3.4 Generators

- County provided.

4.0 Database Systems

Database systems are computer software applications that interact with the user, other applications, and the database itself to store, capture, and analyze data. Database systems are designed to allow the definition, creation, querying, update, and administration of data. The County uses database systems to manage and analyze a high volume of information.

4.1 High Availability

- Databases must be able to run in an enterprise clustered environment.
- Must support high availability.
- Databases must have built in backup and recovery capabilities

4.2 Oracle

- Oracle 12c
- Enterprise Edition
- Applications connecting to Oracle must use Oracle client 11.2.0.4 minimum.

4.3 MS SQL Server

- SQL Server 2016

5.0 Desktop

Desktop provides technical support, including application, equipment and system support, to all County users.

5.1 Encryption

- All endpoint devices (laptops, phones, tablets) must encrypt local storage with FIPS-140 compliant algorithms
- Windows 10 Devices – Microsoft Bitlocker
- IOS/Android – Native encryption on device
- Systems and Storage – Encryption at volume or hardware disk level – storage system native encryption.

5.2 Laptop

- Lenovo ThinkPad (free), Panasonic Toughbook 16GB (vehicle mounted)
- Intel i5-6300U Processor, 2.4GHz
- 8GB DDR4 RAM minimum
- 180GB SSD minimum
- Wireless 802.11ac/a/b/g/n

- Lenovo: 14” or 15" Non-Touch Anti-Glare WLED LCD
- Panasonic: 13.1” Touchscreen Anti-Glare LED LCD
- Panasonic: Integrated 4G LTE mobile broadband
- Warranty 3yr next day onsite, 7x24 Tech Support

5.3 Desktop

- Intel i5-6500T Processor
- 8GB DDR4 RAM minimum
- 256GB SSD minimum
- Integrated Intel Gigabit Ethernet
  23.8in LCD, 1920 x1080, DipslayPort and HDMI
- Warranty 3yr next day onsite, 7x24 Tech Support

5.4 PC Operating Systems

- Windows 10 Enterprise 64 bit – with annual feature updates (current production ver-1709)
- Baseline security model – DISA STIG
- Standard Account Rights – User only

5.5 Software

- Microsoft Office 2016 (Windows 10 PCs)
- Microsoft Internet Explorer 11
- Microsoft Windows Defender AV
- Software depending on third party applications (Java, Flash, Etc.) must be on currently compliant, and supported versions from the aforementioned third party vendors.

5.6 Printers

- Desktop Use – HP LaserJet Pro 400 with Ethernet 10/100/1000 Network, USB 2.0
  Mobile Use – Brother PocketJet 6 Series

5.7 Service Desk

- Cherwell

6.0 Email

Email is a method of exchanging digital messages from an author to one or more recipients, operating across the Internet or a computer network. The County uses email as the primary form of communication between County employees, vendors and other entities. Email is also used to correspond with constituents.

6.1 Internal Mail Delivery

- Proprietary/SOAP API – Exchange 2016 SP1/Outlook 2016 and O365 online.
- Attachment limit is 25MB

6.2 Simple Mail Transfer Protocol (SMTP) Relay

- RFC821 SMTP – Microsoft SMTP

6.3 External Mail Delivery

- RFC821 SMTP w/TLS Encryption optional –7.0 Encryption

Encryption is the conversion of data into a form or code that cannot be easily understood by unauthorized people. The County uses various encryption methods to protect sensitive and valuable data. Encryption must use a FIPS 140-2 validated encryption algorithm.

7.0 Encryption

7.1 Data in Transport

- All applications must use HTTPS
    - NOTE: This includes data channels as well as authentication channels.
- External mail delivery supports opportunistic SMTP TLS

7.2 Data at Rest

- Laptop hard disks must be encrypted using PGP (Windows 7) or Microsoft Bitlocker (Windows 10) whole disk encryption software.

8.0 Facility Security

Facility security is important for the protection of County employees, constituents and the sensitive information kept in County buildings.

8.1 Card access

- Systems must be Lenel and integrated into County Enterprise Lenel System

8.2 CCTV systems

- Systems must consist of Hitachi SmartCAM600, ExacqVision NVR with Hanwha Techwin, Axis, and or Arecont IP Cameras

9.0 Internet Access

Internet access connects individual computer terminals, computers, mobile devices, and computer networks to the Internet, enabling users to access Internet services, such as email. Internet access is important for daily County business function.

9.1 Browser Based

- Via HTTP Proxy Server – browser configured with a proxy pac file.

9.2 Internal Applications

- Explicit Forward HTTP Proxy Server
- Applications needing internet access must be coded to support access behind a proxy server.
- Applications requiring direct internet access will be configured with specific access requirements and tracked via firewall logging

9.3 DMZ Applications

- Direct access to the Internet via NAT

9.4 Mobile Devices (Non-County)

- Public WIFI/Carrier – Open

9.5 Mobile Devices (County Owned)

- WIFI Protected Access (WPA2) WIFI/Carrier – WIFI allows access to internal resources.

9.6 File Transfer Protocol (FTP) Access

- FTP Proxy Server – Secure FTP (SFTP, SCP) for external access

10.0 Mobile Systems

Mobile technology enables workers to perform their duties not only in the field but also while away from their desks.

10.1 Mobile Applications

- Based Application developed for mobile devices. Refer to Sections 1.0 and 17.0.

10.2 Mobile Devices

- iOS devices supported by Apple/S.A.F.E. Android devices currently support by Samsung.
- Devices are Configured and Enrolled with Mobile Device Management Software.
- Devices are Passcode enabled, minimum 6 digits.
- Devices use Enterprise WIFI, WAP2 or higher encryption.

11.0 Network Systems

The network allows for computers and devices to exchange data along network links while supporting internet access and applications.

11.1 Wireless

- Cisco Enterprise Wireless Controllers with LWAPP using various Cisco WAP modules.
- All equipment operates using the recommended software maintenance release by Cisco systems and is upgraded regularly.

11.2 Voice over Internet Protocol (VoIP) and VLAN Trunking Protocol (VTP)

- Cisco Call Manage, Unity and Emergency Responder are the products used in the BCG environment.
- Verizon SIP trunks are the current transport to the PSTN.
- G7.11 and g7.29 are currently supported audio codec.
- Standard Call signaling protocol used by BCG is SIP.
- VOIP and Telepresence communications using public internet connectivity are required to use Secure SIP and firewall traversal methods that protect the internal network.

11.3 Demilitarized Zone (DMZ)

- Is required to have firewall and security protection for all network edges

11.4 Baltimore County Optical Network (BCON)

- BCON established naming conventions are to be applied to all new devices and segments

11.5 Vlan Trunking Protocol (VTP)

- Only utilized in specific networks to decrease administrative effort:
  - Towson Campus
  - PSB building
  - DCG building
- If VTP trunking is enabled elsewhere, convert the site to use manual vlan configuration.

12.0 Radio Systems and Microwave

Radio systems are comprised of interconnected radio transmitters and receivers at fixed locations that are controlled by computer software applications. These radio transmitters and receivers provide communications for police, fire and public works personnel while using motor vehicles and handheld portable units for countywide communications. Communications take place between units in the field and dispatch operations, at the 911 Center, or other fixed dispatch locations or from subscriber to subscriber. Microwave radios connect the fixed components to ensure uninterrupted communications that are not reliant on the public switched network or the internet.

12.1 Radio Systems

- Subscriber Units
    - XTS5000
    - XTS2500
    - XTS1500
    - XTL5000
    - XTL2500
    - XTL1500
    - APX8500
    - APX8000
    - APX7000
    - APX6000
    - APX1000
    - APX7500
    - APX6500
    - APX1500
- Project 25 Digital Simulcast Radio System
- Project 25 Compatible Subscriber Units
- Encryption- AES

12.2 Mobile Data Systems

- Modem Panasonic Laptop, CF31, CF33, CF19, CF20, CF54

12.3 Microwave

- Microwave Networks- Proteus M & MX (3-DS3) 6 & 11 GHz Licensed DC Power – 48 volt DC

13.0 Remote Access

Remote access is the ability to log onto a network from a distant location. Generally, this implies a computer, Internet connection and remote access software to connect to the network. The County uses remote access to allow employees to work from various remote sites and also telecommute.

13.1 Mobile Agencies

- Net motion – Police, Fire, Public Works, etc.

13.2 Virtual Private Network (VPN)

- Cisco Any-connect VPN access being available to OIT and authorized individuals only.

13.3 Citrix

- Provides remote access to applications and systems.
- Includes public access to applications/systems.

13.4 Microsoft Direct Access

- Available on County Windows 10 devices only – not for use on employee owned device
- Provides 'always-on' connection to County network
- Ensure web browsing and email connect through County proxy servers
- Computer functions nearly as if on local County network
- Access available on properly configured County Windows 10 devices

13.5 Bomgar Privileged Access Management (PAM) – Vendor Remote Access

- Session Management
- Session Recording
- Password Management for Vendor Accounts

14.0 Server Systems

A server is a software program, or the computer on which that program runs, that provides a specific kind of service to client software running on the same computer or other computers on a network. Servers are computer programs running to serve the requests of other programs, the clients.

14.1 Application Server OS

- Windows Server 2019
- VMware 6.7
- SLES 12x 64bit, SLES 15, RHEL7 also supported – Intel-based Server Operating

14.2 Server Hardware

- HP ProLiant BL Blades – C class or higher

14.3 Virtual Platforms

- VMWare ESX(i) 6.5
- Microsoft Hyper-V 2016

- Intel-based Server Partitioning

14.4 Web Servers

- IIS 10 , Microsoft Internet Information Server
- Apache Tomcat

14.5 Oracle Database Appliance (ODA)

- Oracle Linux

15.0 Enterprise Monitoring

Monitoring is the practice of proactively and constantly monitoring all aspects of daily internal and customer-facing Information Technology activity. Monitoring is used to detect components that have fallen out of standard threshold ranges due to fault or normal operation in real-time.

15.1 Data Collection Methods

- Simple Network Monitoring Protocol (SNMP) - SNMP Version 2 standard for read only. Version 3 standard for write access and when added security is needed.
- SNMP Strings- 8 characters, 1 capital, 1 number minimum, unique by geography or device functionality. Disable default strings (public and private).
- Windows Management Instrumentation (WMI) - Windows Devices Only. At discretion based on monitoring requirements
- ICMP- Up/Down Only
- SolarWinds Orion Agent- Deep-Metrics needed or complicated network locations. At discretion based on monitoring requirements

15.2 Network / Systems / Application Performance Management

15.2.1 - Custom Property

- Custom Metadata/Attributes for Applications, Groups, Interfaces, Alerts, Reports, Nodes, Volumes, Recordings or Transactions
- Allows for detailed information sharing across teams while retaining data in an extra table format
- Overlaps with other system's information but is not automatically linked

15.2.2 - Network Device Discovery

- Pre-Selected Network Segments
- Automatic, Weekly on Sundays

15.2.3 - Network Device Polling

- See Above 15.2.1

15.2.4 - Application Polling

- Polled Per Application Template
- Critical Processes, Services, Ports, Queues, or other Custom Performance Counters the yield specific data that contribute to accurate application health.

15.2.5 - Critical Network Paths

- Polled per path
- On-or-Off-Premises network paths that lead to critically hosted application or device services.

15.2.6 - WAN Performance Metering

- Cisco IP SLAs to gauge traffic performance across sites

15.2.7 - VoIP Gateway, PRI & SIP Trunk Performance Monitoring

- Up/Down, Audio/Video Quality, Activity & Availability

15.2.8 - Dynamic Baselines

- Automated Data collection based on 7 days of activity
- Updated on-demand

15.2.9 - Availability Statistics

- Automatically collected and displayed in dashboard views
- Available via reporting platform

15.2.10 - Dependency Groups

- Manual Group Creation based on User-facing application or supportive system or platform
- Utilized in overall environment health and targeted alert generation

15.2.11 - Alerting

- Actionable alerts with configurable trigger action on critical systems
- Created on-demand by request
- Documented in Orion

15.2.12 - Topology & Relationship Mapping

- Automatically collected and displayed in dashboard views

15.2.13 - Storage Capacity & Performance

- Automatically collected and displayed in dashboard views
- Available via reporting platform

15.2.14 - Asset Inventory Collection

- Automatically collected and displayed in dashboard views

- Available via reporting platform

15.2.15 - Virtualization Capacity & Predictive Recommendations

- What-If models yield possible performance & resource utilization across CPU, memory, network and storage platforms.

15.2.16 - Web Site Performance

- Deployed on-demand for high-visibility sites
- Provides performance changes, waterfall-charting, synthetic-user activity
- Available from multiple site locations for wide testing

15.3 Networking Monitoring Platform – SolarWinds Orion Modules

Orion Platform
Network Performance Monitor
Server & Application Monitor
Virtualization Manager
VoIP & Network Quality
Web Performance Monitor
Network Configuration Manager
NetPath
Quality of Experience
Cloud Monitoring

15.4 Network Operations Center (NOC) Video Wall Controller

- 6-Display Visualization System

16.0 Storage Systems Access

Computer users, systems & applications need to access and share files across the network.

- CIFS/ Network File System (NFS) /Raw LUN – NETAPP

17.0 Web Development

Web development can range from developing the simplest static single page of plain text to the most complex web-based internet applications, electronic businesses and social network services. Web development includes tasks such as web design, web content development, client liaison, programming, web server and network security configuration and application development.

The County engages in web development with the purpose of providing valuable information and services to constituents and employees in a convenient and efficient way. The public and internal websites and applications are examples of how the County engages in web development.

17.1 Hypertext Markup Language (HTML)

- HTML 4.01
- HTML 5

17.2 Cascading Style Sheets (CSS)

- CSS 2.1
- CSS 3

17.3 JavaScript

- Standard ECMA-262

17.4 Graphics

- JPEG – Photographs or graphics with most complexity (gradients, shadows)
- GIF – Basic, non-photographic use
- PNG – 24 – Images, transparency

17.5 Responsive Design

- Must be used when designing websites: HTML and CSS
    - Fluid grids and images
- Responsive design responds to the user's behavior and environment based on screen size, platform and orientation.

17.6 Audio/Video

- Always provide alternatives for time-based media, such as captions, descriptions or sign language.

- Audio and video are used for enhancing the experience with Web pages to serving music, videos, presentations, etc.

17.7 Accessibility

The Web is fundamentally designed to work for all people, whatever their hardware, software, language, culture, location, or physical or mental ability. When the Web meets this goal, it is accessible to people with a diverse range of hearing, movement, sight and cognitive ability.

- Web content must comply with Section 508 of the Rehabilitation Act of 1973.
- Web applications must meet Accessible Section 508 Compliance of the Rehabilitation Act of 1973.
    - Vendors must provide a Voluntary Product Accessibility Template (VPAT) documenting their product's compliance with Section 508.
    - WCAG 2.0
    - Documentation of Section 508 compliance for In- House applications is on file at the Office of Information Technology.

17.8 Writing & Design Standards

Baltimore County follows the "Associated Press" standard writing guide (https://www.ap.org/en-us/) and also provides their own supplemental writing guide for all County internet and intranet websites. A design guide is also supplied for the County flagship website, www.baltimorecountymd.gov.

- Writing Guide - https://www.baltimorecountymd.gov/styleguide/writing/index.html
- Design Guide - https://www.baltimorecountymd.gov/styleguide/design/index.htmlhttps://www.baltimorecountymd.gov/styleguide/design/index.htmlhttps://www.baltimorecountymd.gov/styleguide/design/index.htmlhttps://www.baltimorecountymd.gov/styleguide/design/index.html

18.0 VTC

Video Teleconferencing allows employees to make audio/video calls, with the ability to share the screen of a connected PC as well as WebEx conference audio/video calls.

18.1 VTC OS

- Cisco CE IOS

18.2 VTC Hardware

- Cisco room and desktop endpoints. Room Endpoints typically use a Touch 10 control panel, rather than a remote.
- Connections to TVs/Projectors/PCs are HDMI.

18.3 VTC PC Software

- Cisco Jabber

18.4 VTC Communication Protocols

- Endpoint is setup with the SIP protocol only.
- H.323 calls (inbound/outbound) are managed by Cisco Expressway Servers allowing calls both within and outside the organization.

18.5 VTC Registration and Management

- Systems are registered to on premises Cisco Unified Call Manager (CUCM) for Call control.
- Systems are managed by on premises Cisco Telepresence Management Suite (TMS) and WebEx.

Revisions

Initial Draft	7/1/2013	Keith Asante
Revision 1	11/1/2014	Heather List/Samantha Marston
Revision 2	7/30/2015	Jeremy Mentzell/Jeff Tompkins
Revision 3	7/30/18	Heather Hudson/ Dontay Moore
Revision 4	7/30/19	OIT Enterprise Standards Committee

Appendix

In-House Applications

This category can include applications developed by a vendor – the distinguishing element is that OIT have access to and maintain the source code. All application standards apply, to include languages, frameworks and coding style. Languages would include C# (back end), ASP.net, HTML and JQuery (front end). In-house applications also include use of MS Entity Framework and MVC3.0 for back end. Coding style and practice standards are something OIT have been working on and have some guidelines, but are not yet fully formalized. ~~.~~The audience for coding standards is OIT developers or a vendor developing code for OIT that OIT will own and maintain. However, this is an uncommon scenario. The developers would be expected to adhere to the standards, and enforced during code review.

Software as a Service (SaaS)

Application hosted entirely by an Application Service Provider. Focus should be on quality of the product, reliability, availability, security and service level agreement. The application must run on all standard browsers as defined in Section 1.1. County OIT may want to leverage the application data (example, reporting) or extend its functionality easily (provide API, use SOA). OIT should specify security standards, for example, HTTPS access to the application, and encryption of data on the server. OIT should have a way to export the application data for use in another application/context should the company go out of business. Must support SAML based authentication.

Vendor Applications

Application provided to OIT by a vendor. OIT hosts the application, but do not maintain the source. The application should adhere to all application standards (as listed in Section 1.0) to include being able to be deployed on OIT standard desktop, database, server/platform and system authentication. The application must ensure sound architecture, such as the ability to separate database and application servers. OIT would usually prefer web applications over thick clients depending on applicability except when not technically feasible (example: console app). Thick client applications should be compatible with Citrix.

Systems Monitoring

- Automatic discovery of all selected nodes, systems, applications and interfaces.
- In depth analysis of network performance.
- Monitor performance of Emergency Call Center (911) and VOIP systems.
- Monitor radio and tower control systems (example, ASTRO 25 HPD, Motorola ACE3600, etc.) Logical grouping.
- Smart classification and mapping for an Enterprise view.
- In depth performance monitoring for proactive fault management.

- Self-healing for automated repair of selected faults and alerts.
- Configuration baseline monitoring for advanced notifications on problem changes. Application performance monitor for critical data services
- Monitor environmental controls, temperature, fans, power (UPS/Generator/ATS) The solution's scalability.
- Integration to third party performance and monitoring tools.
- Intelligent alerting (correlation and de-duplication). System security management for levels of access.