

Policy & Standards Introduction and Index

It is the intent of the West Feliciana Parish Police Jury Department of Information Technology to develop formal I.T. policies relative to information technology activities including but not limited to the following:

1. Implementing of I.T. standards for hardware, software, and consolidation of services.
2. Reviewing and coordinating I.T. planning, procurement and budgeting.
3. Providing oversight for centralization/consolidation of technology initiatives and the sharing of I.T. resources.
4. Assuring compatibility and connectivity of West Feliciana's information systems.
5. Providing oversight on I.T. projects and systems for compliance with parish wide strategies, goals, and standards.

This office is reviewing the content and format of all IT Policies and Standards. Updated versions are being published using a new number scheme. The official method of publishing/distributing IT policies will be via the parish website and the Laserfiche document management system.

Management/Governance Policies

IT_POL_0-00 Cellular Phone Utilization
IT_POL_0-01 Enterprise Shared Services
IT_POL_0-02 Enterprise Governance

Security Policies

IT_POL_1-00 Enterprise Security
IT_POL_1-01 Data Sanitization
IT_POL_1-02 Authentication
IT_POL_1-03 Authorized Access
IT_POL_1-04 Simultaneous Connections
IT_POL_1-05 Antivirus
IT_POL_1-06 Disaster Recovery
IT_POL_1-07 Remote Access
IT_POL_1-08 Acceptable Use
IT_POL_1-09 Data in Transit
IT_POL_1-10 Data capable phones

Computing Infrastructure Policies

IT_POL_5-00 Enterprise Data Centers

General Policies

IT_POL_4-00 Parish Secure Intranet and IP Addressing
IT_POL_6-00 Desktop Management
IT_POL_9-00 Retention of Imaged Records

Standards

IT_STD_0-00 Record Classification
IT_STD_1-00 Data Sanitization Guidelines

IT Policy and Standards Numbering

Historically, policies and standards were numbered sequentially, with no relationship between the numbers and subject areas. To address this perceived weakness and to minimize confusion between historical policies and new or revised ones, and to allow for future expansion, the following procedure is suggested.

All new policies shall be numbered “IT POL x-yy” where x is the prefix assigned to a broad area of standards (e.g., Security) and the yy is a number assigned with that series. The use of a dash (-) within the number provides a cue that the policy is one within a with a broader area of concern, and that it is a new or revised policy, rather than a historical one. Similarly, all standards will be in the form “IT STD x-yy”, with the x and yy as defined previously.

Range	Broad areas	Description and examples
0-00	Management / Governance	Policies and standards that are high-level or broadly applicable to multiple areas of information technology. Does not include the separate broad areas of security (1-00) or budget/fiscal (2-00). Examples: Acceptable use, customer satisfaction
1-00	Security	Policies/standards that promote confidentiality, integrity, availability of information and systems. Examples: Business continuity, authentication, passwords
2-00	Budget & Fiscal	The planning, budgeting, planning, cost allocation, accountability, reporting, and audit of resources. Does not include the actual procurement of goods or services (see 3-00). Examples: operational plans.
3-00	Procurement	How to acquire goods and services. Examples: ITB, RFP, other means.
4-00	Network	Voice, data, video transmission and services. Examples: Protocols, naming, PSI.
5-00	Computing Infrastructure	The basic hardware, software, equipment and environment needed to operate enterprise IT. Does not include customer desktops. Examples: Servers, operating facilities,
6-00	Desktop	The hardware, software and processes used locally by a customer. Examples: Hardware specs, office suite
7-00	Services	Those back-office applications and enabling services that are built upon the network/computing infrastructure and provide a foundation for business applications. Examples: E-mail, web, monitoring, directory, help desk
8-00	Applications	Line of business (front-office) applications used by agency personnel to conduct Parish business, whether acquired, rented, or developed internally. Examples: MIP, BluePrince, CSDC.
9-00	Data / Information	Storing, retrieving, management, and archiving of data. Example: Record retention

Cellular Phone Utilization and Reimbursement of Parish Issued and Employee Owned Cell Phones

POLICY:

PARISH ISSUED CELL PHONE

It shall be the policy of the West Feliciana Parish Police Jury that all requests for parish issued cellular phones be authorized by the department superintendant and approved by the parish manager, and that utilization shall be in compliance with the guidelines and procedures established in this policy including:

- A. **Personal telephone calls, incoming and outgoing, shall be limited in number and length**
(Ref: Personnel Policy & Procedures Manual 8.15.1), and
- B. Personal calls must be reimbursed with a check made payable to the West Feliciana Parish Police Jury using the following guidelines:
 - 1. In the event total minutes utilized exceeds the plan limit, reimbursement shall be based on personal call utilization up to but not greater than the cost of the minutes that exceed the plan
(i.e. your plan calls for 300 minutes – you incur 350 minutes of total utilization – you had 55 minutes of personal utilization – your reimbursement responsibility will be 50 minutes at the plan per minute charge). **Note:** No reimbursement is required when total plan minutes are not exceeded.
 - 2. Any assistance, roaming charges, or other miscellaneous charges which are not clearly business related.
- C. **The user of a parish issued cellular telephone should have no expectation that any communication made on the device is private.**

EMPLOYEE OWNED CELL PHONE

It shall be the policy of the West Feliciana Parish Police Jury that all requests for reimbursement of cellular phone billings be authorized by the department superintendant, and that utilization shall be in compliance with the guidelines and procedures established in the policy including:

- A. Cellular calls for which reimbursement will be claimed during work hours must be limited to parish business,
- B. The length of the conversation should be limited, reasonable and necessary, and
- C. Reimbursement for business calls from an employee's personal cellular phone shall be made in the following manner:

An average cost per minute will be calculated and applied to the number of business call minutes. For example, if the total monthly cost is \$53.34 and the total minutes used was 400, then the average cost per minute would be \$0.13, or $\$53.34/400$. If the total business minutes were 95, the employee would be due \$12.35, or $95 \times \$0.13$.

Employee requests for reimbursement shall be made in writing and a copy of the cellular phone bill indicating the business minutes to be reimbursed must be attached.

SCOPE:

The West Feliciana Parish Police Jury understands that due to the nature of job responsibilities of certain employees, it is necessary to have a cellular phone policy which covers utilization of parish issued cellular phones and which also allows employees to utilize their personally owned devices for business dictated purposes when necessary.

This policy shall be applicable to all employees in all sections of the West Feliciana Parish Police Jury, both general and ancillary appropriations, which shall include Police Jurors. This policy shall supersede and replace any previous or existing Police Jury policy or procedure covering parish issued or personally owned cell phones and their use as presented herein.

RESPONSIBILITY:

Parish Manager is responsible for: Approving all Parish issued cellular phone requests.

Parish Manager is responsible for:

Holding department superintendants under their supervision accountable for adhering to all aspects of this policy.

Department Superintendants are responsible for:

Authorizing their respective department's request for parish issued cellular phones and forwarding those requests to the Parish Manager for approval.

Providing a copy of the monthly bill for each parish issued cellular phone to each respective user in the department, and assuring that:

- a. Each employee has reviewed and signed their respective bill acknowledging the amount of personal costs due,
- b. A check for reimbursable personal costs is attached to the reviewed bill,
- c. Signing each bill after all employees have completed their review.

Assuring that the reviewed bills and any checks are forwarded to the Parish Treasurer.

Periodically reviewing the cellular plan to be sure that the most cost effective plan is being utilized for the employee's business needs.

Determining whether calls made on an employee's personally owned device was actually business related.

Reviewing and approving employee reimbursement requests for calls made on the employee's personally owned device.

Making sure that each employee under his/her supervision is:

Providing for formal review of this policy with all affected employees on a cyclical basis.

EMPLOYEES are responsible for: Complying with all aspects of this policy.

- a. Made aware of this policy and its contents as well as any forthcoming revisions,
- b. Informed that he/she must abide by the terms of this policy as a condition of employment, and
- c. Informed of the consequences of violation of this policy.

Parish Treasurer is responsible for:

Providing the departments with copies of their respective cellular phone bills.

Maintaining the bills with the acknowledgements received from the departments in accordance

with the Jury document retention schedule.

Immediately depositing into the Parish account, checks received from employees for personal cellular phone usage.

QUESTIONS:

Questions regarding this policy should be directed to the Department Superintendent, the Parish Treasurer, or the Parish Manager.

VIOLATIONS:

Employees found to have violated this policy may be subject to disciplinary action in accordance with the personnel policy and procedures manual.

Related Policies, Standards, Guidelines: [IT POL 0-01](#) Enterprise Shared Services, [IT POL 1-10](#) Use of Smartphone

Devices when Accessing Parish Networks

IT POL 0-01

Enterprise Shared Services

Policy:

The Chief Information Officer, through the Information Systems Department, shall oversee and coordinate the definition, projection, procurement, provision, and management of shared information technology services, where it is determined to be in the best interest of the Parish. This may include applications, supporting services, and technical infrastructure.

Scope:

All entities under the authority of the West Feliciana Parish Police Jury, must comply with this policy which includes all departments, boards and commissions, unless otherwise superseded by specific legislation, executive order, or Jury policy.

Responsibilities:

The CIO shall define the overall framework or criteria for identifying and evaluating those services which are shared or agency-specific. Applying sound business practices and design principles, the objective is to provide sound foundational and enterprise services that will allow Departments to focus on their department lines of business.

The Information Systems Department (ISD) shall define those applications and information technology services that are best managed as shared service offerings to entities within the parish.

Designation of a service as an enterprise shared service may include the following criteria:

- Where services support business functions and data that cross departmental boundaries
- Where a shared service is more cost-effective
- Where the shared service facilitates the transfer of information or worker knowledge
- Where consistent qualities of service are required
- Where a shared service is foundational to other needed shared services
- Where a common approach is mandated by competent authority or best practices.

Where possible, services shall be open and standards-based, maximizing the benefits of volume buying, life cycle replacement, interoperability and training.

Stand-alone agency implementation of such services shall migrate to the equivalent shared services, unless otherwise exempted.

The overall responsibility for the projection, fiscal and operational management, and tracking of such services shall be as defined in the ISD Enterprise Governance policy and as further defined in the specific policy governing the shared service.

Related Policies, Standards, Guidelines:

IT POL 0-04 Enterprise Governance

Owner: WFPPJ ISD

Effective Date: 8/10/2010

IT POL 0-02

Enterprise Governance

Policy:

The applications, data, and other information technology resources belonging to the Parish shall be managed in a way that balances central oversight with agency management. As the stewards of taxpayer assets, the responsibility for managing IT resources should be allocated in ways that maximize the results and accountability of the various stakeholders. The objective is to optimize usage of IT resources while providing for agency management of business processes and data.

Scope:

All entities under the authority of the West Feliciana Parish Police Jury, must comply with this policy which includes all departments, boards and commissions unless otherwise superseded by specific legislation, executive order, or Jury policy.

Responsibilities:

The overall responsibility for information technology can be allocated among the agency users, the service providers and the central oversight as follows:

The Police Jury Information Systems Department (ISD) shall define the framework for IT governance, the information technology master plan, and the proposed policies, procedures and service architecture. In conjunction with the Accounting office and other central authorities, ISD reviews requests for resources, services, and the overall performance and cost effectiveness of the solutions requested and obtained. ISD may also designate service providers and define their scope of operation.

The departments, make the business decisions, project the needed resources, prepare the service requests and manage the use of IT services within their department, including the monitoring and management of user demand.

The service providers track the industry forecasts, emerging technology and best practices, and on the basis of customer projections, develop lines of service, project the aggregate usage, and publish budget rates within the confines of applicable cost recovery guidelines. The providers procure the needed resources and tools to ensure the availability of services at the mandated levels of quality and quantity, while providing customers with the tools needed to review usage.

Related Policies, Standards, Guidelines:

IT POL 0-01 *Enterprise Shared Services*

Owner: WFPPJ

Effective Date: 8/11/2010

IT POL 1-00

Enterprise Information Security Policy

Policy:

Responsibility and authority for information management shall be established and maintained by each Parish Agency. The Department's Chief Executive Officer / Secretary or equivalent is designated as the owner of that Department's information and as such must practice due care and due diligence to ensure the confidentiality, integrity and availability of that information. Although this responsibility is often delegated to lower level management, this individual is also responsible for ensuring that all aspects of the organization's planning, development, classification and operation comply with applicable enterprise policies and standards.

Scope:

All entities under the authority of the Information Systems Department, must comply with this policy, which includes all departments, boards, and commissions.

Responsibilities:

Each Parish department is responsible for the following:

- Classification of computer data
- Confidentiality, integrity and availability of computer data
- Access controls that are appropriate for the level of data classification
- Developing, maintaining and regular testing of a disaster recovery/business continuation plan
- Employee awareness training relative to information security
- Assigning responsibilities to implement this policy

Related Policies, Standards, Guidelines:

IT STD 0-00 Record Classification

Owner: WFPPJ ISD

Effective Date: 7/1/2010

IT POL 1-01

Data Sanitization

Policy: Magnetic storage devices, optical storage media and non-volatile memory devices that are surplus, transferred to another government entity or subject to destruction, must use a method of data sanitization compliant with the IT STD 1-00 Data Sanitization Guideline, if the data is determined by the owner to be security-sensitive.

Scope: All entities under the authority of the Information Systems Department must comply with this policy.

Responsibilities:

- Departments must establish policies and procedures to ensure compliance with this policy.
- Departments must adhere to the license terms and agreement for software on a computer that is being transferred to another agency or surplus.
- Departments should conduct periodic checks to determine their method of sanitization is working correctly.
- Departments must maintain records indicating the method of data sanitization utilized when personal computers are surplus or transferred to another agency.

Related Policies, Standards, Guidelines: IT STD 1-00 Data Sanitization Guideline, IT STD 0-00 Data Classification Guideline

Owner: WFPPJ ISD

Effective Date:
7/1/2010

IT POL 1-02

Authentication

Policy:

Departments must use at least one of the following methods of authentication when accessing or utilizing Parish-owned or managed information technology systems:

- Passwords (IT STD 1-01)
- Biometrics (IT STD 1-02)
- Security Tokens (IT STD 1-03)
- Public Key Infrastructure (PKI) (IT STD 1-04)

Scope: All Departments and entities under the authority of the Information Systems Department must comply with this policy.

Responsibilities:

Departments are responsible for developing policies governing the authentication requirements detailed in this policy and the supporting technical standards.

Related Policies, Standards, Guidelines:

IT STD 1-01, IT STD 1-02, IT STD 1-03, and IT STD 1-04

Owner: WFPPJ ISD

Effective Date:

7/1/2010

IT POL 1-03

Authorized Access and Use of Information Technology Systems

Policy: Only authorized personnel will have access to the Parish's information technology systems. Use of the Parish's IT systems must be for official business only. Any other access or use of these systems is prohibited.

Scope: All entities under the authority of the Information Systems Department must comply with this policy.

Responsibilities: Departments must establish policies and procedures to:

- Ensure compliance with applicable statutes, regulations, and mandates regarding the management of information technology systems.
- Establish prudent and acceptable practices regarding the use of information technology systems, including but not limited to, unauthorized deletion and/or modification of data, disruption of IT systems, and unauthorized viewing and use of sensitive personal identification data such as social security number, date of birth, phone number, and home address.
- Educate individuals who may use information technology systems with respect to their responsibilities associated with such use.
- Report any vulnerability or breach in computer security, any incidents of possible misuse or violation of information technology systems security to the appropriate security personnel within the agency.

Departments must establish controls to prevent users of information technology systems from:

- Accessing any data or programs contained on agency systems for which they do not have authorization or explicit consent.
- Sharing their account(s), passwords, Personal Identification Numbers (PIN), Security Tokens (e.g., smart cards), or similar information or devices used for identification and authentication purposes.
- Making unauthorized copies of copyrighted software.
- Downloading, installing or running security programs or utilities that reveal or exploit weaknesses in the security of an information technology system. Department network security personnel are exempt from this requirement.

Owner: WFPPJ ISD

Effective Date: 7/1/2010

IT POL 1-04

Simultaneous Network Connections

Policy: Computer systems connected to department networks must not be simultaneously connected to any other network outside of the agency's control, and beyond the scope of normal business, via a modem, another network interface. This includes but is not limited to; wireless connections and connections to DSL or Cable modems or a Virtual Private Network (VPN) connection.

Scope: This policy applies to all entities under the authority of the Information Systems Department. Departments in compliance with this policy will prevent employees from establishing network connections that may jeopardize the security of internal networks and network assets

Responsibilities: Departments must establish policies and procedures to:

- Provide awareness training to user base in order to prevent exposure through simultaneous connections to un-trusted networks.
- Scan agency's premises for rogue wireless access points.
- Ensure all internal/external modem hardware is removed from network-attached desktop computers.
- Prohibit the installation and use of modem hardware in network-attached desktop computers.
- Periodically verify compliance with this policy.

Owner: WFPPJ ISD

Effective Date:

7/1/2010

IT POL 1-05

Anti-virus / Anti-spyware Software

Policy: Agencies must have an active anti-virus and anti-spyware solution enabled on their networks. This solution may be either software or hardware based, but must be able to scan servers, personal computers, notebooks/laptops, incoming email and email attachments, and traffic coming in and out of the agency's network.

Scope: This policy applies to all Parish-owned computing devices (gateways, servers, personal computers) under the authority of the Information Systems Department.

Responsibilities:

Agencies are required to develop policies and procedures that ensure the following:

- Anti-virus software updates are applied when made available by the vendor.
- Scheduled anti-virus system scans for desktops occur daily during the work week.
- Scheduled anti-virus system scans for servers are determined by the agency, based on its respective environment.
- Non-Parish-owned computing devices (home user and contractor PC's) attached to the agency's internal network utilize anti-virus software with the current updates.

Owner: WFPPJ ISD

Effective Date:

7/1/2010

IT POL 1-06

Disaster Recovery / business Continuity Planning Policy

Policy: Departments must develop, test and maintain disaster recovery/business continuity plans designed to ensure the availability of mission-critical services and functions in the event of a disaster or unscheduled event that impacts the department's information technology or telecommunications systems.

Scope: This policy is applicable to all entities under the authority of the Information Systems Department, which provide mission-critical services to the public, local government, federal or state government and other Parish Departments.

Responsibilities: Departments are required to develop and regularly update disaster recovery/ business continuity plans using the guidelines noted below. Additionally, an electronic copy of the most recent DR/BCP must be submitted to the WFPPJ ISD annually.

- Business Impact Analysis -Conduct risk assessment and document the potential impacts of likely event to the agency. With each risk, an analysis of the likelihood of event should be determined and prioritized in such a manner so that methods of mitigation can be explored. Understand the effect that a business interruption will have on the agency's ability to deliver services. Long and short term interruptions should be considered in this analysis. A worst case event should be assumed and agency business process alternate procedures and established recovery time objectives determined, and recovery priority organized by criticality.
- Develop an agency Disaster Recovery/ Business Continuity Plan (DR/BCP) – Develop a DR/BCP based on accepted industry best practices. The plan should be created to support the department's business objectives and priorities
- Testing and Updating the Plan -Plans must be tested to verify they are effective. Regular updates to the plans are necessary to keep information and processes accurate.
- Management of the Plan -Department leadership sponsors and supports the plan. Responsibilities for the plan will be distributed across the department organization and require support from all levels of management

Owner: WFPPJ ISD

Related Policies, Standards, Guidelines:

Effective Date:

7/1/2010

IT POL 1-07

Remote Access to Internal Networks

Policy: Departments that allow remote access to their internal networks via desktop PC's and laptops must ensure these devices are configured as indicated by IT STD 1-5.

Scope: This policy is applicable to all entities under the authority of the Information Systems Department.

Responsibilities:

- Departments are required to develop policies and procedures that address the requirements of this policy.
- Network capable/PDA devices and "smart phones," due to their fast-paced technological advances, are not within the scope of this policy. However, Departments must assess and take the necessary steps to mitigate the security risks associated with these devices.
- Relative to development and support contracts, Departments are required to include specific contract language that requires the contractor to adhere to ISD Security Policies and Standards if there is need for remote access to the agency's internal network.
- Where applicable, Departments are required to utilize existing enterprise standards.
- Departments should pursue the use of "health-check" software that determines the status (whether or not anti-virus and firewall software are loaded with the latest updates) of remote PC's and laptops before they are allowed access to the internal network.
- Departments should develop an implementation plan detailing the steps required to become compliant with this policy.
- Where possible, Departments should plan to migrate from direct-dial access to broadband connectivity.

Related Policies, Standards, Guidelines: IT STD1-5 Remote Access to Internal Networks

Owner: WFPPJ ISD

Effective Date:
7/1/2010

IT-POL 1-08

Acceptable Internet / Email use

Policy: Internet access and email facilitate the parish in meeting its business needs. Internet access and email are considered parish property and the parish has the right to monitor all use of such property at its discretion. With the exception of information protected by federal/state/parish statutes and agency policies, users should have no expectation of privacy as to their Internet and email usage via parish computers and networks.

The purpose of Internet and email use is to conduct official parish business. Agencies may determine availability of Internet and e-mail services based on employee need and use which are not in conflict with the law.

Users may not download, store, transmit, or display any kind of image or document using any department system or resource that violates federal, state, or local laws and regulations, executive orders, or that violates any Parish or department adopted policies, procedures, standards, or guidelines.

Acceptable use must be legal, ethical, and respectful of intellectual property, ownership of data, systems security mechanisms, and individual rights to privacy and freedom from intimidation, harassment and annoyance. Users must be held accountable for any breaches of policy, security, or confidentiality resulting from their use of Internet or email. An abuse of the privilege of Internet or email use may result in disciplinary action as deemed appropriate by supervising authorities.

Use of the Internet and email as described below is acceptable:

- To provide and facilitate official parish business (intra-agency, parish and state or federal agencies and business partners of parish agencies).
- To use for professional society, university association, government advisory, or standards activities related to the user's employment-related professional/vocational discipline.
- Other uses not in violation of this policy that may be allowed or required by individual department or agency policy.

Scope: All entities under the authority of the West Feliciana Parish Police Jury.

Responsibilities:

- Agencies must develop policies or update existing policies to ensure compliance with the provisions of this policy.
- Each agency is responsible for the activity of its users and must familiarize each user with what is considered appropriate use of Parish-provided Internet and email access.
- Should a conflict arise between an agency's use agreement and this "Acceptable Internet/E-mail Use Policy", the more restrictive policy shall take precedence.

Owner: WFPPJ ISD

Effective Date: 7/1/2010

IT POL 1-09

Data in Transit

Policy:

All sensitive data that are removed from the Parish premises must be encrypted consistent with IT STD 1-6 *Encryption*. This includes both data on agency approved portable storage devices (notebook PCs, USB drives, mini/micro solid Parish disks, CDs, DVDs, diskettes, PDAs, tapes etc.) and data being transferred through network protocols (ssh, https, sftp, etc).

Sensitive data includes: sensitive, proprietary and other data not subject to the Louisiana Public Records Act (LA. RS 44:1 et seq.).

Scope:

All entities under the authority of the Information Systems Department.

Responsibilities:

- Departments must document a business case to support employees or contractors taking sensitive data off Parish premises.
- Departments must make reasonable assurances that only agency approved storage devices will be used if employees or contractors are allowed to take sensitive data off Parish premises.
- Departments must make reasonable assurances that employees subject to this policy are aware of the proper techniques regarding use of encryption on the devices and protocols referenced above.
- Departments must make reasonable assurances that contractors utilize encryption consistent with IT STD 1-6 when taking sensitive data off Parish premises.
- Departments must provide the IT Department with an electronic copy of their deployment plan relative to becoming compliant with this policy.

Related Policies, Standards, Guidelines:

IT STD 1-6 Encryption IT STD 1-7 Approved Storage Devices

Owner: WFPPJ ISD

Effective Date:

7/1/2010

IT POL 1-10

Use of Smartphone Devices when Accessing Parish Networks

Policy: Smartphone devices that are used to access Parish email and/or networks, but not including devices that only access email through a web based interface, must have the following security measures enabled: a minimum of a 4 digit PIN is required to access the device; a Group Policy or setting that is pushed down from the email server or wireless enterprise server, which after ten failed login attempts to the device will initiate a complete data wipe ensuring all Parish data is removed.

A smart phone device includes but is not limited to the following: a personal digital assistant (PDA), a RIM BlackBerry, an Apple iPhone, Windows mobile devices, a Nokia N-Series or any other handheld mobile device with email and web browsing capabilities.

This policy applies to both Parish owned devices and privately-owned devices that are used to access data owned by the Parish, including email.

Scope: All entities under the authority of the Information Systems Department must comply with this policy.

Responsibilities: All entities that maintain an email server will ensure that the proper settings are enabled on all smart phone devices connecting to their mail server. This can be accomplished by, but not limited to, pushing down a Group Policy from the email/wireless enterprise server to devices establishing connections to these servers.

Owner: WFPPJ ISD

Effective Date: 7/1/2010

IT POL 4-00

Parish Secure Intranet/Internet (PSI) Addressing

Purpose:

To maximize the use of local and wide area networks (LAN, WAN) as well as telecommunications systems within the parish government. ISD has created/established the Parish Secure Intranet (PSI) for intra- interagency communications and internet access. In assigning IP address space to end users, ISD takes guidance from assignment policies and procedures set forth in Request For Comments (RFC) repository maintained by the Internet Engineering Task Force (IETF) Secretariat. These guidelines were developed to meet the needs of the larger Internet community in conserving scarce IPv4 address space and allowing continued use of existing Internet routing technologies. In order to standardize the Parish wide IP addressing scheme and apply conservation of IP address space where appropriate ISD follows:

- VSLM (Variable Length Subnet Mask) RFC 2050
- Private / Reserved Addresses RFC 1918
- NAT (Network Address Translation) RFC 1631
- DHCP (Dynamic Host Configuration Protocol) RFC 2131.

RFC'S can be referenced at this site <http://www.ietf.org/rfc.html>

Policy:

Departments participating in the PSI are required to comply with the internet protocol (IP) addressing scheme established by ISD.

Scope:

This policy mandates that all Parish entities participating in the PSI shall participate in a scheme for IP addressing that will ensure internet access while using unique IP addresses within the PSI and the Parish wide DMZ.

Responsibilities:

ISD shall assign each agency a subnet appropriate to the agency size from the RFC 1918 10.xxx.xxx.xxx IP address space to support agency users and network devices inside the PSI. The assigned address space shall be large enough to accommodate the agency's current and anticipated IP devices.

ISD shall assign each agency a public IP subnet appropriate to the agency size to support agency's public access servers located within the DMZ. The assigned address space shall be large enough to accommodate the agency's current and anticipated IP devices.

ISD shall assign each agency a public IP subnet from its pool of Parish wide public IP addresses for private to public IP address mapping for network devices inside the PSI. Once an agency is moved to the inside of the PSI, all public IP addresses delegated to that agency by the InterNIC or American Registry of Internet Numbers (ARIN) shall become part of the pool of Parish wide public IP addresses to be used at ISD's discretion.

ISD shall provide Network Address Translation (NAT) and Public Address Translation (PAT) at the ISD-managed firewalls for mapping of private to public IP addresses. NAT will be implemented using a public to private address ratio appropriate to the needs of each agency, with the goal being to minimize the use of PAT.

Departments are required to coordinate with ISD and develop a transition plan that addresses the new IP scheme assigned by ISD.

Owner: WFPPJ ISD

Effective Date: 7/1/2010

IT POL 5-00

Enterprise Data Centers

Policy:

The Parish shall manage the provision of enterprise data centers to be used by all departments within the Police Jury. The Information Systems Department shall define the standards for enterprise data centers and shall designate those centers that are approved for use by Departments.

Enterprise data centers shall be used to house all computing equipment that:

- 1 Supports mission critical applications, or
- 2 Must be available outside of a normal Monday-Friday, 8 a.m.-5 p.m. timeframe, or
- 3 Requires high system availability, or
- 4 Requires a secure environment, or
- 5 Supports applications accessed by users who work outside of the facility containing the equipment, or
- 6 Requires raised flooring, special air conditioning for humidity and temperature control, or conditioned power supported by an uninterruptible power subsystem.

Scope:

This policy is applicable to all entities under the authority of the Information Systems Department, unless exempted in writing by the Chief Information Officer.

Equipment that should be housed in a designated enterprise data center includes:

- Server systems
- Server storage subsystems
- Server tape or other type of backup subsystems
- Storage Area Networks (SAN)
- Mid-range systems, including storage and tape subsystems
- • Mission-critical production servers
 - ○ Web servers (Public access/Enterprise)
 - ○ Application servers (System servers, such as DNS, e-mail, database, gateways, remote dialup, backup, system management)
- • Network support equipment
 - ○ Front-end processors
 - ○ Firewalls
 - ○ Virtual Private Network (VPN)
 - ○ Network management servers
 - ○ DHCP servers
 - ○ Routers, hubs, switches (in support of WAN for agency)

Components that may be housed outside of an enterprise data center include:

- Local file and print servers
- Non-production servers
- Development/Intranet servers that are not accessed by remote users
- Scanning/imaging equipment (agency discretion)
- Printers
- Post-processing equipment

Responsibilities:

The IS department will assist departments in determining what equipment may remain outside the enterprise data centers and in planning to relocate items that are candidates for the enterprise data centers.

Related Policies, Standards, Guidelines:

IT POL 0-01 *Enterprise Shared Services* IT POL

0-02 *Enterprise Governance*

Owner: WFPPJ ISD

Effective Date: December 20, 2009

IT POL 6-00

Desktop Management

Purpose:

The utilization of desktop power management will result in energy savings for the parish. Securing the desktop will result in fewer PC support requests (help desk calls, PC support staff assistance), enhance network security and facilitate standardization.

Policy:

1. *Power Management* - A reduction in desktop energy consumption can occur by user intervention and the utilization of power management features within the operating system.

- a) Departments must require users to logoff and power down desktop personal computers (system units, monitors, direct attached printers, scanners, external drives, speakers and other peripheral equipment) at the end of the work week (usually each Friday). The parish IT Director may grant exemptions, based on job function on a case-by-case basis.
- b) Departments must configure all desktop PC's to utilize the power management features of the operating system that place the monitor and hard disk drive in a "sleep" mode after a period of inactivity no greater than sixty (60) minutes

2. *Secure the Desktop* - Departments are required to disable administrative privileges (lockdown) on all user PCs, preventing unauthorized changes to PC configurations and the loading of unauthorized software. The parish IT Director may grant exemptions, based on job function on a case-by-case basis.

Scope:

Departments under the authority of the Information Systems Department should develop policies that are specific to their environment to ensure compliance with this policy.

Responsibilities:

Each agency must develop a transition plan to ensure that all desktop PCs in its inventory are configured to utilize power management and desktop lockdown as specified in items *1B* and *2* of this policy.

Departments are required to determine which applications, if any are not compatible with the operating system power management feature. Desktop PCs using applications that meet this criterion will be exempt from item *1B* of this policy.

Owner: WFPPJ ISD

Effective Date: 7/1/2010

IT POL 9-00

Retention of Imaged Records

Purpose:

The purpose of this policy is to establish retention schedules for records stored and managed by imaging systems.

Policy:

A retention schedule approved by the custodian of records must be in place for the records series contained in any imaging system.

Scope:

Any Parish department requesting IT funds for maintenance, migration or establishment of an existing or new imaging application, requiring ISD approval, under the authority of the ISD must have a retention schedule approved by the custodian of records in place for the records series contained in the existing application or intended to be placed in a new imaging system. Any system request without a retention schedule approved by the custodian of records will not be considered for approval.

Responsibilities:

The department shall contact the custodian of records to ensure that the records contained in their current or proposed system are included on their department's retention schedule approved by the custodian of records.

Contact the department custodian of records for additional information on record retention.

Owner: WFPPJ ISD

Effective Date: 7/1/2010

IT STD 0-00

Record Classification

Purpose:

The purpose of this standard is to establish an enterprise definition of the classification for records stored and managed by all police jury entities, boards and departments.

Scope: This policy applies to all entities under the authority of the West Feliciana Parish Police Jury.

Responsibilities: Departments, boards and other entities must establish policies and procedures to ensure compliance with this standard.

Standard: Data Classification Guideline

CONFIDENTIAL / SENSITIVE – This information if released could potentially cause harm to a person, an agency or the parish. The information is CONFIDENTIAL / SENSITIVE if protected by one or more of the following: department policy, State policy, Local law, State law or Federal law.

INTERNAL– This is information intended for use within the department, board or other entity. An accidental release of this information will not cause harm to a person, an agency or the State.

PUBLIC – This is information specifically prepared and formatted for consumption by the general public.

The above classifications should be utilized for existing data and new data that is created internally or received from an external source.

The methods used in protecting data, as described in associated policies, shall address not only the storage of the data but also the transport of the data to other systems and the delivery / display of the information to a workstation.

Related Policies, Standards, Guidelines:

IT POL 1-01, 1-02, 1-00, 1-07, 1-09

IT STD 1-01,1-02,1-03,1-04,1-05,1-06,1-07

Owner: WFPPJ ISD

Effective Date:

7/1/2010

IT STD 1-00

Data Sanitization Guidelines

Purpose:

The purpose of this Guideline is to provide instructions on proper sanitization of data in both electronic and paper form. This Guideline also provides instruction on secure disposal of electronic storage media.

Scope: All entities under the authority of the Information Systems Department must comply with this policy.

Definitions: The National Institute of Standards and Technology (“NIST”) has defined four methods of data sanitization in NIST Special Publication [800-88](#), Guidelines for Media Sanitization. These four methods are as follows:

- *Disposal* is defined as the act of discarding media with no other sanitization considerations. Examples of Disposal include discarding paper in a recycling container, deleting electronic documents using standard file deletion methods and discarding electronic storage media in a standard trash receptacle.
- *Clearing* is defined as a level of sanitization that renders media unreadable through normal means. Clearing is typically accomplished through an overwriting process that replaces actual data with 0's or random characters. Clearing prevents data from being recovered using standard disk and file recovery utilities.
- *Purging* is defined as a more advanced level of sanitization that renders media unreadable even through an advanced laboratory attack. In traditional thinking, Purging consists of using specialized utilities that repeatedly overwrite data; however, with advancements in electronic storage media, the definitions of Clearing and Purging are converging. For example, Purging a hard drive manufactured after 2001 only requires a single overwrite. For the purpose of this Guideline, Clearing and Purging will be considered the same. Degaussing is also an acceptable method of Purging electronic storage media; however, this typically renders the media unusable in the future.
- *Destroying* is defined as rendering media unusable. Destruction techniques include but are not limited to disintegration, incineration, pulverizing, shredding and melting. This is a common sanitization method for single-write storage media such as a CD or DVD for which other sanitization methods would be ineffective. This is also a common practice when permanently discarding hard drives.

Electronic Storage Media is defined as any electronic device that can be used to store data. This includes but is not limited to internal and external hard drives, CDs, DVDs, Floppy Disks, USB drives, ZIP disks, magnetic tapes and SD cards.

Non-public Information is defined as: Any information that is classified as private or restricted according to federal, state or local ordinance, law or amendment to such ordinance or law.

Responsibilities:

The following are requirements for when data sanitization should occur:

- All paper-based media should be disposed of when it is no longer necessary for business use, provided that the disposal does not conflict with parish data retention schedule or policies, or any regulatory requirements (e.g. electronic discovery).
- All electronic storage media should be sanitized when it is no longer necessary for business use, provided that the sanitization does not conflict with parish data retention policies, or any regulatory requirements (e.g. electronic discovery).
- All electronic storage media should be sanitized prior to sale, donation or transfer of ownership. A transfer of ownership may include transitioning media to someone in your department with a different role, relinquishing media to another department, or replacing media as part of a lease agreement.

The **IT STD 0-00** defines three classifications of data: PUBLIC, INTERNAL and CONFIDENTIAL / SENSITIVE. The following table illustrates what levels of sanitization are generally acceptable based on these classifications. For media that contains more than one classification of data, the sanitization method selected should be consistent with the most restrictive classification.

Classification	Disposal	Clearing and Purging	Destroying
PUBLIC	X	X	X
INTERNAL		X	X
CONFIDENTIAL / SENSITIVE		X	X

The following are recommended tools and techniques for sanitization and disposal of paper-based media:

- Cross shredding should be used for Clearing and Purging of paper-based media.
- A third-party document destruction services should be leveraged for destroying paper-based media. A Certificate of Destruction should be requested, as evidence that documents were destroyed, and retained for future reference.

The following are recommended tools and techniques for sanitization and disposal of Electronic Storage Media:

- Clearing and Purging of writeable Electronic Storage Media should be performed using seven overwrites for media manufactured prior to 2001 and a single overwrite for media manufactured after 2001.

- Destruction techniques should be used when Clearing and Purging are not effective (e.g. single-write media or media that is permanently write protected).
- Cross shredding should be used for Destroying non-writeable CDs, DVDs and Floppy Disks.
- Destruction of all Electronic Storage Media should be handled by the parishes ISD, unless otherwise specified in this Guideline. ISD will coordinate destruction with a third-party service provide and retain a Certificate of Destruction for all media that is destroyed.
- In situations where a third-party warranty or repair contract prevents proper sanitization of Electronic Storage Media, the ISD should be contacted for further guidance.

Related Policies, Standards, Guidelines: IT POL 1-01 Data Sanitization, IT STD 0-00 Data Classification Guideline

Owner: WFPPJ ISD

Effective Date: 7/1/2010