APPENDIX 1

Alabama Voter Registration and Election Management System

Security Policy

Table of Contents

Document Revision History

Modification Date	Description	Version
June 30, 2008	Initial Draft	Draft 1
August 8, 2008	Final Draft	Final Version 1.0

Introduction

The purpose of this policy is to ensure the integrity and security of the Alabama Voter Registration and Election Management System. With the implementation of a centralized, uniform HAVA compliant voter registration and election management system, security is more important than ever.

Each user of the system shall be bound by the conditions defined herein. Counties that are not fully in compliance with this security policy by *September 30, 2008* will be subject to disconnection from the central system.

This policy identifies authority and access levels of the various users within the Alabama elections community. This policy should not prevent any user from accessing the system to perform their appropriate duties.

Application Security Overview

There are two layers of security to the voter registration and election management system. The first layer of security grants each user access to the centralized system via a security product called Citrix. ES&S administers the Citrix environment under the guidance of the Governor in his role as Special Master and eventually under the Secretary of State when the responsibilities for the HAVA system are transferred back to that office.

The second layer of security is administered locally within each county and must be done so in accordance with the User Roles and System Administration policy as defined below. The second layer, called PowerLock, allows each county to add and maintain users once a Citrix account has been created by ES&S for those users. For election management users, a PowerLock Account still must be created at the central level in order for a user to access data locally.

Each user must have both a Citrix account and a PowerLock account in order to access the system.

User IDs

Each User ID should be the user's first initial and last name followed by their county code. In the unlikely event that there are two users with the same name in the county, the middle initial should be used. ES&S will automatically use this schema for the Citrix accounts and county administrators should adhere to the same policy for tracking purposes

Example:
Name:	User ID:
Jane Smith	jsmith01
Janice E. Smith	jesmith01

Passwords:

Each user should maintain secure passwords for both their Citrix and PowerLock User IDs. Each password should contain the following:

- Be at least six characters in length
- Contain one numeric character
- Contain one capital letter

The password should not contain any aspect of the user's name. The password should not be written down anywhere or hidden under keyboards, etc. or in/on the user's desk. Users should never share their password with another individual. If a user feels that their password has been compromised, they should contact their local security administrator and/or ES&S immediately.

User Access and Responsibilities

Each user is responsible for accessing the system in accordance with all applicable Federal, State and local laws in order to perform their duties. Each user may have only one User ID and shall not share their password or access methods with any other user under any circumstances. Because the security of voter registration data is critical to the integrity of elections in Alabama, any user that knowingly violates this security policy may be subject to removal from access to the system, regardless of position, and possibly subject to legal sanctions.

There are six overall user groups within the system, excluding vendor system administration and support functions:

1. State users– consist of the Secretary of State as system owner and her staff personnel and temporarily includes the Special Master and his staff personnel in his Court-appointed role. The State is responsible for statewide and federal election definitions as well as state level reporting and statistics. The State shall not edit any county's voter registration or election management data.
2. County users - Voter Registration / Registrars – Registrars are responsible for Voter Registration activities within the system. Only Registrars or those they specifically delegate to may edit voter registrant data.
3. County users - Election Management / Probate –The Probate Judge serves as the chief election official(s) in each county. He or she and their Election Management staff may perform most functions within the system with the exception of voter registration or absentee management. Election Management staff is specifically prohibited from editing individual voter registrant data.
4. County users - Absentee Management / Circuit Clerks-Absentee Managers – are responsible for absentee election management duties and may not perform voter registration or election management functions within the system.
5. County users – Street file / precinct maintenance – These users are responsible for maintaining/updating the street files and precinct definitions. This role will be filled by different users from county to county as designated in writing by the County Commission.
6. County users – County System Administrator – This user will administer the PowerLock security components of the system as defined further below. This user shall not grant access to any unauthorized user nor shall they grant any user inappropriate access to any unauthorized aspect of the system. This role

will be filled by different users from county to county as designated in writing by the County Commission.

Because the system is a fully integrated voter registration and election management system and is designed to serve as a single source of elections data for the State of Alabama, there will be some overlap in functions among the three areas for some aspects of the system. At a minimum, however, users must be set up systematically within the minimum groups as described above in order to prevent unauthorized use of the system.

System Administration

Each County System Administrator is responsible for maintaining the county's user accounts within the PowerLock security module and should notify ES&S when users should be added or deactivated from the system at the Citrix or top layer of security access. Absentee Managers have the authority to grant absentee users access, registrars have the authority to grant access for voter registration and election management personnel have the authority to grant access for probate/election management functions. The Secretary of State shall have the authority to grant state level users access.

Within each county, a PowerLock System Administrator shall be established by consensus within the county and by the County Commission if that consensus cannot be reached. The County System Administrator will ensure that each user is properly assigned to one of the three county user type PowerLock Groups below. Additional Groups may be defined to better manage the workflow and responsibilities within the county. The roles defined within each group below represent the permission levels appropriate for each user type.

Registrars – each registrar or authorized user that performs registration duties shall be assigned to this PowerLock group. No other users may be assigned to this group unless specifically authorized by the registrars in that county.
>Role Restriction: Registrars cannot perform Election Management functions or Absentee Management Functions

Probate – each probate judge or his/her staff that requires access to the system shall be assigned to this group. No other users may be assigned to this group unless authorized by the probate judge in that particular county.
>Role Restriction: Probate users cannot perform any entry or update on any registrant data

Circuit Clerk/Absentee - each absentee manager that requires access to the system shall be assigned to this group. No other users may be assigned to this group unless authorized by the Circuit Clerk or Absentee Manager.
>Role Restriction: Absentee Managers/Circuit Clerks cannot perform Election Management functions or perform any entry or update on any registrant data

Antivirus Software

Each desktop or laptop computer used to access the Alabama Voter Registration and Election Management System shall have up to date antivirus software installed and running. For State provided equipment, antivirus software has been installed and set to automatically update without any action required on the part of the user.

Users have the responsibility for making sure that antivirus software is current and operating on any computer used to access the Voter Registration and Election Management System.