Y22-02-SS
ORANGE COUNTY
GOVERNMENT EMPATHY TRAINING SIMULATION SERVICES

Orange County, Florida requires a software solution to support First Responders. To date, research within the industry has indicated to the County that **Engineering & Computer Services, Inc. (ECS)** is the sole provider of **Government Empathy Training Simulation Services** to achieve the following objectives:

(1) Understand, identify, and measure empathy, communication, and trust related to frontline professionals' response to emergency situations, high stress scenarios, and specific outcomes;

(2) Design and develop an immersive system for frontline professionals with virtual humans capable of detecting, modeling, and fostering techniques to reduce the deleterious effects of empathy in his or her daily handling of emergency and/or stressful situations; and

(3) Test the immediate and long-term effectiveness of the immersive empathy training environment on frontline professionals' awareness of and ability to accurately, effectively, and professionally respond and resolve empathy related opportunities encountered daily in various situations.

Research indicates that ECS is the only software meeting the County's requirements, which are as follow:

1. Government-off-the-Shelf (GOTS) Software. The County is seeking a configurable solution. Custom Software Development services will not be considered.

2. Software shall provide gaming and computer simulation services using Virtual Reality (VR) and Immersive Training Environments (ITE)

3. Software shall possess Certified Capability Maturity Model Integration (CMMI) Level 3

4. The existing baseline software (including the source code) shall be suited for refinement and adaptation to first-person frontline professional empathy training.

5. Software shall be compliant with the National Institute of Standards & Technology (NIST) standards

6. Compliant or easily adaptable to be compliant with security requirements of the County (attached hereto).

Any vendor that wishes to determine if they meet the County's requirements is invited to contact Alina Hernandez Fernandez by email at Alina.Hernandez@ocfl.net by phone at (407) 836-5548. This information will be available for review until **5:00 PM, October 27, 2021**.

Orange County, Florida,
Information Technology Standards

9/23/2021

Table of Contents

1.0 Introduction to Orange County IT Standards

This guide provides a framework for documenting policies, business processes, and internal controls used to effectively support the information technology (IT) resources of the government of Orange County, Florida, Board of County Commissioners (County). It explains the role of the County's Information Systems and Services (ISS) personnel in approving, ordering, delivering, and maintaining IT services and products (hardware, software, networks, security, and other IT components) for employees throughout the County. It identifies County-approved products and procedures for acquiring IT systems and services. This guide also establishes County IT standards for use by third-party vendors providing externally hosted systems to various County departments.

The goal of ISS is to build an efficient, effective, and cost-efficient operation with an excellent return on investment by delivering new technologies and a state-of-the-art network server infrastructure. ISS is dedicated to providing prompt problem resolution through the customer service of its Help Desk. ISS seeks to maintain a diverse computing environment designed to meet the requirements of all County departments, while minimizing the risk of data loss or downtime. All computer hardware and software must be approved by ISS prior to purchase.

The ISS Department is comprised of 160+ employees, who are committed to its customer relationship-building attitude. ISS provides a business approach to serving all County agencies, which together form a partnership with ISS personnel to enhance productivity and service to the community.

The following standards apply to any device approved for connection to the County IT network or in use by County employees:

- ISS personnel are responsible for ordering all new computers, software, servers, telephones, and mobile devices for use by County employees. Hardware and software orders arrive at the ISS Warehouse at 3517 Parkway Center Court, Orlando, FL 32808.

2 Submit orders by opening a ticket to request the new equipment or software using the ISS Support Center's SupportCenter@ocfl.net email address. All purchase requests require approval in two forms. Initial request approval is by the customer's manager as indicated in the Peoplesoft "Reports To" field. Updates and Changes should be submitted through an ECN to HR. The secondary approval must come from a divisional representative with purchasing limit approvals. The emails will include pertinent information about the requested item(s). If sufficient details are not included in the initial email request, ISS staff will reach out to gather necessary information for the order. A list of authorized new products for purchase begins on the following page.

- ISS Warehouse personnel are responsible for coordinating with the Comptroller's Office staff to apply County asset inventory tags on computer components, as necessary, prior to installation of the equipment. No one but the Comptrollers staff an add or remove asset tags.
- ISS Support personnel will install all operating systems and software. At the time of installation, ISS Support personnel must receive a copy of all installation software, along with written installation instructions, and licensing documentation. ISS will not install software without proof of licensing.
- All installed computers must, at a minimum, have the following:
  - ISS-installed anti-virus software
  - Computer configuration policy control for group management of devices by Active Directory
  - Remote access only as designated by ISS (ISS prohibits the use of Virtual Network Computing [VNC] and Remote Desktop computing.)
  - ISS-approved remote monitoring and management tools
  - Only ISS personnel shall have administrative rights.
  - Hardware must be a standard supported model
- ISS Enterprise Security is responsible for ISS video service; however, deployment of video equipment on the local government network must be discussed with staff members of the Data Network Team prior to purchase to determine compatibility, bandwidth, network equipment requirements, and installation feasibility.

- Generally, ISS does not support multicast on the County networks, except in specific special cases.

2.0 Authorized Products for New Purchases

This section includes detailed information about products authorized for use with the County's IT Systems.

2.1 Authorized Hardware

Dell Desktop Computer

Dell OptiPlex 7090 Small Form Factor (SFF) (does **not** include monitor or Microsoft Office Software)

- Intel Core i5 Processor
- Windows 10 Professional 64-bit
- 256 GB Solid State Drive (SSD) Hard Drive
- 8 GB Random Access Memory (RAM)
- USB Keyboard and Mouse
- Display Port to DVI Adapter 6' Cable
- 3-Year Onsite Hardware warranty

Dell Precision CAD Workstation

Dell Precision T3431 SFF (does **not** include monitor or Microsoft Office Software)

- Intel Core i7-9700 Processor
- Windows 10 Professional 64-bit
- 32GB RAM
- 512GB SSD Hard Drive
- NVIDIA Quadro P1000 4GB, (4 mDP) Video
- DVD RW Optical Drive
- USB Keyboard and Mouse
- 3-year Onsite Hardware warranty
- StarTech Mini DP to DP 1.2 4k 6' Cable (Included separately)

Dell Latitude Laptop - Standard User CDW # 6417629 Mfg., Part# : 3000077256394 (valid until July 14/2021)

Dell Latitude 5420 Laptop (does **not** include Docking Station, Case, or Microsoft Office Software)

- Intel Core i5
- Windows 10 Professional 64-bit
- 14.0" FHD (1920 x 1080) Non-Touch Anti-Glare LCD
- 512 GB SSD Hard Drive
- 8 GB RAM (16GB Optional)
- Internal Aircard (Optional)
- **NO** DVD-ROM Drive
- HD & IR Camera w/Microphone
- 3-Year Absolute Resilience Protection
- 3-Years Onsite Hardware warranty
- Optional Accessories (must be explicitly requested)
  - Dell WD19TB Docking Station
  - Dell KM717 Premier Wireless Keyboard/Mouse Set
  - Pro Briefcase 15 Carrying Case
  - Backpack Case

Dell Precision Laptop - Standard User **CDW #6506832 Mfg., Part# : 3000083439959 (valid until July 14/2021)**

Dell Precision 3560 Laptop (does **not** include Docking Station, Case, or Microsoft Office Software)

- Intel Core i5
- Windows 10 Professional 64-bit
- 15.6" FHD (1920 x 1080) Non-Touch Anti-Glare LCD
- 512 GB SSD Hard Drive
- 8 GB RAM (16GB Optional)
- Internal Aircard (Optional)
- **NO** DVD-ROM Drive
- LCD RGB & IR Camera w/Microphone
- 3-Year Absolute Resilience Protection
- 3-Years Onsite Hardware warranty
- Optional Accessories (must be explicitly requested)
  - Dell WD19TB Docking Station
  - Dell KM717 Premier Wireless Keyboard/Mouse Set
  - Pro Briefcase 16 Carrying Case
  - Backpack Case

Dell Docking Stations

- Dell 5410 Compatible:: CDW # 6081932, DELL CTO THUNDERBOLT DOCKMfg. Part# : 3000061015836
- Dell Precision Compatible: Dell Performance Dock. Model#WD19DC

Dell Wireless Keyboard /Mouse

- CDW # 6081940, DELL CTO PREMIER WRLS KEYB/MOUSE KM717Mfg. Part#: 3000061015837

DELL CTO PRO BRIEFCASE

- CDW # 6081935, DELL CTO PRO BRIEFCASE 15Mfg. Part#: 3000061015839

2.2 Authorized Software for Desktops and Laptops

- Microsoft Windows 10 Pro Operating System current version or 1 version prior
- Internet Explorer 11 and Google Chrome (**Note:** Browser customizations are unsupported)
- Microsoft Office 2019 Pro Plus Microsoft Office Pro Plus, current version or 1 version prior
- All Microsoft Office applications on the same PC must have matching software versions (i.e., Project, Visio, Word, Power Point, Access, etc.).
- Microsoft Visio 2019 Pro/Standard Microsoft Office Pro Plus, current version or 1 version prior
- Microsoft Project 2019 Pro/Standard current version or 1 version prior
- Microsoft Visual Studio 2019 Pro current version or 1 version prior
- ISS Desktop Support must pre-approve any application requiring the use of Active X controls. At a minimum, the application must meet the following criteria:
  - It must be an .MSI file with silent installation/distribution from the command line.
  - It must install and operate without end-user administrator permissions.
- Java 1.8.25 – Only supported version of Java
- Silverlight – latest version
- Bomgar or WebEx for remote access
- Adobe Acrobat Pro 2020, current version or 1 version prior.
  - Please note that older versions may not be able to view newer version files. Check compatibility before ordering.
- Adobe Acrobat Reader DC.

2.3 Authorized Network Connectivity

- AT&T Wireless AirCards
- Cisco AnyConnect VPN Client
- Hosted applications must be accessible from devices with automatically assigned network settings. (Dynamic Host Configuration Protocol (DHCP) should supply all settings. Fixed addresses are not allowed.)

For all devices joined to our domain (this also applies to “vendor supported” devices and applications):

- ISS must install the Operating System and software on the device.
- ISS must receive a copy of all software and installation instructions.
- Hardware must be a standard supported model (see also hardware section 2.1).
- SCCM management client and Antivirus software must be installed.
- PGP is required on all laptops.
- The device must receive Windows updates and computer configuration changes via Active Directory policies.
- Only ISS personnel shall have administrative rights.
- VNC and Remote Desktop are not permitted.

2.4 Authorized Client Based Databases

- Oracle (network based database)
- SQL Server (network based database)

2.5 Authorized Mobile Devices

ISS personnel are responsible for placing orders for all new phones and mobile devices. Individual departments may purchase chargers, holsters, rugged cases, and other accessories, along with other office supplies. Department manager approval is required for all mobile device requests.

Conventional Phones

Legacy phone with data & texting disabled

- Kyocera DuraXE Epic

Android Phones

County Android phones must run Android Version 9.0 or above.

- Samsung Galaxy S20FE (AT&T)
- Samsung Galaxy S20FE (Verizon)
- Samsung XCover Pro (Rugged. Only on Verizon)

Tablets

- Tab S7FE 64GB (Wi-Fi Only) **Android**
- Tab S7FE 64GB (Wi-Fi & Cellular Capable) **Android**
- iPad 8th Gen 128GB (Wi-Fi Only) **iOS**
- iPad 8th Gen 128GB (Wi-Fi & Cellular Capable) **iOS**

2.6 Authorized Peripherals and Accessories

Black and White LaserJet Printers

- HP LaserJet Pro 404n (500 to 2,000 pages per month) < 4 users
- HP LaserJet M506dn or M507dn (5-10 people, 1,500 to 5,000 pages per month + secure printing)
- HP LaserJet M608dn (10-25 people, 5,000 to 16,000 pages/month + secure printing)

Color LaserJet Printers

- HP Color LaserJet Pro M454 (750-4,000 pages per month, small paper tray)
- HP Color Laserjet Enterprise M652dn (2,500 to 17,000 pages/month + secure printing)

HP Multi-Function Devices (MFD) (Print/Scan/Copy)

- HP MFP M428fdn (750 to 4,000 pages per month, B/W)
- HP color MFP M281fdw (1 or 2 people, occasional scanning)
- HP color MFP M479fdn (750 to 4,000 pages per month)
- HP color MFP M578dn (2,000 to 7,500 pages per month)

Specialty Printers

- Label Printers: Zebra
- Badge Printers: Fargo Model HDP6600
- Note: *Zebra printers are label printers for Pharmacies and the Fargo printers are HR printers for ID badges.*

Large Copiers (Full Sized, often leased) – Vendor Supported

- Toshiba Copiers
- Canon Copiers

Scanners (all come with Adobe Acrobat and Automatic Document Feeders [ADF])

- Fujitsu ScanSnap iX1500 (30 pages per minute [ppm], 50 sheet ADF, Connected via USB)
- Fujitsu fi-7160 (60 ppm-mono and color, 80 sheet ADF, Connected via USB
- Fujitsu N7100 (25ppm, 50 sheet ADF, Networked)

Note: Printers must use Original Equipment Manufacturer (OEM) toner cartridges only.

Note: ISS must review and approve Desktop, Copier, and combo unit purchases used for printing from the PC. Contact *SupportCenter@ocfl.net* for more information and assistance.

3.0 Unsupported Products

3.1 Unsupported Hardware

- Pentium dual-core and older desktop systems, Optiplex 755, 960, 990, 9010
- Latitude D-series Laptops, Latitude E6500, E6510, E6520, E6530, E65xx
- Non-Dell PCs
- Wireless keyboards and mice (except conference rooms)
- Desktops and Laptops over 5 years old
- See also *Section 3.4, Peripherals and Accessories*.

3.2 Unsupported Software

- MS Office platforms 2 versions prior to current (including Visio & Project)
- Non MS Windows-based operating systems
- Safari Web Browser
- MS Office plug-ins or VBScripts
- Windows Applications from the Windows App Store
- Freeware
- Microsoft Windows 7, XP, 98, 95 and 3.5.1 are no longer Orange County Standard (No new applications can be purchased for Win 7 computers)
- Freelance
- SHL Vision & Vision Express, WIN9x/WINNT/UNIX
- Reflections
- Chrome extensions

3.3 Unsupported Client Databases

- No client-based databases are supported (e.g., Microsoft Access, Filemaker Pro)

3.4 Unsupported Peripherals and Accessories

- Inkjet printers
- Printers over 7 years old
- Scanning to multiple folders per device
- Address books in scanners/copiers (users manage their own)
- Personal (non-County) mass storage devices (hard drives, thumb drives, etc.)

4.0 Prohibited Products

4.1 Prohibited Hardware

- Non MS Windows-based PCs, laptops, and tablets
- Recycled, Remanufactured, and non-OEM toner Cartridges
- Refurbished PCs
- Personal (non-County) computing equipment
- Any network (voice or data) device not operated, administered, or expressly approved by ISS
- Any internet access device not operated, administered, or expressly approved by ISS
- Donated and vendor-provided PCs that do not meet County standards

4.2 Prohibited Software

Note: This list is not all inclusive of prohibited software. If you have questions concerning a specific application, please open a ticket or contact the Desktop Support Supervisor.

- Microsoft Internet Explorer version 10 and below
- Server software is not permitted on workstations (SQL server, print servers, web server, file sharing)
- Cloud-based collaborative software (data must be stored within our datacenter).
- Personal Software (purchased for non-commercial use)
- Firefox, Opera, Vivaldi Web Browsers
- Any Alpha, Beta, Shareware, Trialware software not operated, administered or expressly approved by ISS and Purchasing.
- Anti-virus products not operated or administered by ISS
- Personal firewall products
- Network scanning tools
- Remote access software other than that ISS explicitly authorizes
- Desktop sharing, remote control, or remote communications software such as Remote Desktop
- Web page editing tools (without prior approval)
- Software coding tools (without prior approval)
- User installed screen savers
- Games
- Third Party Desktops
- Disk Compression
- Non-Static BITMAP Backgrounds or screen savers
- iTunes or other content sharing applications
- P2P software
- MS Access Run-time Libraries
- Zoom installed Application (Web ok)

4.3 Prohibited Network Protocols

- NETBUI
- AppleTalk
- Any network (voice or data) software or service not operated, administered or expressly approved by ISS.
- Any Internet access service not operated, administered, or expressly approved by ISS.

4.4 Prohibited Peripherals and Accessories

- Portable music devices
- Webcams (exceptions with Manager approval)
- Printer sharing through a PC
- Wireless printing

5.0 Standards for In-House Servers and Server Operating Systems

The following server standards apply to all servers on the Orange County network maintained by County ISS personnel:

- Only ISS personnel shall have administrative rights to server-class devices.
- All servers shall operate in a VMWare-based virtual environment. The ISS Infrastructure Manager must approve in writing any exceptions to this rule prior to project implementation.
- Any device that cannot run in a VMWare-based virtual environment ("stand-alone") must have hardware and software approved by ISS Infrastructure Manager prior to its connection to the County network.
- All servers will comply with ISS standard resource configurations. The ISS Infrastructure Manager must pre-approve any deviation from this standard and may incur additional costs.
- No server shall be configured as a 'file share'. File storage shall be NAS based.
- In addition to the requirements listed above, all stand-alone devices must, at a minimum, meet the following requirements:
  - Be installed at the County's Regional Computing Center (RCC)
  - Be rack-mountable
  - Only run server-class operating systems
  - Be configured for out-of-band management and have remote monitoring software installed
  - Meet ISS minimum hardware requirements including, but not limited to:
    - Dual power supplies
    - Dual NIC's
    - Dual processors
    - Dual HBA's
    - Dual hard drives, redundant array of independent disks (RAID) configurable for boot drive
    - Use storage area network (SAN) for attached storage devices

The following lists the default standards used for specific server operating systems:

5.1 Microsoft Windows-Based Server Requirements

In no case shall an operating system be installed that is not under current manufacturer support (typically this is N-2 for Microsoft operating systems).

- The Boot partition "C Drive" shall be 100 GB (Thin Provisioned).
- The Data partition shall be 40GB to 100 GB (Thin Provisioned).
- 8 GB RAM
- The C: drive will contain only the operating systems. Databases must reside on separate servers from that of application or Web servers.
- Application, service, or vendor accounts will not be members of the domain administrator's group.
- Application, service, or vendor accounts will not be in the local administrator's group for any server.
- Applications must run as a service. ISS prohibits applications that require a user account to remain logged in.

5.2 Linux-Based Server Requirements

- RHEL 7 or greater, kernel 3.0 or greater, 64 bit architecture
- 40 GB Boot partition
- 4 GB memory
- Applications will **not**:
  - Have a web interface that allows users to access the system as a privileged account.
  - Run root processes.
  - Be installed in any file system that is part of root.
  - Write log files to any file system that is part of root.
  - Update root system's files during installation.
- Applications will be installed using a unique user ID and unique group ID.
- Purge application and system logs, as needed.
- Disable Telnet and the "r" commands on all Linux servers.
- .rhost file is not available.

5.3 Oracle-Based Server Requirements (Legacy Support)

- County-supported Oracle versions are: Oracle Enterprise Edition current version or 1 version prior that is supported by Oracle.
- County-supported environment for Oracle databases is RHEL Linux.
- Database setup shall be compliant with Oracle's Optimal Flexible Architecture (OFA) file naming conventions
- Applications must be installed under separate schema not requiring Database Administrator (DBA) privileges or DBA type privileges. Applications will not require or use the Linux Oracle account.
- Applications will provide a security module to manage user IDs and permissions.
- Applications shall support Orange County's Encryption policy's whether at table space or column level for Sensitive/Protected data without impacting performance.
- Application vendors shall identify and document Sensitive/Protected data field/s as defined in Orange County Security Standards Policy.
- Application vendors shall provide all database creation scripts and any other required scripts to build, maintain, and support the database environment.
- Application vendors shall provide all documentation related to all database creation scripts and any other required scripts to build, maintain, and support the database environment.
- ISS personnel shall install databases using vendor provided scripts, initialization parameters, and any special performance related parameters.
- Oracle's Administrator (SYSADM) account must not be required for software to operate.
  NOTE: If SYSADM privileges are required for installation, a County Database Administrator shall perform the installation vendor supplied scripts under the application vendor's direction.

5.4 Microsoft SQL-Based Server Requirements (Preferred Standard Database for current and future use)

- County-supported Microsoft SQL Server versions are: MS SQL Server Enterprise Edition current version or 1 version prior that is supported by MS.
- Database installations must be on a separate server from the application executables and support files. Database installations cannot be installed to the C: drive of the Windows Server. Applications will allow the ISS Database Administrator to specify the drives and directories where the database files will reside.
- MSDE, SQL Server Express, or MS Access based software are prohibited.
- Applications must support SQL Servers Integrated Security model.
- Applications shall support Orange County's Encryption policy's weather at table space or column level for Sensitive/Protected data without impacting performance.
- Application vendors shall identify and document Sensitive/Protected data field/s as defined in Orange County Security Standards Policy.
- Applications must contain a security module to manage user ID's and permissions, with no blank or hard-coded passwords allowed.
- Applications shall support a Cluster aware environment.
- ISS prohibits use of applications that create, update, or delete of any files on the database server outside the constructs of the database engine.
- ISS prohibits use of applications that create new databases or persistent database objects as part of its operation.
- Applications shall support application database backups/restores using the County's Enterprise Backup Tool. Currently, the County standard is CommVault's Galaxy iData-Agent for SQL Server.
- Applications must provide an audit mechanism to record the date, time, and user id that last modified a given row in an application table.
- Applications must utilize database referential integrity.
- Server Administrator privileges are not permitted.

NOTE: If Server Administrator privileges are required for installation, an ISS Database Administrator shall perform the installation.

6.0 Network Systems Requirements

6.1 Protocol Node Names and Addresses

- The ONLY protocol allowed on the County Data Network is the Internet Protocol referred to as Internet Protocol (IP) or Transmission Control Protocol/Internet Protocol (TCP/IP) Version 4.
- There can be only one unique address for each node on the network. Node naming and addressing conventions will conform to the guidelines established here.
- The NOC assigns all addresses for all devices connecting to the County Network. All IP addresses must conform to R.F.C. 1918:

  10.0.0.0 - 10.255.255.255/8

  172.16.0.0 - 172.31.255.255/12

  192.168.0.0 - 192.168.255.255/16

- The NOC maintains an addressing plan and uses the plan to assign addresses. The Internet Addressing Authority, a private entity, assigned a block of addresses for the County. The NOC will maintain and assign these addresses, as needed.
- Use of Registered Internet addresses on the County network is not allowed.
- All network numbers for "special function" TCP/IP networks will be assigned by the NOC.
- No INTERNET connections are allowed from any node, modem, or communications device on the network without NOC and Enterprise Security approval.
- A network-wide, shared-use Internet connection is available to all entities.
- TCP/IP DOMAIN NAME SERVERS (DNS) are an alternative to local administration and maintenance of a "hosts" file. Any Divisions, Elected Officials, or agencies wishing to use the DNS may send a list of IP addresses to be included in the DNS to the ISS Support Center, (407-836-2929 or 6-2929), which will be routed to the NOC staff.
- Entities who have dedicated network staff and wish to be assigned their own IP address space will request the assignment from the NOC through the ISS Support Center, (407-836-2929 or 6-2929). These entities will provision their own DNS and be responsible for administration of their own IP address spaces (as assigned by the NOC for the agency to administer).
- Only routed networks with at least 254 IP nodes are eligible for this option. DHCP is provided by the NOC.
- No shared device (printer, server) may use a DHCP address. Static IP addresses are available in limited amounts on request.

6.2 Bridges, Routers, and Gateways

- Routers are required at points in the network where traffic control and/or broadcast domain segmentation needs exist.
- Routers are required on all Wide Area Network connections.
- Protocol conversion is not supported on this network, as one common protocol (TCP/IP) is standard for all nodes.

6.3 Network Security

- All default accounts on all processors connected to the network will either be disabled or have the default password changed. No accounts are allowed without passwords.
- The default "privileged password" on all network electronics will be changed.
- All dial-up access must be provided through secure access servers. No direct access via dial-up lines is allowed on any type of device, processor, terminal, server, or PC connected to the network.
- The NOC provides and maintains a secure access server for Dial-up use. Contact the ISS

Support Center (407-836-2929 or 6-2929) for remote access authorization by the Enterprise Security Team.

- The requesting department will provide the hardware & software for the employee's home use, unless the employee provides their own.
- Vendor field service will have remote access through NOC provided access servers. VPN access is available for use.
- No entity on the network shall make any connection to the Internet, dial-up service, wireless provider, or wireless access-point without written permission from the ISS Enterprise Security Team and Network Operations.
- An Internet gateway is provided for all entities on the network to use.
- Any entity that directly connects their network to the Internet may not remain connected to the County network, due to security risks. If the Internet connected entity supplies, at their own expense, an acceptable Firewall between their networks and the County networks, the County network connection can resume via the Firewall provided.

Wireless Local Area Network (LAN) (Ethernet) Security

- All 802.11x wireless LANs must use a DOT1X supplicant for network admission control.
- All 802.11x clients must use VPN triple Data Encryption Standard (DES) or Advanced Encryption Standard (AES) encryption. Client authentication via RADIUS server is required. The RADIUS server is provided and administered by ISS Enterprise Security.
- All access points attached to the County network must be Lightweight Access Point (LWAP). (No stand-alone access points are permitted)

Wireless Wide Area Network (WAN) Security

- The County maintains a contract with a wireless provider. A gateway is available for connecting to the contracted wireless provider. The County prohibits access to the network using any other wireless provider.

6.4 Network Components

Transmission Media

- Fiber-optic, Category 5, 5e, and 6, and Category 3 Unshielded Twisted Pair (UTP), Shielded Twisted Pair (STP), and radio (802.11x) are all permitted for IP data communications in the network.

Transmission Methods

- Optical, metallic cable, leased data circuits (analog, digital), private (analog, digital), and wireless (802.11x) are all permitted for IP data communications in the network.

Supported LAN Types

- ETHERNET, 802.3, 10 BASE T, 100 BASE TX, 100 BASE FX, 1000 BASE xx (Gigabit), 802.11x (wireless Ethernet), 10 GIGABIT.
- Etherchannel: The only Etherchannel protocol supported by the County is 802.3ad Link Aggregation Control Protocol (LACP).

6.5 Network Circuits

- The NOC will design all WAN networks and, if required, procure leased data communications circuits from the Carrier.
- The NOC will act as the central point of contact between all entities using WAN circuits.
- The NOC will be notified by the affected entity and/or the ISS Support Center of service affecting WAN outages.
- The ISS Support Center (407-836-2929 or 6-2929) and the NOC will be responsible for coordinating successful repair of WAN circuits.
- The NOC will be responsible for ordering the disconnection and termination of leased data circuits upon notification by the customer.

- Critical LANs and/or WANs may be designed with duplicate, automatic, redundant circuits and electronics to provide automatic recovery of data communications.
- Circuits leased by any entity (other than the County) will be managed by that entity's technical staff.
- A Remote Site is available for recovery of certain critical applications and County networks in the event of a formally declared disaster.

6.6 Network Installation

- In situations where installation of network equipment by one entity may affect customers from other entities, the installation will be jointly coordinated by representatives of the NOC and the other entities.
- The NOC will design and install all LAN and WAN networks, except in special circumstance.

6.7 Network Trouble Reporting

- Customers exclusively confined to applications delivered by networks supplied by the NOC will call or e-mail the ISS Support Center (407-836-2929 or 6-2929) to report trouble, request service, and get technical advice. The ISS Support Center will screen all calls, resolve any problems it is able to resolve with ISS Support Center staff, and refer unresolved network problems to the NOC.
- Customers exclusively confined to applications on networks supplied by other entities will call that entity's network staff to report trouble, request service, and get technical advice.
- Customers on a mix of processors and networks supplied by the NOC and other entity's processors and networks will call the ISS Support Center (407-836-2929 or 6-2929) to report trouble, request service, and get technical advice.
- The NOC employs a variety of network management and troubleshooting tools and systems. These network management systems are used by the NOC staff to test, troubleshoot, and diagnose all devices attached to the network.
- All LAN equipment attached to the network must support Simple Network Management Protocol (SNMP) and/or SNMP-2. Remote Monitoring (RMON) is also allowed, but not instead of SNMP. RMON is in addition to SNMP. Older equipment not supporting these standards will be phased out. The NOC is the only organization permitted to run SNMP on network equipment.
- Network problems that can be repaired by the NOC will be scheduled in a repair queue. Repair priority is based on the severity of the problem and quantity of customers affected.
- All devices attached to the network must have at least a minimum SNMP profile entered, consisting of the entity's name, address, and technical support staff phones number(s). This will assist NOC staff in locating the network on which the equipment is located, when troubleshooting.

6.8 Network Performance Management

- The NOC is responsible for monitoring all LAN and WAN performance. This includes all SNMP and RMON.
- Only NOC staff members are allowed to run SNMP/RMON on network devices.
- The NOC will redesign networks, which sustain traffic loads that adversely affect customer interactive response times and/or reliability.
- The NOC will assist other entities with managing the performance of their networks as requested.

6.9 Network Documentation

- Each entity on the network will provide the NOC with a current diagram of network topology, equipment location, and configuration (including building address and floor location).
- The NOC will provide a diagram of the network as well as tables and listings of all physical and logical components to any approved requesting entity.

- Each entity on the network will provide on-going, updated information to the NOC reflecting components, circuits, and logical changes.
- The NOC will add this information to its diagram and database, and will provide the revised network documents to all requesting entities.

7.0 IP Telephony Standards

- The definition of IP telephony is telephones and a Private Branch Exchange (PBX) with an integral Ethernet Network Information Card (NIC) using the Internet Protocol to communicate.
- All telecom related applications must be certified under the Avaya DevConnect program and compatible with the County's current level of Avaya Communications Manager for the appropriate site.
- The Telecom Unit must approve all peripheral applications, or software, prior to purchase.
- IP phones must derive their electrical power from the CAT-5e Ethernet cable. (POE type-1, 802.af standard)
- Ethernet switches in the closets will be used to provide in-line DC power through the CAT-5e patch panels.
- All Ethernet electronics used in this configuration will have a UPS attached.
- If the IP phone has a provision to connect the desktop PC into the same Ethernet as the phone, then the IP phone must use Ethernet switch technology. Use of a hub/repeater is not allowed.
- IP phones must operate in a separate subnet from the attached PC.
- IP phone packets will be given the highest priority of all IP communications traffic on the LAN. Other non-telephony applications will have their "IP Precedence" bit modified at the Ethernet switch to conform to this standard.
- IP phone access to the network through the internet provider will use the ISS provided VPN services.
- Direct access to internal devices is prohibited.

8.0 Externally-Hosted System Standards

This information is for all vendors, networks, systems, and applications that will transmit, process, store, or handle electronic data provided by County.

8.1 Data Input and Processing

- Any use of Social Security Number information shall adhere to and abide by Florida Statutes, specifically F.S. 119.071, which provides detailed guidelines on usage of Social Security Numbers.
- The hosted application shall not have access to Social Security information.
- The hosted application shall not have access to data containing bank information.
- The hosted application shall not have nor be granted direct or indirect access to the County's Active Directory user names.
- The hosted application shall not have access to the County's internal or DMZ networks.

8.2 Data Storage and Handling

- The provider shall encrypt any data accessible from the hosted application meeting the following criteria at rest and in transit:
  - Names
  - Addresses
  - Phone numbers
  - Email addresses
  - Birth dates
  - Federal/state/local documents numbers
  - Account numbers
  - Race or religious information
  - User names
  - Passwords
  - Employee identification numbers
  - All Health Insurance Portability and Accountability Act (HIPAA) information
  - All Purchase Card Industry Data Security Standards (PCI DSS) information
- Any data, accessible from the hosted application or directly accessible from it, should be encrypted.

8.3 Transmission of Data

An encrypted tunnel must be used to transmit any data referenced above.

8.4 Disposal of Data

When no longer needed, or when data must be removed from the system, it shall be sanitized and disposed of using one of the methods listed below:

- **Sanitization** – Overwriting data previously stored on a disk or drive with a random pattern of meaningless information
- **Destruction** – Physically damaging a medium, so that it is not usable by any device that may normally be used to read information on the media, such as a computer, tape reader, audio or video player
- **Purging Data** – Using a strong magnetic device, such as a degausser, to render data unrecoverable

8.5 External Audits

- The vendor must ensure that the web hosting environment and application is secure using IT security best practices.
- The external service, system, and application must pass a yearly penetration test performed by ISS personnel.

9.0 Computing Center Standards

In addition to standards outlined in *5.0, Standards for In-House Servers and Server Operating Systems*, the following requirements apply to hardware installed in an Orange County Regional Computing Center, such as, network switches, appliances, servers, storage arrays, etc. These requirements apply to orders placed by Orange County personnel, vendor special orders, and orders placed by RCC tenants:

- Standard rack configuration is 42U
- PDU orders need network monitoring (smart PDU) for rack
- Mounting hardware for racks should be included in order
- Dual power supplies for all equipment
- Dual NIC cards for any hardware needing to connect to network

10.0 Acronyms

ADF	Automatic Document Feeder
County	Government of Orange County, Florida, Board of County Commissioners
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
DVI	Digital Visual Interface
DVD+/-RW	Digital Versatile Disk-Rewritable
GB	gigabyte
ISS	Orange County Information Systems and Services
IP	Internet Protocol
IT	Information Technology
NOC	Network Operations Center
OEM	Original Equipment Manufacturer
ppm	Pages per minute
RAM	Random Access Memory
RMON	Remote Monitoring
SAN	Storage area network
SNMP	Simple Network Management Protocol
SSD	Solid State Drive
SFF	Small Form Factor
TCP/IP	Transmission Control Protocol/Internet Protocol
USB	Universal Serial Bus
WAN	Wide Area Network
VNC	Virtual Network Computing
VPN	Virtual Private Network