Since 2013, there has been more than 170 publicly acknowledged ransomware attacks aimed directly at state and local governments.

While one of the best defenses against ransomware is to maintain current and frequent backups, the IT team will extensively **research and implement additional best practices against ransomware**.

The IT team will also need to consider how to mitigate against loss of data due to loss or theft of agency-owned workstations. Mobile workstations running on Windows 10 Pro come equipped with Bitlocker drive encryption, a feature that helps protect data because it allows access only to those who have authorization. The IT team will consider **agency-wide deployment of device encryption**.

Within the Office 365 environment, the IT team will create and **implement data loss prevention policies**. As a best practice, when companies use cloud services like Office 365, it is important to have a data loss prevention solution in place. Utilizing a data loss prevention solution helps to prevent the unauthorized sharing of company information by malicious insiders and outsiders. Office 365's Data Loss Prevention (DLP) policies use rules to determine which files and data are considered confidential, critical, or sensitive and protect those files from being shared or transmitted outside the organization. Any malicious or accidental attempt to send sensitive information out of the network will be blocked and logged.

Finally, the IT team will research and implement Office 365's **email retention policies** on the Authority's Exchange Online email server. Having an email retention policy saves storage capacity on the email server, leading to better performance, and complies with record-keeping regulations. Furthermore, with the growing amount of data stored in emails, including attachments, routine archival and deletion of email records the Authority is no longer required to keep can help reduce the impact of a security breach.

Estimated Implementation Timeline

The aforementioned list of projects and process improvements are estimated to be completed within the next five years. Implementation of these projects are prioritized based on an analysis of several factors, including but not limited to staff capacity, costs and return on investment, strategic alignment, and dependencies on other projects. The estimated implementation timeline for the projects proposed are as follows:

PROJECT DESCRIPTION	YEAR				
	1	2	3	4	5
File naming conventions / File management protocols					
SharePoint					
automation improvements to programmatic processes					
IT knowledgebase					
Helpdesk tracking solution					
Business Continuity / Disaster Recovery Plan					
cloud archive solution					
software subscription database					
automate IT maintenance tasks					
upgrade network infrastructure					
password manager					
staff training on cybersecurity					
device encryption					
email retention policies					
data loss prevention policies					

Approval of Projects

Before submitting any of the aforementioned projects into the Authority's annual work plans, the IT team will reevaluate its alignment with the agency's current goals and objectives, calculate the updated costs and benefits to the agency, and submit a scope of work to Leadership for review.

Projects recommended in this Information Technology Plan may proceed upon authorization by the Board of Directors by approval of the agency's annual work plans and/or budget

GLOSSARY

Bandwidth – the volume of information per unit of time that a internet connection can handle.

Capture Advanced Threat Protection – Sonicwall’s cloud sandbox service for detecting and blocking zero-day threats before it enters a local area network.

Central Processing Unit (CPU) – the electronic circuitry within a computer that executes instructions that make up a computer program.

Content Filtering – the use of a program to screen and/or exclude access to web pages deemed objectionable.

End of Life Date – refers to a product not receiving continuing support which can include updates and/or customer support.

Fiber-Optic Communication – a method of transmitting information from one place to another by sending pulses of infrared light through an optical fiber.

Intrusion Prevention System (IPS) – a network security system designed to prevent malicious activity within a network.

Latency – the time it takes for data or a request to go from the source to the destination.

Local Area Network (LAN) – a collection of devices connected together in one physical location.

Mesh Network – an integrated set of devices that are designed to work seamlessly together to extend networks.

Modem – a telecommunication device that converts digital signals to analog and vice versa.

Operating System (OS) – a system software that manages computer hardware, software resources, and provides common services for computer applications.

Phishing – a form of fraud in which an attacker masquerades as a reputable entity or person in email or other forms of communication.

Private Branch Exchange (PBX) – allows an organization to manage incoming and outgoing phone calls, as well as internal communication using both hardware and software appliances.

Power over Ethernet (PoE) – a technology for wired ethernet LANs that allows electrical current necessary for the operation of each device to be carried over data cables rather than by power cords.

Primary Rate Interface (PRI) – a telecommunications interface standard used on a integrated services network (ISDN) for carrying multiple voice and data transmissions between the network and user.

Rack Server – a structure that is designed specifically to house technical equipment including firewalls, routers, switches and servers.

Rack Unit – a means of measurement for IT equipment. One single U space is equivalent to 1.75 inches.

Redundant Array of Inexpensive Disks (RAID) – data storage virtualization technology that combines multiple physical disk drive components into one or more logical units for the purposes of data redundancy, performance improvement, or both.

Random Access Memory (RAM) – a form of computer memory that can be read and change in any order, typically used to store working data and machine code.

Recovery Time Objective (RTO) – the targeted duration of time between the event of failure and the point where operations resume.

Social Engineering – the psychological manipulation of people into performing actions or divulging confidential information.

Switch – networking hardware that connects devices on a network by using packet switching to receive and forward data to the destination device.

Throughput – throughput refers to how much data can be transferred from source to destination within a given timeframe.

Uninterrupted Power Supply (UPS) – an electrical apparatus that provides emergency power to a load when the input power source fails.

Virtualization – refers to the act of creating a virtual version of something, including virtual computer hardware platforms, storage devices, and computer network resources.

Virtual Local Area Network (VLAN) – a logical subnetwork that groups a collection of devices from different physical LANs.

Virtual Private Network (VPN) – a technology that uses a public network, such as the internet, to transmit encrypted data between a private network and a remote authorized user.

Voice over Internet Protocol (VoIP) – a method and group of technologies for the delivery of voice communications over Internet Protocol (IP) networks.

EXHIBIT A

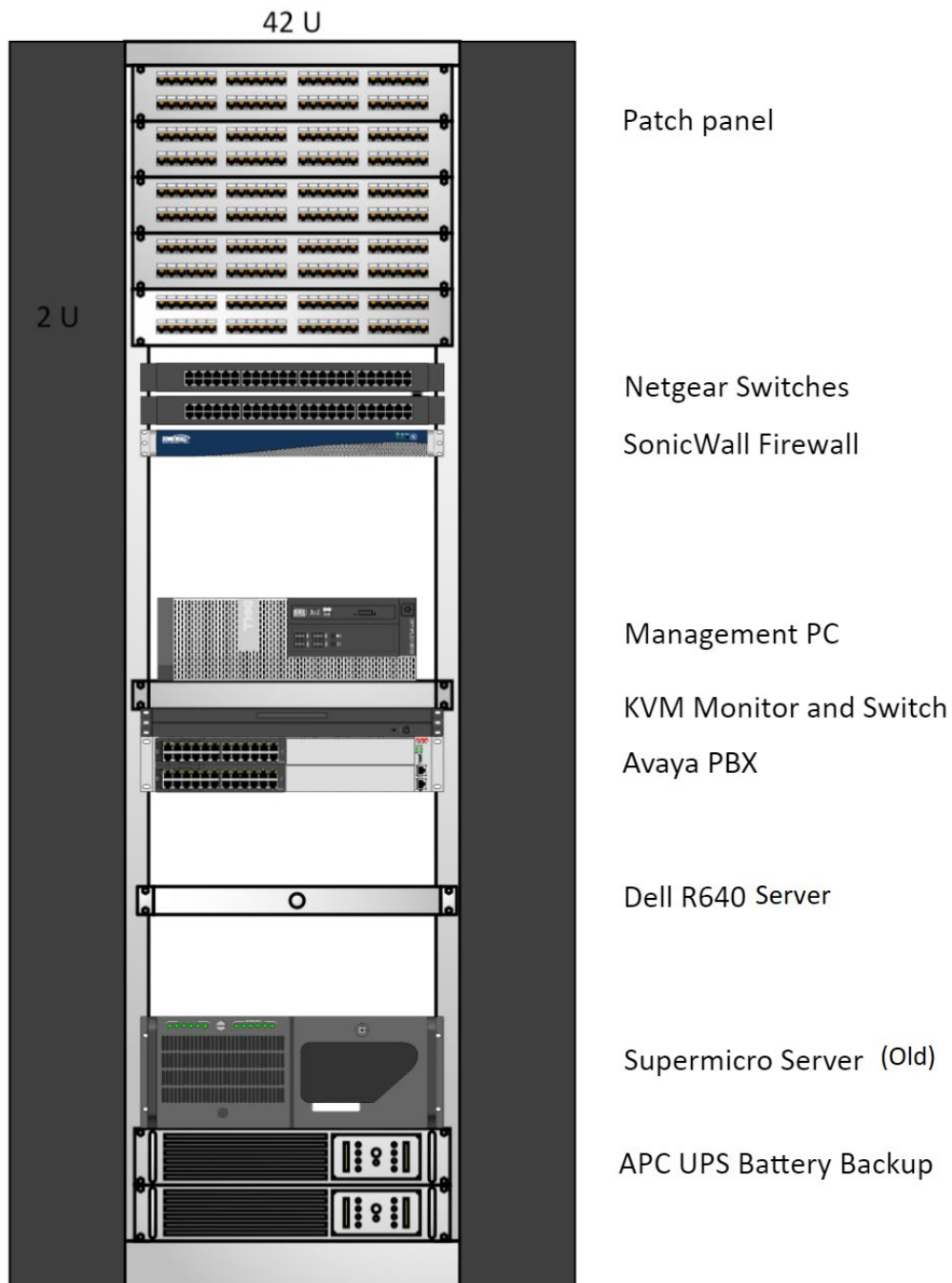
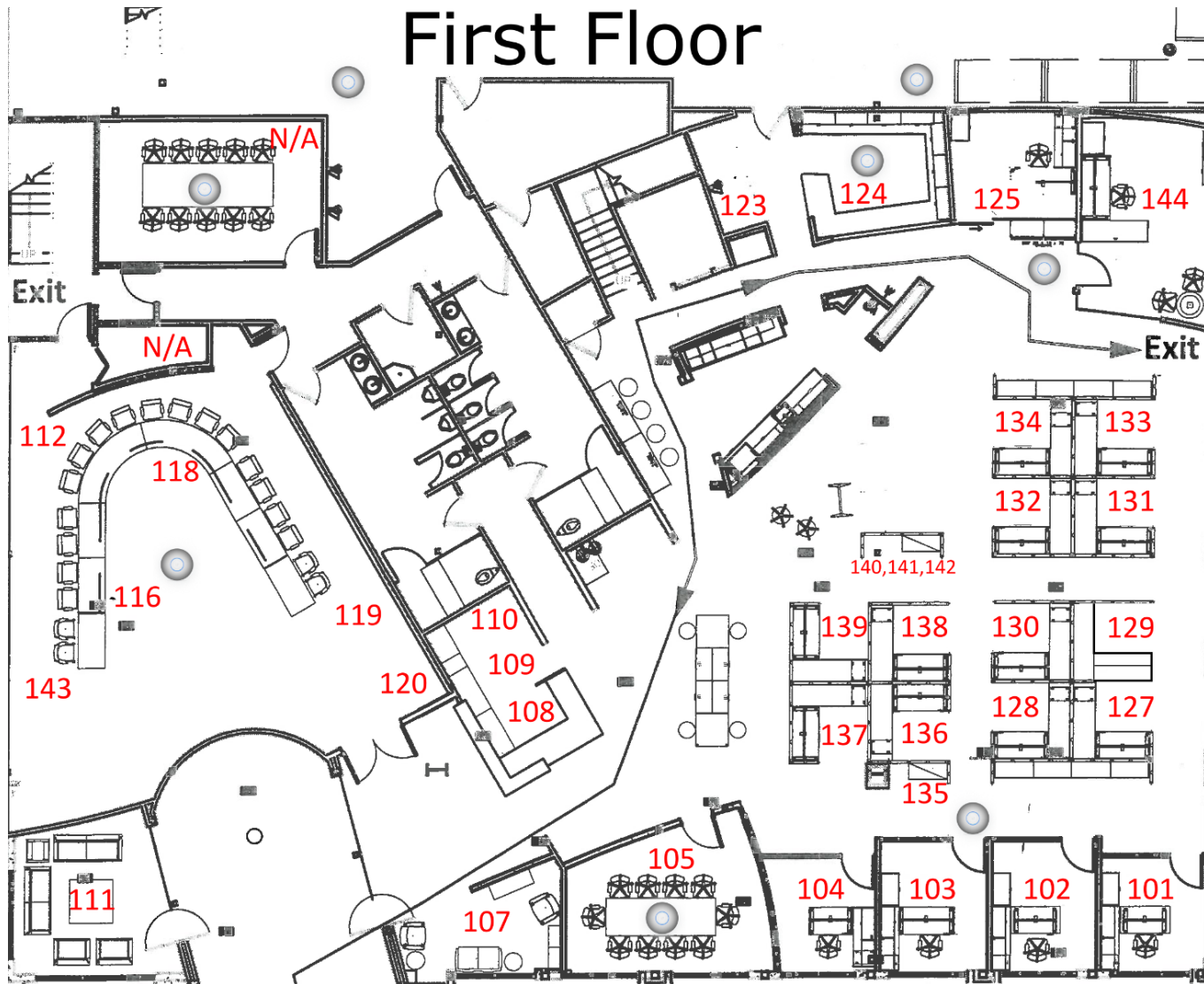


EXHIBIT B

First Floor



Second Floor

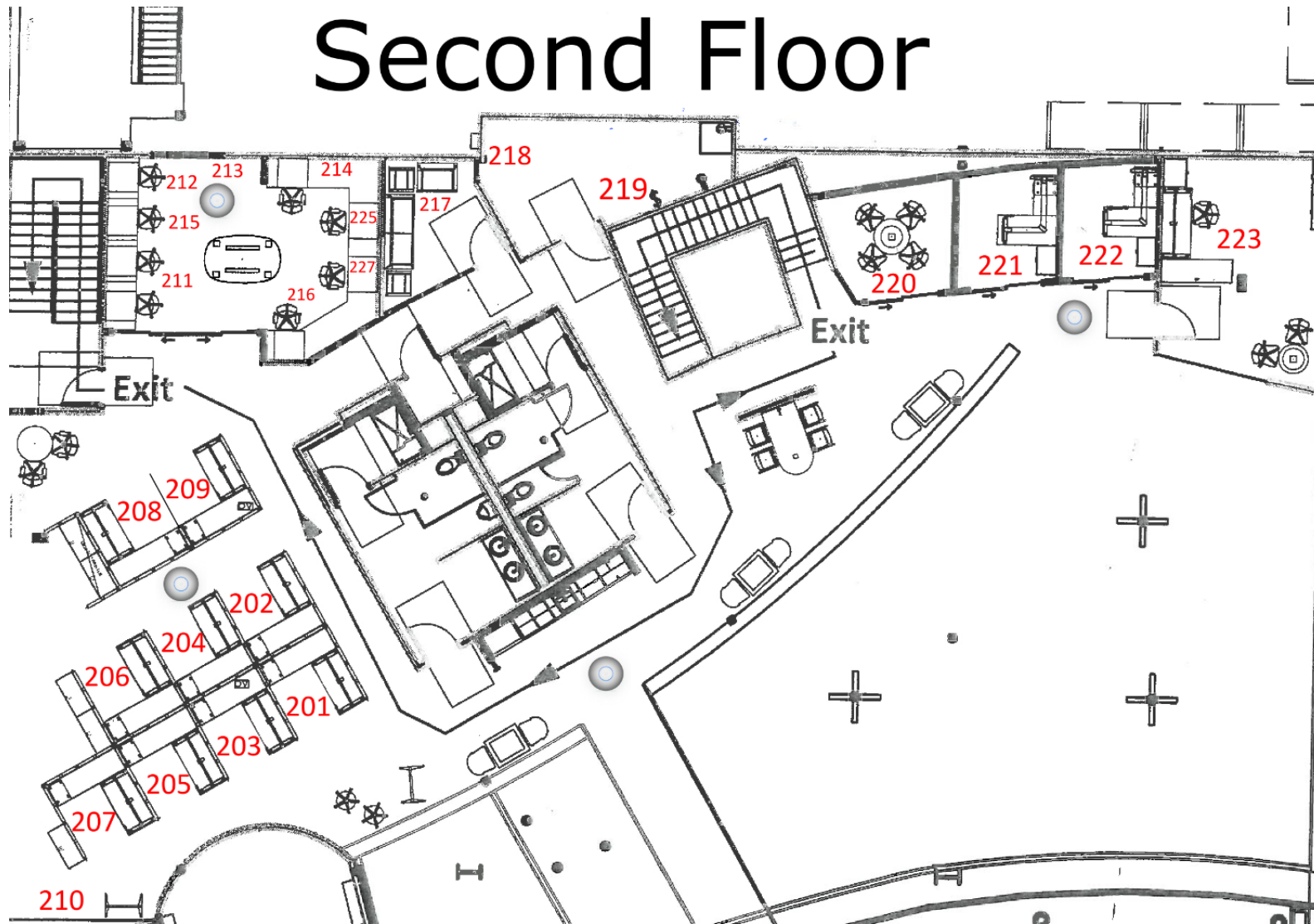


EXHIBIT C

UAP-AC-PRO Specifications

UAP-AC-PRO	
Dimensions	196.7 x 196.7 x 35 mm (7.74 x 7.74 x 1.38")
Weight	350 g (12.4 oz)
With Mounting Kits	450 g (15.9 oz)
Networking Interface	(2) 10/100/1000 Ethernet Ports
Port	(1) USB 2.0 Port
Buttons	Reset
Power Method	Passive Power over Ethernet (48V), 802.3af/802.3at Supported (Supported Voltage Range: 44 to 57VDC)
Power Supply	48V, 0.5A PoE Gigabit Adapter*
Power Save	Supported
Maximum Power Consumption	9W
Maximum TX Power	
2.4 GHz	22 dBm
5 GHz	22 dBm
Antennas	(3) Dual-Band Antennas, 2.4 GHz: 3 dBi, 5 GHz: 3 dBi
Wi-Fi Standards	802.11 a/b/g/n/ac
Wireless Security	WEP, WPA-PSK, WPA-Enterprise (WPA/WPA2, TKIP/AES)
BSSID	Up to Four per Radio
Mounting	Wall/Ceiling (Kits Included)
Operating Temperature	-10 to 70° C (14 to 158° F)
Operating Humidity	5 to 95% Noncondensing
Certifications	CE, FCC, IC

* Only the single-pack of the UAP-AC-PRO includes a PoE adapter.

Advanced Traffic Management	
VLAN	802.1Q
Advanced QoS	Per-User Rate Limiting
Guest Traffic Isolation	Supported
WMM	Voice, Video, Best Effort, and Background
Concurrent Clients	250+

Supported Data Rates (Mbps)	
Standard	Data Rates
802.11ac	6.5 Mbps to 1300 Mbps (MCS0 - MCS9 NSS1/2/3, VHT 20/40/80)
802.11n	6.5 Mbps to 450 Mbps (MCS0 - MCS23, HT 20/40)
802.11a	6, 9, 12, 18, 24, 36, 48, 54 Mbps
802.11g	6, 9, 12, 18, 24, 36, 48, 54 Mbps
802.11b	1, 2, 5.5, 11 Mbps

DATASHEET

UniFi

EXHIBIT D

NSA Series system specifications

	NSA 2600	NSA 3600	NSA 4600	NSA 5600	NSA 6600
Operating system	SonicOS 6.1				
Security cores	4	6	8	10	24
10 GbE interfaces	—	2 x 10-GbE SFP+			4 x 10-GbE SFP+
1 GbE interfaces	8 x 1 GbE	4 x 1-GbE SFP, 12 x 1 GbE			8 x 1-GbE SFP, 8 x 1 GbE (1 LAN Bypass pair)
Management interfaces	1 GbE, 1 Console				
Memory (RAM)	2.0 GB			4.0 GB	
Expansion	1 Expansion Slot (Rear)*, SD Card*				
Firewall inspection throughput ¹	1.9 Gbps	3.4 Gbps	6.0 Gbps	9.0 Gbps	12.0 Gbps
Full DPI throughput ²	300 Mbps	500 Mbps	800 Mbps	1.6 Gbps	3.0 Gbps
Application inspection throughput ²	700 Mbps	1.1 Gbps	2.0 Gbps	3.0 Gbps	4.5 Gbps
IPS throughput ²	700 Mbps	1.1 Gbps	2.0 Gbps	3.0 Gbps	4.5 Gbps
Anti-malware inspection throughput ²	400 Mbps	600 Mbps	1.1 Gbps	1.7 Gbps	3.0 Gbps
IMIX throughput ²	600 Mbps	900 Mbps	1.6 Gbps	2.4 Gbps	3.5 Gbps
SSL Inspection and Decryption (DPI SSL) ²	200 Mbps	300 Mbps	500 Mbps	800 Mbps	1.3 Gbps
VPN throughput ³	1.1 Gbps	1.5 Gbps	3.0 Gbps	4.5 Gbps	5.0 Gbps
Connections per second	15,000/sec	20,000/sec	40,000/sec	60,000/sec	90,000/sec
Maximum connections (SPI)	225,000	325,000	400,000	750,000	750,000
Maximum connections (DPI)	125,000	175,000	200,000	500,000	500,000
SonicPoints supported (Maximum)	32	48	64	96	96
Single Sign On (SSO) Users	250	500	1,000	2,500	4,000
VPN	NSA 2600	NSA 3600	NSA 4600	NSA 5600	NSA 6600
Site-to-site tunnels	75	800	1,500	4,000	6,000
IPSec VPN clients (Maximum)	10 (250)	50 (1,000)	500 (3,000)	2,000 (4,000)	2,000 (6,000)
SSL VPN licenses (Maximum)	2 (25)	2 (30)	2 (30)	2 (50)	2 (50)
Encryption/Authentication	DES, 3DES, AES (128, 192, 256-bit)/MD5, SHA-1				
Key exchange	Diffie Hellman Groups 1, 2, 5, 14				
Route-based VPN	RIP, OSPF				
Networking	NSA 2600	NSA 3600	NSA 4600	NSA 5600	NSA 6600
IP address assignment	Static (DHCP PPPoE, L2TP and PPTP client), Internal DHCP server, DHCP Relay				
NAT modes	1:1, many:1, 1:many, flexible NAT (overlapping IPS), PAT, transparent mode				
VLAN interfaces	50	50	200	400	500
Routing protocols	BGP, OSPF, RIPv1/v2, static routes, policy-based routing, multicast				
QoS	Bandwidth priority, max bandwidth, guaranteed bandwidth, DSCP marking, 802.1p				
Authentication	XAUTH/RADIUS, Active Directory, SSO, LDAP, Novell, internal user database, Terminal Services, Citrix				
VoIP	Full H323-v1-5, SIP				
Standards	TCP/IP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3				
Certifications	VPNC, ICSA Firewall, ICSA Anti-Virus				
Certifications pending	FIPS 140-2, Common Criteria EAL1+				
Common Access Card (CAC)	Pending				
Hardware	NSA 2600	NSA 3600	NSA 4600	NSA 5600	NSA 6600
Power supply	200W	Single, Fixed 250W			Dual, redundant, hot swappable
Fans	Dual, Fixed				
Input power	100-240 VAC, 60-50 Hz				
Maximum power consumption (W)	49.4	74.3	86.7	90.9	113.1
Form factor	1U Rack Mountable				
Dimensions	1.75 x 10.25 x 17 in (4.5 x 26 x 43 cm)	1.75 x 19.1 x 17 in (4.5 x 48.5 x 43 cm)			
Weight	10.1 lb (4.6 kg)	13.56 lb (6.15 kg)			14.93 lb (6.77 kg)
WEEE weight	11.0 lb (5.0 kg)	14.24 lb (6.46 kg)			19.78 lb (8.97 kg)
Shipping weight	14.3 lb (6.5 kg)	20.79 lb (9.43 kg)			26.12 lb (11.85 kg)
Major regulatory	FCC Class A, CE (EMC, LVD, RoHS), C-Tick, VCCI Class A, MSIR/KCC Class A, UL, cUL, TUV/GS, CB, Mexico CoC by UL, WEEE, REACH, ANATEL, BSMI, CU				
Environment	32-105 F, 0-40 deg C				
Humidity	10-90% non-condensing				
MTBF (Years)	20.2	16.8	16.0	15.4	13.3

¹ Testing Methodologies: Maximum performance based on RFC 2544 (for firewall). Actual performance may vary depending on network conditions and activated services. ² Full DPI/ Gateway/Anti-Spyware/IPS throughput measured using industry standard Spirent Webflow/lanche HTTP performance test and iis test tools. Testing done with multiple flows through multiple port pairs.

³ VPN throughput measured using UDP traffic at 1280 byte packet size adhering to RFC 2544. All specifications, features and availability are subject to change. *Future use.

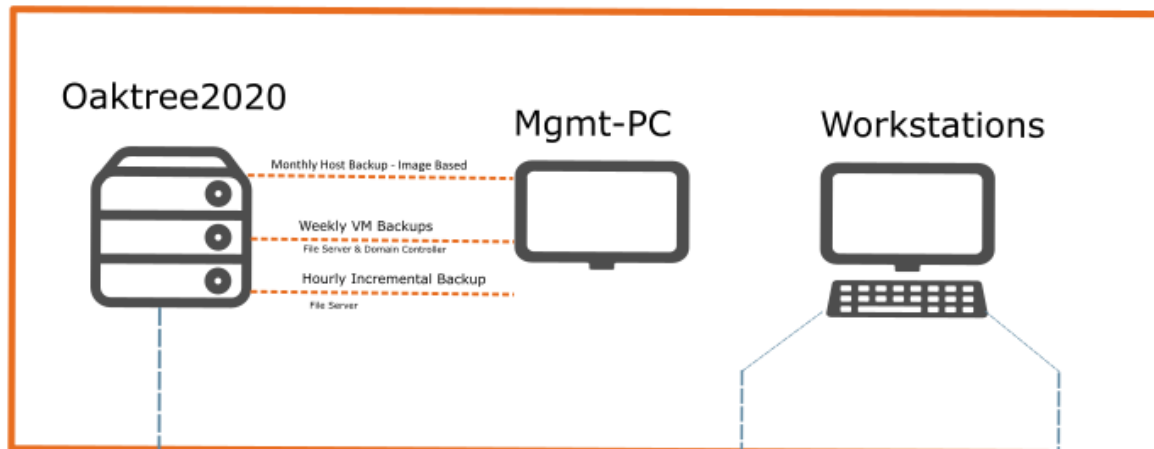


EXHIBIT E

ProSafe® 24- and 48-port Gigabit Stackable Smart Switches		GS728TS, GS728TPS, GS752TS and GS752TPS	
Manageability and Support		<p>There are various easy and convenient ways to manage the Stackable Smart Switch. The new Stackable Smart Switches can be managed by the Smart Control Center software which comes free with the switch. With it, you can discover and manage all NETGEAR Smart Switches from a central location, conduct mass configuration and firmware upgrade. If you have other NETGEAR business products in your network, you can also use the NMS200, NETGEAR's management platform for discovery and configuration of all your NETGEAR products in the network. For peace of mind, these Stackable Smart Switches are backed by the NETGEAR ProSafe Lifetime Hardware Warranty and 1-year 24x7 Advanced Technical Support*.</p>	
Technical Specifications			
• Network Protocol and Standards Compatibility <ul style="list-style-type: none"> – IEEE® 802.3 10BASE-T – IEEE 802.3u 100BASE-TX – IEEE 802.3ab 1000BASE-T – IEEE 802.3z 1000BASE-X – IEEE 802.3x full-duplex flow control – IEEE 802.3az (EEE) – IEEE 802.3af (DTE Power via MDI) – IEEE 802.3at (DTE Power via MDI Enhancements) 		<ul style="list-style-type: none"> – IEEE 802.3ad Static or Dynamic Link Aggregation (LACP) – IEEE 802.1D Spanning Tree Protocol – IEEE 802.1w Rapid Spanning Tree Protocol – IEEE 802.1s Multiple Spanning Tree Protocol – SNMP v1, v2c, v3 – RFC 1213 MIB II – RFC 1643 Ethernet Interface MIB – RFC 1493 Bridge MIB – RFC 2131 DHCP client – IEEE 802.1x (RADIUS) – RADIUS accounting – IEEE 802.1x Dynamic VLAN Assignment – HTTPS/SSL: Secure HTTP GUI – Layer 3 (DSCP) Quality of Service (QoS) – TACACS+ – Port-based security by locked MAC addresses – TCP/UDP-based priority mapping – IGMP snooping v1, v2, v3 – MLD snooping – ACLs (MAC, IPv4, IPv6 and TCP/UDP based) – Storm control for broadcast, multicast and unknown unicast packets – Port-based ingress/egress rate limiting – SNMP – DNS – DoS and Auto DoS prevention – IPv6 management, multicast and QoS – Static Routing – DHCP snooping – Green Features: <ul style="list-style-type: none"> • EEE (Energy Efficient Ethernet) compliance • Lower power consumption during link-down or idle mode or with shorter cable length – Protocol and MAC-based VLAN – RMON group 1, 2, 3, 9 – Private Enterprise MIB – Port mirroring – many-to-one – IEEE 802.3ab LLDP 	
• Interfaces <ul style="list-style-type: none"> – GS728TS/GS752TS <ul style="list-style-type: none"> • 24/48 x 10/100/1000 Mbps copper ports • 2 x Combo ports to support 10/100/1000 Mbps copper ports or 1 G/100 M optical module • 2 x SFP slots (port 25 and 26) to support 1 G optical module • 2 x SFP slots (port 27 and 28) to support 1 G optical module (uplink) and 2.5 G stacking (via stacking cable AGC761) – GS728TPS/GS752TPS <ul style="list-style-type: none"> • 24/48 PoE-capable 10/100/1000 Mbps copper ports (8 PoE+ capable) • 2 x Combo ports to support 10/100/1000 Mbps copper ports or 1 G/100 M optical module • 2 x SFP slots (port 49 and 50) to support 1 G optical module • 2 x SFP slots (port 51 and 52) to support 1 G optical module (uplink) and 2.5 G stacking (via stacking cable AGC761) – Auto-sensing and auto-negotiating capabilities for all copper ports – Auto Uplink™ on all ports to make the right connection 		<ul style="list-style-type: none"> – LLDP-MED – Protected ports – Cable test – Smart Control Center discovery – Web-based configuration – Configuration backup/restore – Password access control – Firmware upgradeable 	
• Administrative Switch Management <ul style="list-style-type: none"> – IEEE 8021.Q VLAN (256 groups, Static) – IEEE 802.1p Class of Service (CoS) – 8 hardware queues (1 is reserved for CPU; 7 queues are user configurable) – Port-based QoS 		• Performance Specifications <ul style="list-style-type: none"> – Forwarding modes: Store-and-forward – Bandwidth (per unit): 56 Gbps for GS728TS/TPS, 104 Gbps for GS752TS/TPS – Stacking up to 6 switches or 300 ports per stack – Mix and match stacking supported on the GS7xxTS/GS7xxTPS family (GS728TS, GS752TS, GS728TPS and GS752TPS) – Stacking bandwidth: 5 Gbps (bidirectional) – Network latency: Less than 20 microseconds for 64-byte frames in store-and-forward mode for 1000 – Mbps to 1000 Mbps transmission – Buffer memory: 2 MB – 128 Mbytes System DDR SDRAM (32Mbx16) – 32 Mbytes flash size – Address database size: 16 K media access control (MAC) addresses per system – Addressing: 48-bit MAC address – Number of VLANs: 256; Maximum VLAN ID: 4093 – Number of 802.1p traffic classes: 7 – Number of LAGs: 8 – Number of static routes: 32 – Number of routed VLANs: 15 – Number of ARP Cache entries size: 1024 – Queues used for DiffServ: 7 – Number of ACLs (IPv4/IPv6): 100 – Number of DHCP snooping binding: 8K – Number of DHCP static entries: 1024 – Mean time between failures (MTBF): <ul style="list-style-type: none"> • GS728TS <ul style="list-style-type: none"> - 595,423 hours (~68.9 years) at 25°C - 174,070 hours (~20.1 years) at 55°C 	

EXHIBIT F

Onsite



Cloud

