

Department of Natural Resources

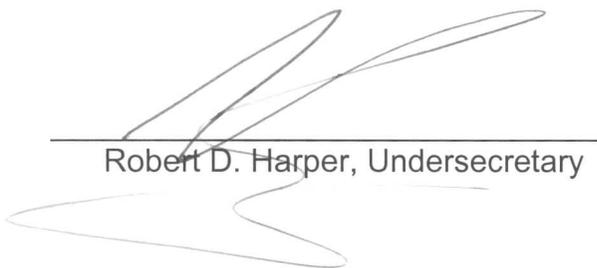
Information Technology Policy No. 2

Effective Date: March, 1999
Revised Date: September, 2006; May 1, 2009

Subject: General Purpose IT Policies

Authorization: R.S. 36:353

Approved By:



Robert D. Harper, Undersecretary

5/1/09
Date

Table of Contents

1. Purpose of this Document	3
2. Policies	3
2.1 Policies	3
2.2 Standards and Procedures	3
3. Organization of the IT Division	4
4. Committees	5
4.1 IT Steering Committee	5
4.2 IT Security Committee	5
5. Infrastructure	6
5.1 Technology	6
5.2 Purchasing	6
6. Software	7
6.1 Corporate Database	7
6.2 Development Methodology and Tools	7
6.3 Application Development Environment	8
6.4 Changes & Enhancements (Service Order)	9
7. Security	10
7.1 Access to Restricted Areas	10
7.2 System Integrity	10
7.3 Segregation of Duties	10
7.4 System Access	11
7.5 New Employee Orientation	11
7.6 Adding Access for a New Employee	12
7.7 Change of Access for an Employee Transfer	12
7.8 Deletion of Access upon Employee Termination	12
7.9 System Access by Third Parties	12
8. Data Backup, Archiving and Sanitization	13
8.1 Data Backup and Archiving	13
8.2 Data Sanitization	13
9. OIT Standards & Policies Implemented at DNR	14
Amendments	15

1. Purpose of this Document

This document is designed to be a compilation of general purpose IT policies of the DNR Information Technology Division (ITD). This manual is not intended to be used for the purpose of day-to-day activities, but rather as a guide to the main IT policy issues within the Department and the Division.

2. Policy

2.1 Policies

The following IT-related policies have been adopted by the Department:

DNR IT Policy 1	Computer Use Policy
DNR IT Policy 2	General Purpose IT Policies (<i>this document</i>)
DNR IT Policy 3	Acquisition of Data Processing and GIS Equipment & Software
DNR IT Policy 4	Deactivation of Inactive User Identification

Policies stated in this document are intended to comply with the laws of the State of Louisiana, other Department of Natural Resources' (DNR) policies, and policies of the Division of Administration's Office of Information Technology (OIT). Any change to the General Purpose IT Policies document will require the approval of the DNR Undersecretary.

2.2 Standards and Procedures

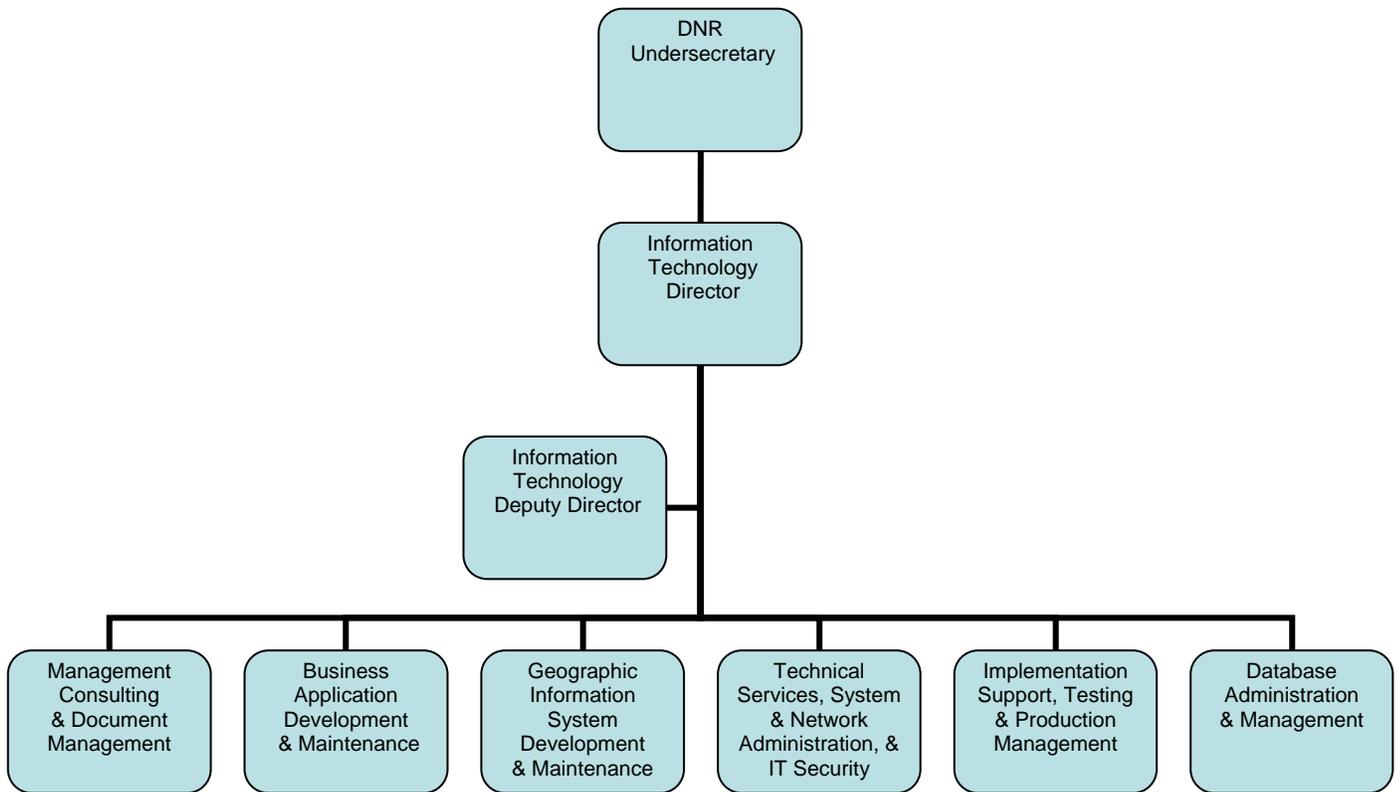
This manual serves as a basis for other standards and procedure manuals designed, developed, and maintained by individual sections within the IT Division. These standards and procedures must comply with the overall IT policies of the Department. All changes and/or additions/deletions to the standards and procedures will require authorization from the Information Technology Director.

All Information Technology software applications, software packages, Geographical information system, content management systems, and all other software and hardware applications developed and/or acquired by DNR to support DNR's functions and any other functions supported by DNR such as Office of Coastal Restoration and Protection will be under the program name SONRIS – Strategic Online Natural Resources Information System. There will be NO exception to this general DNR Policy.

3. Organization of the IT Division

To provide state-of-the-art, high-technology support for its offices and divisions, DNR operates the Information Technology (IT) Division to deliver a wide range of information services to internal-DNR employees, other state government agencies, and external private-sector users. Through IT, DNR possesses the ability to plan, implement and support complex information system projects, including its major focus, the enterprise-wide Strategic Online Natural Resources Information System - SONRIS.

The DNR IT Division is organizationally located in the Management & Finance program of the Office of the Secretary. The Division is headed by the Information Director, who reports to the DNR Undersecretary. The Information Technology Deputy Director reports to the Director, as do managers of each of the six sections, as shown below. This chart is included to illustrate the policy on segregation of duties that is described elsewhere in this document.



4. Committees

4.1 IT Steering Committee

The DNR Internal Audit Advisory Committee is authorized, as part of its responsibilities, to function as the IT Steering Committee, and oversee and prioritize major IT projects.

The Committee, which meets at least once every quarter, has the following broad objectives relative to IT review:

- Review progress of major IT projects
- Prioritize major IT projects
- Review IT audit reports and recommend necessary process adjustments
- Prepare and provide an executive summary to the Undersecretary of DNR
- Recommend IT system enhancements

The committee is comprised of the following staff members of DNR:

Chairman:	Undersecretary
Members:	Information Technology Director DNR Internal Auditor
Ad-Hoc members:	Assistant Secretary of OMR, or designee Assistant Secretary of OCRM, or designee Commissioner of Conservation, or designee Office of the Secretary designee IT Deputy Director, or designee Human Resources Director

4.2 IT Security Committee

The DNR IT Security Committee's purpose is to review IT security policy, security issues, procedures, security responsibility and provide reports and recommendations as needed to senior DNR management.

The committee is comprised of the following staff members of DNR:

Chairman:	Undersecretary
Members:	DNR Internal Auditor Assistant Director of the Technology Assessment Division
Ad-Hoc member	IT Director

5. IT Infrastructure

5.1 Technology

The DNR IT infrastructure will be based on an open, industry standard architecture, using commodity desktops and server hardware, to allow DNR to take advantage of emerging technologies at the lowest cost to the State.

The current infrastructure is based on a three-tier Client/Server environment:

- client (typically a Microsoft Windows desktop)
- application servers
- database server

The IT Division will closely monitor emerging technology and will adopt cost-effective and well-tested technology as appropriate for the benefit of DNR.

5.2 Purchasing

All data processing hardware, geographical information system (GIS), global positioning system (GPS), and software purchased in the department will comply with IT infrastructure standards.

The purchase of any hardware or software must have the approval of the Information Technology Director prior to procurement by the DNR Purchasing Division. (See *DNR IT Policy No. 3 for details*)

6. Software

6.1 Corporate Database

DNR will use the Oracle relational database management system (RDBMS) as its corporate database.

No other database system will be purchased unless it is justified by a compelling business need. All such purchases will have to be approved by the IT Director.

All software packages must also use Oracle as RDBMS.

6.2 Application Development Methodology and Tools

The division will use a CASE (Computer Assisted Software Engineering) method to develop and maintain core business applications.

The IT Division will also review other methods and will adopt new methods if proven to be cost-effective and provide improvement.

Oracle Designer will be used as the only tool to develop core business applications.

Any deviation will require the IT Director's authorization.

For other development and package enhancements and interface programs, only widely-used languages such as Visual Basic will be used.

6. Software (continued)

6.3 Application Development Environments

Three distinct environments will be set up for in-house development and enhancement.

Each of the environments will have an appropriate access mechanism. Employees will not be given authorization to more than one environment.

1. The **development environment** will be used by developers. They will be able to develop and test all or part of an application in this environment. The respective development manager will copy the final product to Staging Area 1.
2. The **implementation environment** will be used by the implementation team to perform acceptance testing. The Implementation Manager will copy the product delivered by the development team from Staging Area 1 to the implementation environment. Once the acceptance testing is complete, the Implementation Manager will copy the final product to Staging Area 2.
3. The **production environment** will be used for production. The System Administrator and/or Database Administrator will copy the final product from Staging Area 2 to the production environment.

All movement from one environment to another environment will require the IT Director's authorization.

6. Software (continued)

6.4 Changes & Enhancements (Service Order)

All requests for software changes, software enhancements, system software implementation and changes due to an incident will be processed through an automated Service Order process.

A Service Order process will generally have the following work flow:

- Initiated by any employee of DNR
- Approved by designated employee of the office
- The IT manager will estimate resource requirements
- IT Director will authorize all development, implementation and enhancement efforts. All major projects (greater than 6 man-months effort) will require the IT Steering Committee's approval
- The IT manager will allocate resources and monitor the project
- All progress reporting will be maintained on-line and users will have access to it
- IT manager or designee will select test data for the project and ensure that the system is tested properly
- Database Administrator will be involved in the Analysis phase and will be responsible to make all physical database changes
- IT manager will release the project for implementation after testing is complete and approval is obtained from the IT Director
- Implementation Manager will perform acceptance testing with the users. Necessary changes will be done by the appropriate development team
- The final product will be placed in production by Database Administrator and System Administrator
- Implementation team will follow-up

7. Security

7.1 Access to Restricted Areas

It is the policy of DNR to restrict access to sensitive IT areas on a need-only basis.

- Access to the IT Division's computer room and the Technical Services Work Area room on the 11th Floor of the LaSalle Building will be restricted on a need-only basis, and require a stripe-card for access.
- Access to server areas in the Division of Administration's Information Services Building (ISB), where DNR servers are located, will utilize security mechanisms provided by ISB. When possible and when funding permits, DNR will also utilize locking mechanisms on servers and server consoles.
- Authorization from the IT Director will be required for access to the above-named areas.

7.2 System Integrity

Necessary measures will be adopted to ensure overall system integrity, including but not limited to the following:

- All external access will go through a firewall.
- Data encryption will be considered when necessary and when feasible.
- System will be scanned for viruses on a regular basis.
- User ID audit report will be produced on a monthly basis.

7.3 Segregation of Duties

Security access will be maintained through password assignments and 30 days automatic expiration cycle. The System Administrator, Network Administrator and Database Administrator will assume responsibility of maintaining passwords.

The System Administrator, Network Administrator and Database Administrator will not participate in application software development efforts.

The software development staff will not have rights to make changes to passwords of anyone but their own.

See also Section 6.3 of this document for related information on segregation of duties.

7. Security (continued)

7.4 System Access

System access will be user id and password driven. The password will automatically expire in 30 days if not changed by the individual employee. The password scheme will require a minimum of seven (7) characters (one of which must be numeric).

In addition, the account of any employee who has not logged into the system for 30 days will be deactivated (*see DNR IT Policy No. 4 for details*).

IT will create, and delete, system user accounts only upon proper notification by DNR Human Resources (see Section 7 of this document for details).

The password maintenance will be carried out by the System Administrator, Network Administrator and Database Administrator.

All change requests or new assignments requests will be channeled through the IT Help Desk.

Where applicable, role-based passwords will be assigned. A role will be created for one or more employees performing the same tasks.

The IT Division will continually monitor the availability of better methods of password administration and control. Concepts such as a single sign-on and biometric sign-on will be explored for applicability, usability, and level of protection, and implemented when technically and financially feasible.

7.5 New Employee Orientation

As part of the DNR New Employee Orientation session, each employee will be given a copy of DNR IT Policy #1 "Computer Use Policy" and briefed on the importance of the Policy and adhering to its contents.

7. Security (continued)

7.6 Adding Access for a New Employee

When a new DNR employee is hired, the DNR Human Resources Division will send appropriate notification to the IT Division. This notification will serve as authorization for the creation of appropriate system user accounts, and establishment of appropriate security clearances and roles.

7.7 Change of Access for an Employee Transfer

When an employee is transferred from one office or division to another and/or from one role to another role, supervisors of both offices/divisions must send the request in writing to remove the employee from one role and then assign him/her another role that is appropriate for the new office/division assignment.

All documentation must be maintained by the IT security administration staff and have it available for internal/external audit at any time.

7.8 Deletion of Access upon Employee Termination

When a DNR employee is terminated, the DNR Human Resources Division will send appropriate notification to the IT Division. This notification will serve as authorization for the IT Division to delete all system user accounts associated with that employee, and remove all security clearances and roles.

All documentation must be maintained by the security administration staff and have it available for internal/external audit at any time.

7.9 System Access by Third Parties

Procedures will be put in place (similar to those outlined above for employees) for other parties requiring system access, including but not limited to: contractors, consultants, temporaries, Federal Government workers, and State employees from other Louisiana agencies.

8. Data Backup, Archiving and Sanitization

8.1 Data Backup and Archiving

DNR will utilize a sophisticated, single data backup and archiving system, using both a tape library system for optimum integrity, and a disk-based backup system to facilitate quick recovery as part of DNR's Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP).

Daily, monthly, yearly (calendar and fiscal) back up will be automated where possible.

The backup data will be stored near line (in the storage library), in the building in a 4-hour rated fire safe, and to a managed off-site location. Additional disk backups will be stored in another geographical part of the State.

All required data such as year-end will be archived and stored at a managed off-site location.

8.2 Data Sanitization

The DNR IT Division will establish procedures to insure the removal of data deemed security-sensitive/confidential from departmental storage media prior to being transferred to another government entity, or to the Louisiana Property Assistance Agency.

The IT Division will degauss, overwrite, remove or erase storage devices and media as appropriate, as required by the Division of Administration's OIT Policy relative to Data Sanitization (IT-POL-03), and document such actions.

9. OIT Standards & Policies Implemented at DNR

The Department of Natural Resources adheres to all OIT policies.

Amendments

#	Date	Rem*	Add*	Description	Approval
1	3/01/1999			Original version	
2	6/14/2005			No pages added or changed; only minor updates and clarifications made on these pages: 3,4,5,7,8,9,10,11,13,14,15,20	
3	09/01/2006			No pages added or removed. One bullet added to Section 7.2, page 10.	
4	05/01/12009			No pages added or changed. A paragraph added to Section 2.2, page 3; one bullet removed and one added to Section 7.2, page 10; Section 9, pages 14 & 15 rewritten.	
5					
6					
7					
8					
9					
10					
11					
12					
13					

- Rem = Page(s) removed, Add = Page(s) added