BOBBY JINDAL
GOVERNOR

State of Louisiana
Governor's Office of Homeland Security
and
Emergency Preparedness

MARK A. COOPER
DIRECTOR

**System Access Policy**
**Policy Number: GEN-0010**

| | |
|---|---|
| **Issue Date:** | **August 3, 2009** |
| **Effective Date:** | **August 3, 2009** |
| **Revised Date:** | **July 17, 2009** |
| **Approval:** | Mark A. Cooper, Director |

## I. POLICY

It shall be the policy of the Governor's Office of Homeland Security and Emergency Preparedness (GOHSEP) that the agency's Information Technology Section shall establish and maintain the Policies and Procedures for access to required systems within the GOHSEP.

## II. PURPOSE

A. Develop and maintain clear, concise, and consistent policies and procedures across the GOHSEP distributed systems enterprise.
B. Establish a formal process of granting access to the various data systems maintained and supported by the GOHSEP Information Technology Section. Access to systems and data should be granted to users only on a "*need to know*" basis.
C. The Information Technology Section is responsible for protecting the integrity of the distributed information systems and for configuring system security parameters consistent with State Security Standards and Industry Best Practices.

## III. APPLICABILITY

This policy applies to all organizational units and personnel of GOHSEP to include contractor staff working for GOHSEP.

## IV. RESPONSIBILITY

A. Information Technology will create, manage and monitor accounts for;
   1. Network Access
   2. E-mail
   3. Virtual Private Network (VPN)
   4. Account Setup for specific application, i.e Lotus Notes
   5. Virtual Louisiana

B. Operations system Administrator will create, manage and monitor:
   1. WebEOC

C. Louisiana Public Assistance System Administrator will create, manage and monitor:
   1. Louisiana Public Assistance (LAPA)

B. Finance System Administrator

   1. ISIS

E. Homeland Security

   1. Automated Critical Asset Management System (ACAMS)

## I. Appendix

- Procedures for System Access

## APPENDIX TO POLICY GEN-0010 – System Access Policy

## PROCEDURES FOR SYSTEM ACCESS

### Overview

Request for access to the Governor's Office of Homeland Security and Emergency Preparedness's (GOHSEP) network infrastructure and/or associated applications and databases requires the completion and approval of system specific forms and or processes as outlined in the Procedure section below. The exception to this procedure is the access established for the Emergency Support Function (ESF) workstations located in the Emergency Operations Center (EOC).

Once system access is established, the designated System Administrator will be responsible for the periodic review of authorized system users. Unauthorized systems users are defined as employees, who have resigned, been terminated or no longer have a need to access certain applications and/or databases.

### Purpose

To establish standards and controls for system access within GOHSEP's computing environment.

### Access Request Procedures

***New Hire Access Request***

The hiring Section Chief or designated staff member will notify the Human Resources Section of the selected candidate and the required resources the new hire will need to accomplish his/her duties and responsibilities;

The Human Resources Section representative will initiate the request via I.T. Division Request / User Forms to obtain the following:

***GOHSEP Domain Accounts***

GOHSEP Domain Accounts – Access to the GOHSEP Domain (Infrastructure / E-mail / Virtual Private Network (VPN) / Lotus Notes) is managed by the Information Technology Section System Administrators. The request to establish a domain account are received from the Human Resource Section on an I.T. Division Request / User Form.

Basic Domain accounts (Infrastructure / E-mail) are created for all new hires. Access to the GOHSEP infrastructure through the VPN client and Lotus Notes are granted on the new hire's job responsibilities.

### System Requests

***Virtual Louisiana***

Virtual Louisiana – Access to the Virtual Louisiana application is managed by the Information Technology Section's GIS System Administrator. The request for access is made through the on-line request form associated with the Virtual Louisiana link

on the GOHSEP web page. The on-line form is reviewed and generated by the System Administrator.

Virtual Louisiana accounts are typically generated for any emergency response personnel.

***WebEOC***

WebEOC – Access to the WebEOC application is managed by a System Administrator assigned to the Operations Section. The request for access is made either verbally or through an e-mail to the System Administrator.

Access is not granted to individuals. Access is granted by position within the Operations Section or to the ESF workstations in the EOC.

***Louisiana Public Assistance (LAPA)***

LouisianaPA.com – Access to the LAPA application is managed by the Application Support Team assigned to the Disaster Recovery Division within GOHSEP. The request for access is made through the on-line request forms associated with the Resource Tab on the LouisianaPA.com web site.

LouisianaPA.com accounts are generated for Applicants, State Agencies, and GOHSEP staff. Request forms can be faxed to (225) 267-2832 or emailed to La.Pa@la.gov. All requests for access to LouisianaPA.com will be processes by the Document Services (DS) Section.

***ISIS***

ISIS – Access to the ISIS application is managed by the System Administrator assigned to the Finance Section. The request for access is made either verbally or through an e-mail to the System Administrator.

Access is granted to Finance staff personnel on a need to know basis.

***Automated Critcal Asset Managememnt System (ACAMS)***

ACAMS – Access to the ACAMS application is managed by the System Administrator assigned to the Homeland Security Section. The request for access is made either verbally or through an e-mail to the System Administrator.

Access is granted to Federal/State/Local/Private Sector Asset Managers who have law enforcement, emergency management or homeland security responsibilities and have a valid need to know. Access is only granted once pre-requisites have been met. DHS promulgates regulations and requirements.

**System Account Controls**

Domain Accounts – All accounts conform to naming standards and password policies. After fifteen (15) minutes of inactivity, accounts will have access to the desktop locked automatically.

Virtual Louisiana – All accounts conform to naming standards and password policies.

WebEOC – All accounts conform to naming standards and password policies.

LAPA – All accounts conform to naming standards and password policies.

ISIS – All accounts conform to naming standards and password policies.

ACAMS – All accounts conform to naming standards and password policies.

Disabled Accounts – All disabled accounts will be deleted after ninety (90) days. Exceptions will be considered on a situational basis only or if the account is required for proper functioning of a system. Accounts may be disabled for the following reason but not limited to termination, resignation and administrative leave.

All account information and data will be backed up prior to account deletion.

Inactive Accounts – On a bi-annual basis all user account repositories will be reviewed. Any account that is identified as unnecessary will be investigated and deleted as appropriate.

Non-GOHSEP Accounts (Contractors and Vendors) – All non-GOHSEP accounts must be unique. All non-GOHSEP accounts must be validated every ninety (90) days, unless established during setup. All non-GOHSEP VPN accounts will have limited access based on time of day and the systems to which they connect.