TO: **ALL COUNTY PERSONNEL**

FROM: **VERDENIA C. BAKER**
COUNTY ADMINISTRATOR

PREPARED BY: **INFORMATION SYSTEMS SERVICES (ISS) DEPARTMENT**

SUBJECT: **ACCESS TO THE PALM BEACH COUNTY ENTERPRISE NETWORK**

PPM #: **CW-O-061**

==========

ISSUE DATE	**EFFECTIVE DATE**
August 6, 2019	**August 6, 2019**

==========

PURPOSE:

To provide standards and guidelines for access to the Palm Beach County Enterprise Network, including definitions of the types of access, conformance to public records law, user responsibilities, and the actions that will be taken if this policy is not followed.

UPDATES:

Future updates to this PPM are the responsibility of the Network Services Division Director under the direction of the Chief Information Officer of ISS.

AUTHORITY:

1. Information Resource Security Program Policies (PPM # CW-O-059) as may be amended
2. Records Management Program (PPM # CW-R-005) as may be amended
3. The Use, Retention, and Destruction of Electronic Mail (PPM # CW-R-006) as may be amended
4. Electronic Mail Privacy Electronics Commission Privacy Act (Public Law 99-508--OCT 21, 1986) as may be amended

BACKGROUND:

The Palm Beach County Enterprise Network contains important intellectual property. The Enterprise Network houses both information that is restricted from public access and information required to be available for public access. The Enterprise Network also contains resources that can be damaged if not managed properly by trained IT professionals.

Users accessing the Enterprise Network typically fall into one of four groups, including County employees, vendors, subscribers to County services, and members of the public. Access

privileges to the Enterprise Network and the information contained therein are different for each of these user groups.

DEFINITIONS:

*(Refer to **Exhibit A** for a listing of definitions related to this PPM.)*

POLICY:

I. Usage of Enterprise Network

Access to the Enterprise Network is provided with the stipulation that it is used by Elected Public Officials and their staff, County Employees, Subscribers, Telecommuters, and Vendors in support of their job requirements, governmental related activities, or to access information that is authorized. The Enterprise Network will be used in strict compliance of the Information Resource Security Standards and Guidelines and any user guides that are published for users of the access services.

The Enterprise Network is a County resource. No activities that would waste resources or jeopardize public or private information will be tolerated. Any attempt to break into accounts, access information that is not authorized, or disrupt service is prohibited. The use of the Enterprise Network for personal or economic gain, unless specified in a contractual agreement, is a direct violation of County policy. Copyrighted and licensed software may not be duplicated unless permission is explicitly stated in the copyright statement or granted in writing by the copyright authority. Users should not assume that a file being globally readable grants them the authorization to reuse it.

II. Access to Enterprise Network

Access to County information resources must be strictly controlled. County information resources must be used only for official County purposes. Such official County purposes include complying with the public access requirements of the Public Records Act, Chapter 119, Florida Statutes, and the ISS Governance Policy. Information which, by law, is sensitive or confidential must be protected from unauthorized access or modification. Access to any service that is not specified on the access profile is restricted.

Access policies and standards apply to:

- all departments of the County government, including all levels of management and to the personnel they supervise;
- County automated information systems that access, process, or have custody of data;
- all elements of the Enterprise Network infrastructure including servers, personal computers, mobile devices, IoT devices, distributed processing, client/server and web-based networking environments of the County, other enterprise technologies acquired and approved for enabling electronic access to County resources and data; and

- information resources owned by others, such as political subdivisions of the County, elected officials, or departments of the state and federal government, including cases where the County has a contractual or fiduciary duty to protect the resources while in the custody of the County.

III. Data Integrity

Data which is essential to critical County functions must be protected from loss, contamination, or destruction. The integrity of data, its source, its destination, and processes applied to it must be assured. Data must change only in authorized, predictable, and acceptable ways.

IV. Sensitive Information

Users who have access to sensitive information must insure they comply with the Information Resource Security Program, PPM #CW-O-059. Special procedures, such as data encryption, shall be implemented when required to ensure the security and confidentiality of non-public information transmitted over the network.

V. Security

Risks to information resources must be managed. Security needs must be considered and addressed in all phases of Enterprise Network development or acquisition. The expense of security safeguards must be appropriate to the value of the assets being protected, considering value to both the County and a potential intruder.

Security awareness and training of employees is one of the most effective means of reducing vulnerability to errors and fraud, and must be continually reinforced at all staff levels.

VI. Threat Management

A. Vulnerability Management

Computers, laptops, mobile devices, personal devices and other connected devices with access to the Palm Beach County Enterprise network are required to maintain up-to-date operating system revision levels to mitigate exploitable threats to the network and connected computers. Applying patches or changing configuration settings can often address computer operating system vulnerabilities. Operating system vulnerabilities can be exploited causing harm to a computer and corrupting sensitive data. Keeping computers in compliance with latest vendor software patch levels and best practice configurations will mitigate operating system vulnerabilities.

ISS will monitor the environment for deviations from the policy and to identify new vulnerabilities.

B. Anti-Malware Protection

Computers are vulnerable to malicious threats in the form of "malware." Malware can corrupt, hijack and manipulate protected data. A malware-infected computer can be used to attack other networked computers. Some forms of malware can send protected data to third parties intending to do harm. Computer based viruses can spread to networked computers and flood the network with harmful traffic that can cause system-wide network outages. Computers found to have malware infections can degrade the integrity of the Enterprise Network, infect surrounding computers and compromise critical data.

Computers must be protected at all times against such threats. Computers must have installed antivirus programs running the latest malware protection software. Antivirus programs must be configured to protect against the latest malware threats. To maintain the integrity of the Enterprise Network, malware infected computers must be immediately cleaned of all malware infections or risk removal off of the Enterprise Network.

C. Perimeter Network Security

The perimeter network is where the Palm Beach County internal private network interfaces with trusted agencies and the Internet. A "firewall" acts as perimeter defense and a checkpoint that provides safeguards between a trusted and untrusted network. Firewalls keep malicious threats from untrusted networks at bay while allowing authorized access to public and private data. Firewalls implicitly deny all non-authorized access.

Interconnections of the Enterprise Network to the Internet or extranet must pass through firewalls that inspect transactions and validate access to County resources based upon source, destination, port, and protocol.

All County business units needing access to remote agencies or access to the Internet will be protected by ISS-managed enterprise firewalls. Business units are not permitted to install independent firewalls. If a need is contemplated, then the business unit must create a Service Request System (SRS) work order for ISS to determine the appropriate measure, policy impact, authorization, and implementation. Similarly, firewall change requests will only be approved when a clear business requirement or impact has been determined and a risk analysis has been performed.

VII. Intellectual Property

The County shall support and uphold the legitimate proprietary interests of intellectual property holders. County personnel will observe information technology copyright laws. County personnel will not install any software, including but not limited to free, or trial

software without the explicit approval of the Chief Information Officer of ISS, or designee. will take appropriate action if unauthorized software is found on the Enterprise Network.

VIII. Electronic Mail

The use of electronic mail is an important method of information interchange. Messages, documents and files can be mailed worldwide using the Enterprise Network and its Internet gateway. The user must make special efforts to comply with County security requirements for sending sensitive information, copyrighted material, or any other information that is not authorized or in compliance with the Electronic Mail Privacy Electronics Commission Privacy Act (Public Law 99-508--OCT 21, 1986). Countywide PPM # CW-R-006 sets forth policies governing the use, retention, and destruction of electronic mail.

IX. Cost Recovery

Charges may be made for services provided on the Enterprise Network. Any charges will be consistent with Public Records Act and County Policy CW-F-002 Fees - Duplication of Public Records. Charges to user agencies will be determined based on the annual updates to the ISS Cost Allocation Plan.

RESPONSIBILITIES:

I. (ISS) Department

ISS is responsible for providing system connectivity and network services that are used for the benefit of the County. In this capacity, ISS will enforce methodologies and procedures to ensure public access and compliance with public records law, make public access available to unrestricted information, secure restricted information and protect the Enterprise Network from abuse and misuse.

Privileged administrative access accounts needed for internal or external audits, investigations, software development, software installations or other defined needs, shall be authorized by ISS, created with an expiration date, and disabled when no longer needed,

II. Management

The management of the business unit is responsible for insuring that each employee of the business unit be accountable for his or her actions relating to access to information resources. Management is also responsible for monitoring compliance with contracts and third party agreements.

III. Enterprise Network Users

Users of the Enterprise Network are responsible for being aware of and complying with all requirements governing access and use of the Enterprise Network.

IV. Remote Users, Telecommuters, and Mobile Users

The remote user and telecommuter will have the sole responsibility to back up the information in their remote system. It is strongly recommended that a backup of files be done at the end of each session.

Remote access to Palm Beach County information resources will be capable only through approved and encrypted remote access implementations to ensure the confidentiality and integrity of remote access sessions. ISS will monitor for unauthorized access and violations of usage restrictions.

County mobile communication devices approved by ISS to access Enterprise Network shall only use County-approved remote access applications or methods, and shall be compliant with established ISS technical standards and policies. Personally-owned mobile devices shall not be connected to the Enterprise Network unless approved by ISS.

V. Vendors

Vendors must ensure that IT systems and applications developed for the County conform to this and other applicable Enterprise Information Technology Policies, Standards, and Procedures. Non-conforming IT systems cannot be deployed unless the purchasing entity and their contractor have jointly applied for and received, in written notice from the ISS Director (CIO) or designee, that a specified exemption will be permitted.
Vendors shall only use Palm Beach County information and systems for the purpose of the business agreement. Any other information acquired by the third party in the course of the contract cannot be used for the third party's own purposes or divulged to others. Unless stipulated in the contract, a third party may not give access to or distribute Palm Beach County systems, information and data to another third party without permission by Palm Beach County.

PROCEDURES:

I. Network Access Authorization

Elected Public Officials and their staff, County Employees, Subscribers, Telecommuters, and Vendors will have access to the Enterprise Network. Access will be determined by each business unit or Elected Public Official.

A. An ISS System SRS work order will be completed for each individual request for network access.

B. ISS will set up accesses and permissions specified in the work order. Internet users will only be able to access the County web page through the Internet.

C. Users will be assigned a unique account and user ID. Credentials should not be shared or used by anyone but the individuals to whom they have been issued. Similarly, users shall be forbidden to perform any activity with user credentials

belonging to others.

D. Working with other business units, as necessary, ISS will identify all devices (including IoT) connecting to the County Enterprise Network. ISS will monitor access, traffic and priority of IoT devices.

II. Password Issuance and Modification

The first line of security is the user ID and password. Passwords should be unique and not include the user's or family member names, phone numbers, social security numbers or address. Users shall not reveal passwords to anyone.

A. The business unit systems administrator will issue initial user IDs and passwords.

B. The password should be periodically changed per the Information Resource Security Standards and Guidelines.

C. Should there be any suspicion that a password has been compromised, the password should be changed immediately.

III. Enterprise Network Access Methods

A. Virtual Private Network (VPN)

VPN is the preferred method of entry to the Enterprise Network. This method affords an acceptable level of security. It provides a central point of control, system administration and security threat monitoring.

ISS will provide the acceptable level of security in compliance with the Information Resource Security Program Policies PPM CW-O-059 and the Records Management Program PPM CW-R-005.

B. Outbound VPN Access

Outbound VPN will be used in strict compliance with the Information Resource Security Standards and Guidelines.

1. The use of a VPN to gain access to resources that are outside of the Enterprise Network will be authorized for County employees when required to perform their job requirements.

2. If access of this type is required, the methodology and security procedures shall be approved by ISS.

C. Kiosk Access

Palm Beach County may provide kiosk access to certain information. This service provides specific information via a terminal that is typically connected directly to the Enterprise Network.

1. The systems will be designed to provide the information specified with an acceptable level of system security.

2. The menus and ability for information access will be locked down to only allow pertinent kiosk required information.

D. Computer Telephony Integration (CTI)

CTI represents another method of public access to the Enterprise Network. CTI can be used to provide Integrated Voice Response applications for use in providing information to the public.

1. CTI applications will be developed with network security as part of the design elements.

2. CTI projects will be developed in compliance with the Information Resource Security Standards and Guidelines.

E. Wireless Network Access

Wireless networks are accessed using radio wave transmission systems. Private data traveling through radio waves can be picked up through malicious scanning techniques and be used to gain access to data and the Enterprise Network.

1. Wireless devices accessing the Enterprise Network will be configured to use encryption and authentication services specified by ISS.

2. ISS will monitor for unauthorized wireless connections.

3. ISS will scan for an unauthorized wireless access points and take appropriate action if an unauthorized connection is discovered.

IV. Addressing Policy Violations

A. Any suspected attempts or violations of this policy shall be reported to the CIO or designee and the business unit manager.

B. Policy violations will be handled in accordance with the Information Resource Security Standards and Guidelines.

V. Dissemination of Enterprise Network Access Information

Pertinent information which explains in detail the methodology to access the Enterprise Network and the Internet services offered by Palm Beach County will be posted on the home page of the Palm Beach County Intranet.

VERDENIA C. BAKER
COUNTY ADMINISTRATOR

Supersession History:
1. PPM # CW-O-061, effective 1/19/1996
2. PPM # CW-O-061,effective 10/2/2012

EXHIBIT A

DEFINITIONS

1. Business Unit

   An agency, department, division group, unit or organization under the control of the Board of County Commissioners or Elected County Officials.

2. Computer Telephony Integration (CTI)

   The technology to integrate the computer to the telephone to create integrated telephone and computer applications.

3. Elected County Officials and Staff

   Elected Constitutional Officers such as the Tax Collector, Property Appraisers, etc., whose employees have access to the Enterprise Network.

4. Enterprise Network

   "Enterprise Network" refers to the Palm Beach County network managed and maintained by the Network Services Division of the Information Systems Services (ISS) Department.

5. Inbound Access

   Access to the Palm Beach County network from a remote location using a virtual private network (VPN), modem or firewall controlled access.

6. Internet of Things (IoT)

   The network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment.

7. Kiosk

   A network workstation that is configured for the public to access information available on the Enterprise Network.

8. Malware

   Short name for "malicious software." Malware includes computer viruses, worms, Trojan horses, spyware, adware, scareware, crimeware, rootkits and other malicious unwanted software or programs.

EXHIBIT A

DEFINITIONS

9. Modem

A device that can be attached to a computer to encode digital information through an analog carrier signal such as a telephone line.

10. Network

A collection of hardware components and computers interconnected by communication channels that allow sharing of resources and information.

11. Network Card

A hardware component that connects a device to a computer network. Also known as network interface card or network adapter.

12. PC

Abbreviation for "personal computer".

13. Outbound Access

Connecting to a remote network or computer from a PC that is connected to the Enterprise Network.

14. Public Access

The process used by the public to connect to the Enterprise Network from a remote location, PC or kiosk.

15. Remote Access

The process of connecting to the Enterprise Network from an untrusted network.

16. Remote Location

Any location that is not a part of the Enterprise Network.

17. Subscriber

An authorized individual, organization, corporation or entity that has subscribed to a service offered by Palm Beach County.

EXHIBIT A

DEFINITIONS

18. Telecommuter

An authorized individual that is granted access to connect to the Enterprise Network that is connecting from a remote location.

19. Vendor

An Individual or business that has a contractual agreement with the County to provide goods or services to the County.

20. Wireless Network

Network communications that are implemented and administrated using radio wave transmissions.

21. Virtual Private Network (VPN)

A computer network that uses a public telecommunication infrastructure such as the Internet to provide remote offices or individual users with secure access to their organization's network.