



ATTORNEY GENERAL OF TEXAS  
GREG ABBOTT

---

**Office of the Attorney General**  
**Information Technology Security**  
**Policy Manual**

---

Version 4.3  
April 5, 2011

Presented by:  
Kathleen Donaho-Jaeger  
CS Information Security Officer  
Mike O'Connell  
A&L Information Security Officer

## Table of Contents

1.	Information Security Policy .....	4
1.1.	Attorney General Policy Statement .....	4
1.2.	Scope of Policy .....	4
1.3.	OAG Information Security Policy Purpose & Intent .....	4
1.4.	Definitions.....	4
2.	Management Security Controls.....	5
2.1.	State Agency Head - Attorney General .....	5
2.2.	Management Responsibility.....	5
2.3.	Information Resources Manager (IRM).....	5
2.4.	Information Security Officers (ISO).....	5
2.5.	Information Resource Owner.....	6
2.6.	Information Custodian .....	7
2.7.	Information Technology User.....	8
3.	Operational Security Controls.....	8
3.1.	Risk Management Framework.....	8
3.2.	Risk Assessment .....	8
3.3.	Asset Management.....	8
3.4.	Disaster Recovery & Business Continuity.....	9
3.5.	Outsourced Data Center Operations & Security Responsibility.....	9
4.	Personnel Security Policy .....	9
4.1.	Statement of Responsibility .....	9
4.2.	Reporting of Security Incidents .....	9
4.3.	Computer Security Incident Response Team (CSIRT).....	9
4.4.	Information Security Violations .....	10
4.5.	Acceptable Use of OAG Information Technology Assets.....	10
4.6.	Access to OAG Information Technology Assets.....	11
4.7.	User Identification .....	11
4.8.	Personal Software, Hardware and Modems.....	11
4.9.	Security Awareness Program .....	11
4.10.	Warning Statements .....	11
4.11.	Termination of Employment.....	12
4.12.	Automatic Suspension / Deletion of User ID's.....	12
4.13.	Positions of Special Trust .....	12
5.	Technical Security Controls.....	12
5.1.	System Security Policy .....	12
5.2.	System Administrators.....	12
5.3.	System Developers.....	12
5.4.	Information Technology Asset Protection .....	13
5.5.	Vendor Access to OAG Systems .....	13
5.6.	Classification of Electronic Data and Assets .....	13
5.7.	Data Destruction .....	13
5.8.	Configuration Management .....	14
5.9.	Change Management .....	14
5.10.	Data Integrity .....	14

Office of the Attorney General

5.11.	Voice/Phone Mail .....	14
5.12.	E-mail.....	14
5.13.	Wireless Systems .....	15
5.14.	Copyright .....	15
5.15.	Personal Software, Shareware and Freeware.....	15
5.16.	Data Encryption .....	15
5.17.	Portable and Mobile Devices.....	15
5.18.	Malware Protection Software .....	15
5.19.	Intrusion Detection.....	15
5.20.	Internal Electronic Investigations .....	16
5.21.	Screen Savers .....	16
5.22.	User Passwords .....	16
5.23.	Administrator Passwords .....	16
5.24.	System Log On & Re-Boot.....	16
5.25.	System Settings.....	16
5.26.	Control of Peripherals .....	16
5.27.	Security Breaches.....	17
5.28.	Dial-up Access.....	17
5.29.	Purchasing/Development Pre-Approval .....	17
5.30.	Contract Security Provisions.....	17
5.31.	System Development, Acquisition and Testing.....	17
6.	Exception, Waiver and Modification.....	18
6.1.	Waivers and Exceptions.....	18
6.2.	Modification or Significant Changes to Procedures .....	18
6.3.	Executive Management Waiver .....	18
7.	Document Acceptance and Release Notice .....	19
8.	References.....	20

## **1. Information Security Policy**

### **1.1. Attorney General Policy Statement**

The Office of the Attorney General (OAG) is committed to protecting the information resources that are entrusted to this agency. An effective data security protocol, supported by an appropriately rigorous security structure, is critical to the success of an information security program. The OAG's Information Security Officers are responsible for managing and developing the information security program, which includes identifying and resolving all at-risk information system assets, as well as supporting the operational needs of the agency.

An effective information security program encompasses many activities requiring commitment and cooperation among both employees and management of the OAG. All information resources users must be involved in the success of this strategic effort.

### **1.2. Scope of Policy**

This policy applies to all OAG "information assets" that are used by or for the OAG throughout its life cycle. "Information assets" are the procedures, equipment, and software that are employed, designed, built, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information, and associated personnel including consultants and contractors.<sup>1</sup>

This policy also applies to all users of OAG information assets, and electronic data regardless of location.

To the extent there is any conflict between this policy and the Sensitive Personal Information Privacy Policy (found at <https://intranet.oag.state.tx.us/admin/hrd/policies/policy.php>), the latter shall control.

### **1.3. OAG Information Security Policy Purpose & Intent**

The purpose and intent of this policy document is to familiarize users of OAG information resources with the need to protect these resources in a prescribed manner and in accordance with appropriate standards.

### **1.4. Definitions**

#### **Access:**

The physical or logical capability to interact with, or otherwise make use of information assets.

#### **Business Continuity Planning:**

The process of identifying mission critical data systems and business functions, analyzing the risks and probabilities of service disruptions and developing procedures to restore those systems and functions.

**Control:**

Any action, device, policy, procedure, technique, or other measure that improves security.

**Encryption:**

The conversion of plain text (human readable) information into a mathematical cipher or algorithm to create an electronic message that conceals the true meaning.

**Information Asset:**

The term information asset is defined in Section 1.2 of this policy.

**Information Resource Data:**

Any data electronically produced, modified, transmitted, or stored while in electronic form.

**Information Technology Asset:**

A subset of the term information asset that refers to computing hardware such as a laptop computer, desktop PC, network server, or computer software.

## **2. Management Security Controls**

### **2.1. State Agency Head - Attorney General**

The Attorney General, as the state agency head, is responsible for establishing and maintaining an information security and risk management program.<sup>ii</sup> It is the responsibility of the Attorney General to ensure that the agency's information assets are protected from the effects of damage, destruction, and unauthorized or accidental modification, access or disclosure.

### **2.2. Management Responsibility**

The protection of information assets is a management responsibility. Managing information security within the OAG requires commitment and support on the part of executive, technical and program management. All managers must be involved in the security and awareness program, and be familiar with and enforce OAG policies and procedures among their staff and employees.

### **2.3. Information Resources Manager (IRM)**

The IRM is the agency executive who must approve the information technology assets and services necessary to conduct the information security program, as well as use executive authority where necessary to enable the success of the information security program.

### **2.4. Information Security Officers (ISO)**

A full-time ISO will oversee the Administrative and Legal Divisions (A&L), while another full-time ISO will oversee the Child Support Division (CS). The A&L ISO and CS ISO will report

## Office of the Attorney General

directly to their respective IT Directors and indirectly to the IRM. It is the ISO's duty and responsibility to:

- Manage, develop and coordinate the development of the OAG information security program and all other information security policies, standards and procedures.
- Collaborate with IT divisions, information asset owners and executive management in the development of procedures to ensure compliance with external information security requirements.
- Develop training materials on information security for employees and all other authorized users, and collaborate with agency training staff to establish a standardized agency-wide information security training program.
- Develop and implement incident reporting and incident response processes and procedures to address any security incident/breach, violation of policy or complaint.
- Serve as the official agency point of contact for all information security inquiries and audits.
- Develop and implement an ongoing risk assessment program, including recommending methods for, and overseeing of, vulnerability detection and testing.
- Monitor security legislation, regulations, advisories, alerts and vulnerabilities, and communicate accordingly with IT divisions, data owners and executive management.
- Review agency information systems and provide written reports that identify potential security risks and recommended solutions as appropriate.
- Provide annual report to executive management on security program and risk mitigation.
- Collaborate with IT personnel, the Records Management Officer, and legal counsel to preserve data in accordance with appropriate data preservation and litigation hold procedures.

### **2.5. Information Resource Owner**

An information resource owner is defined as a person responsible for a business function and for determining controls and access to information resources supporting that business function.<sup>iii</sup> The state agency head or his or her designated representative(s) shall review and approve ownership of information resources and their associated responsibilities.<sup>iv</sup> For the OAG Information Resource Owners are typically Division Chiefs.

Where information resources are used by more than one division, the owners shall reach a consensus as to the designated owner with responsibility for the information resources and advise the A&L or CS ISO of their decision.<sup>v</sup>

## Office of the Attorney General

The information owner or his or her designated representatives(s), with the CISO's concurrence, are responsible for and authorized to:

- Approve access to, and formally assign custody of, an information asset;
- Determine the asset's value;
- Specify data control requirements and convey them to users and custodians;
- Specify appropriate controls, based on risk assessment, to protect the agency's information resources from unauthorized modification, deletion or disclosure. Controls shall extend to information resources outsourced by the agency in accordance with the Department of Information Resources' (DIR) information security policy;
- Confirm that controls are in place to ensure the accuracy, authenticity and integrity of electronic data;
- Ensure compliance with applicable controls;
- Assign custody of information technology assets and provide appropriate authority to implement security controls and procedures; and
- Review access lists based on documented security risk management decisions.

### **2.6. Information Custodian**

An information custodian is defined as any person or group who is charged with the physical possession of information technology assets.<sup>vi</sup> Custodians are the technical managers that provide the facilities, controls and support services to owners and users of information. Custodians of information technology assets, including entities providing outsourced information resources services to state agencies, must:

- Implement the controls specified by the owner(s);
- Provide physical and procedural safeguards for the information assets;
- Assist owners in understanding and evaluating the cost-effectiveness of controls and monitoring;
- Administer access to the information assets; and
- Implement appropriate monitoring techniques and procedures for detecting, reporting and investigating incidents.

## **2.7. Information Technology User**

All authorized users of OAG information technology assets (including, but not limited to, OAG personnel, temporary employees, contractors, sub-contractors, auditors, consultants or agents), shall formally acknowledge that they will comply with the OAG's security policies and procedures or they shall not be granted access to the information technology assets. Each division's ISO will determine the method of acknowledgement and how often this acknowledgement must be re-executed by the user to maintain access to OAG information technology assets.<sup>vii</sup> Users also have the responsibility to report all suspected violations of OAG information security policies to their Division Chief and the ISO responsible for their division. The ISO will then report the suspected violation to the IRM and appropriate IT Director. (See section 3.4)

Users of OAG information technology assets shall have no expectation of privacy for information contained within or processed by an OAG information technology asset. Electronic files created, sent, received by, or stored on, OAG information technology assets that are owned, leased, administered, or otherwise under the custody and control of the OAG are not private and may be accessed by OAG IT employees at any time without knowledge of the information technology asset user or owner. Electronic file content may be accessed by appropriate personnel, including, but not limited to, information security personnel, records management personnel and legal counsel.<sup>viii</sup>

## **3. Operational Security Controls**

### **3.1. Risk Management Framework**

The OAG employs a risk-based information security strategy, which provides a method to eliminate or mitigate identified risk to an organization in order to maximize the positive effects of information security activities while minimizing costs to the organization.

### **3.2. Risk Assessment**

It is the responsibility of the ISO's to regularly assess the risk to all OAG electronic data, systems, networks and information technology operations, and report the results of the assessment to OAG executive management and other appropriate personnel.

### **3.3. Asset Management**

Management of OAG equipment including laptops, PDAs, and other IT equipment is an asset control and physical security issue and not within the scope of this Information Technology Security policy. For policy regarding those items, refer to the OAG's general Policies and Procedures, as well as the Special High-Risk Items Policy, which may be found at <https://intranet.oag.state.tx.us/admin/hrd/policies/policy.php>.

### **3.4. Disaster Recovery & Business Continuity**

The OAG is charged with providing a comprehensive disaster recovery plan and business continuity procedure for all essential Data Center and field operations. This activity will be supported in part by the Information Security Division (ISD).

### **3.5. Outsourced Data Center Operations & Security Responsibility**

As a requirement of House Bill 1516 by the 79th Legislature, OAG information technology systems will be consolidated at the DIR Consolidated Data Centers (CDC).

While DIR and their contractor will supply much of the required services and activities to protect OAG data, systems and networks, the OAG still has responsibility for ensuring the safety of OAG data.<sup>ix</sup>

## **4. Personnel Security Policy**

### **4.1. Statement of Responsibility**

OAG personnel are required to sign a Statement of Responsibility acknowledging that they agree to comply with all applicable information security policies, protocols and procedures as set forth in the OAG Information Security Policy Manual. This statement of responsibility will remain a part of the employee's file.

### **4.2. Reporting of Security Incidents**

A security incident is defined as an event which results, or may result in unauthorized access, loss, disclosure, modification, disruption, or destruction of information resources whether accidental or deliberate.<sup>x</sup>

Employees and all other users shall immediately report all actual or suspected security incidents to their Division Chief and the appropriate ISO. The ISO will promptly notify the IRM and appropriate IT Director of the actual or suspected security incident. The ISO shall report any security incidents that affect critical systems and/or that could be propagated to other state systems outside the OAG to DIR within twenty-four hours.<sup>xi</sup>

### **4.3. Computer Security Incident Response Team (CSIRT)**

The OAG Computer Security Incident Response Team (CSIRT) is responsible for the detection, triage, response, communication and management of all information security incidents. The CSIRT will:

- Provide a single point of contact at OAG for managing all reported OAG information resource electronic attacks, whether suspected or actual;
- Identify and analyze what has occurred, including impact and threat;
- Research and recommend solutions and mitigation strategies;

- Share response options, recommendations, incident information and lessons learned with appropriate entities; and
- Coordinate response efforts.

The CSIRT is comprised of three separate groups that include both permanent IT personnel certified in CSIRT operations, and ad hoc personnel based on the nature of the incident:

1. Management Group:
  - Membership includes: The affected division's ISO and IT Director.
  - May include: IRM.
  - Responsibilities: Manage CSIRT operations (ISO), manage overall incident response, document activities, and produce appropriate reports. Also responsible to communicate internally to executive management.
2. Technology Group:
  - Membership includes: Director of impacted network and Director of impacted infrastructure and/or application.
  - May include subject matter experts (SMEs) from specific disciplines.
  - Responsibilities: Analyze event, recommend possible courses of action, and coordinate selected response.
3. Legal Group:
  - Membership includes: Attorney(s) from, or assigned by, the General Counsel Division, and the Records Management Officer.
  - May include: Law enforcement investigators.
  - Responsibilities: Produce draft of external communications; function as team's legal representative for guidance regarding evidence gathering and other possible legal issues and activities.

#### **4.4. Information Security Violations**

Violations of information security policy could result in a security breach. For this reason, violations of information security policy will be investigated by the appropriate IT personnel. If the violation is found to be deliberate in nature, an official Information Security Violation Report (ISVR) will be issued by the appropriate ISO, with an informational copy provided to the Records Management Officer. Additionally, such violations will be reported to the employee's Division Chief and the Human Resources Director for corrective action. Any corrective action involving use of information technology resources must be documented and reviewed by the appropriate ISO prior to implementation.

#### **4.5. Acceptable Use of OAG Information Technology Assets**

State information technology assets will be used primarily for official State purposes. Software for browsing the Internet is provided to authorized users to conduct official State business. Compliance with this policy will be electronically monitored. Any personal use must be in accordance with the OAG's policy regarding the Unauthorized Use of Government Time,

Property, Services, and Facilities, found at <https://intranet.oag.state.tx.us/admin/hrd/policies/policy.php>.

Violations may result in disciplinary action, up to and including termination of employment. The unauthorized use of OAG information assets will be considered as a relevant factor in evaluating the performance of OAG employees.

#### **4.6. Access to OAG Information Technology Assets**

Access to OAG information technology assets must be strictly controlled and monitored to provide users with only the minimum level of system access necessary to allow them to perform assigned business tasks. When access by the user requires the use of a password, or other security measure, those security measures must be kept confidential by the intended user. Remote access to OAG information systems and assets must be accomplished only through the use of an OAG-approved remote access software application.

#### **4.7. User Identification**

Except for public users of systems where such access is authorized by the appropriate ISO or other appropriate IT personnel, each system user shall be assigned a unique personal identifier or user identification (User ID) to allow system access.

#### **4.8. Personal Software, Hardware and Modems**

Personal software may not be loaded onto any OAG computer, nor may personally-owned hardware, including modems and wireless routers, be connected to OAG information systems. Any hardware or software required for a business purpose of the agency must be approved for use by the appropriate ISO and must be obtained through the appropriate ITS Division.

#### **4.9. Security Awareness Program**

The OAG will provide an ongoing Information Security Awareness training program to educate employees and all other personnel with access to OAG data and information systems about data security and the protection of OAG information resources. This training will include the establishment of security awareness and familiarization with OAG security policies and procedures through both New Employee Orientation and ongoing refresher training.

#### **4.10. Warning Statements**

System identification screens will be provided at the time of initial logon to the mainframe or LAN/WAN. These screens will provide the following warning statements:

- Unauthorized use is prohibited.
- Usage may be subject to security testing and monitoring.
- Misuse may be subject to disciplinary action.
- No expectation of privacy is to be anticipated by the user.

#### **4.11. Termination of Employment**

Computer user identifications (User IDs) for employees that have voluntarily terminated employment with the OAG must be removed from the computer system immediately following termination. For involuntary terminations, the ID should be removed prior to, or at the same time the employee is notified of the termination in order to protect OAG data and information assets.

#### **4.12. Automatic Suspension / Deletion of User ID's**

Mainframe, LAN and Remote Access User IDs will be monitored for usage to protect system security, and any unused user IDs will be subject to automatic suspension after 30 days, and deletion after 60 days without notice to the user, unless an exception has been approved in accordance with this policy.

#### **4.13. Positions of Special Trust**

The ISOs will establish procedures for reviewing information resource functions to determine which positions require special trust or responsibilities. These include, but are not limited to:

- Network and system administrators;
- Users with access to information systems that process or contain federal tax information;
- Users with access to child support systems and data that may include federal tax information;
- Users with access to financial and accounting systems or networks;
- Any user with agency-wide access to data and information systems; and
- Any user required to undergo a background check as a prerequisite to employment or grant of system access.

## **5. Technical Security Controls**

### **5.1. System Security Policy**

The following policies cover specific issues as they relate to the security of information systems and data within the OAG, and are governed by the procedures outlined in the OAG Information Security Procedures Manual.

### **5.2. System Administrators**

System administrators are responsible for adding, removing or modifying user accounts as employees change roles within the agency. This activity must be accomplished in a timely manner to ensure only authorized personnel have access to OAG systems and information. Changes to user accounts may be subject to independent audit review.

### **5.3. System Developers**

All production software development and software maintenance activities performed by in-house staff must adhere to agency security policies, standards, procedures, and other systems development conventions including appropriate testing, training and documentation.

#### **5.4. Information Technology Asset Protection**

OAG data and information technology assets will be protected from unauthorized access, use, modification or destruction through the deployment of protective measures. The design, acquisition and use of all protective measures must be reviewed and approved by the appropriate ISO.

#### **5.5. Vendor Access to OAG Systems**

Access to OAG systems and data by vendors (including contractors, sub-contractors, auditors, consultants or agents) must be appropriately controlled depending on the work to be performed, sensitivity levels of the data involved, work location, and other relevant considerations. All requests for vendor access must be coordinated with and approved by the appropriate IT department and ISO prior to access being granted.

#### **5.6. Classification of Electronic Data and Assets**

OAG electronic data and the information technology assets used to process, transmit, and store it should be assigned an appropriate classification level to assist in the proper safeguarding of the data. As higher classification levels require the agency to incur greater costs in order to safeguard data, care should be taken to accurately classify assets. Assets of varying classifications that are co-mingled in a single database or file system shall be classified at the highest level of the information contained in the data.

For the limited purposes of this policy, the OAG has two classifications of electronic data:

- **CONFIDENTIAL AND SENSITIVE** - This classification includes data that may be deemed confidential or protected by Texas or federal laws and/or administrative rules, and sensitive information, which if subject to a security breach, could compromise the agency's business functions or the privacy or security of agency employees, clients, or partners. Information in this category may only be provided to external parties in accordance with OAG policies and procedures.
- **UNCLASSIFIED** - This refers to all data that does not meet the requirements for **CONFIDENTIAL AND SENSITIVE** as described herein, as designated by the originating source of the data and/or the originator of any derivative data with guidance from 1 TAC § 202.1(3); DIR Classification Guidance, and any other applicable regulation or law.
- The default classification for all electronic data is **CONFIDENTIAL AND SENSITIVE**.

#### **5.7. Data Destruction**

OAG data should only be destroyed in accordance with the applicable records retention schedule, or upon the receipt of proper authorization from the State Library and Archives Commission. OAG data contained on magnetic or optical media must be removed from the media prior to the media being transferred out of the control of the authorized user, or the media must be physically destroyed in accordance with the appropriate document destruction guidelines applicable to that information.

## **5.8. Configuration Management**

Configuration management (CM) is the process of managing the effects of changes or differences in configurations of an information system or network through the implementation of strict protocols and testing in order to reduce the risk of changes resulting in a compromise to data security, confidentiality, integrity, or availability. All systems will be configured and maintained only in accordance with approved IT and Information Security configuration management (CM) guidelines.

## **5.9. Change Management**

Change management refers to the safeguards and procedures established for making modifications to OAG systems and networks. All such modifications must be processed through the appropriate change control procedure, with any OAG systems residing at a Consolidated Data Center (CDC) additionally being subject to the DIR and its contractor change management process.

## **5.10. Data Integrity**

Data integrity refers to ensuring that data remains complete and unchanged during the course of any electronic processing, transfer, storage, or retrieval. To promote data integrity, individual users of OAG information assets must follow data integrity procedures applicable to their level of user access to OAG data, and take adequate precautions to safeguard against the loss of OAG data, including but not limited to:

- Performing regular backups of OAG data as may be appropriate;
- Taking physical and procedural safeguards to avoid the accidental loss, destruction or unauthorized modification of OAG data;
- Ensuring proper and routine use of virus protection software/anti-malware; and
- Coordinating with and seeking assistance from IT personnel as may be appropriate to safeguard OAG data.

## **5.11. Voice/Phone Mail**

The OAG's voice or phone mail systems use agency information assets. Accordingly, each user is responsible for ensuring that use of these services is in compliance with applicable law, policy and procedures. All requests for changes, modifications, or termination of voicemail services must be initiated through the ITS Division.

## **5.12. E-mail**

Electronic mail (e-mail) is a form of communication that uses agency information assets. All use of e-mail must be in accordance with OAG policies and procedures regarding the use of information assets.

Upon the OAG's implementation of an agency-approved email encryption process, employees may not send CONFIDENTIAL AND SENSITIVE OAG data in the body of an email or as an email attachment across unsecured connections such as the Internet, unless it is encrypted using a process approved by both the appropriate IT Director and ISO.

### **5.13. Wireless Systems**

Wireless networks or routers may not be used without the prior authorization of both the appropriate IT Director and ISO. All wireless connectivity (Wi-Fi) to OAG networks must be in accordance with current IT architectural direction, Information Technology Security Policy, and OAG policies and procedures relating to the use of mobile telecommunications devices.

### **5.14. Copyright**

Generally, the reproduction of copyrighted information is a violation of federal law. Therefore, OAG information assets should not be used to reproduce copyrighted information. Unauthorized copies of software shall not be loaded or executed on OAG information technology assets. Regular audits will be conducted to search for unauthorized software installed on machines.

### **5.15. Personal Software, Shareware and Freeware**

Personal software, shareware and freeware may not be loaded or otherwise used on OAG systems unless there is a business necessity for the use of such programs, and their installation and use is specifically approved by both the appropriate IT Director and ISO.

### **5.16. Data Encryption**

All OAG laptops must have encrypted hard drives to safeguard data in the event the device is lost or stolen. Those divisions who choose to employ data encryption for transmission or storage of CONFIDENTIAL AND SENSITIVE data shall adopt the 256 bit Advanced Encryption Standard (AES), or 128 bit Single Sockets Layer (SSL/TLS) as a minimum. No encryption will be used without the prior approval of both the appropriate IT Director and ISO.

### **5.17. Portable and Mobile Devices**

All laptops and other mobile telecommunications devices (PDAs, network capable cell phones, BlackBerry's, etc.) must be approved for use and supplied by the appropriate ITS Division. Only OAG laptops installed with full-disk encryption, anti-malware safeguards, and secure connectivity are authorized for use with OAG data and networks.

### **5.18. Malware Protection Software**

All workstations and laptops must use approved malware protection software and configurations, regardless of whether they are connected to OAG networks or are used as a standalone device. Additionally, each file server attached to the OAG network and each e-mail gateway must utilize OAG IT-approved e-mail malware protection software and/or hardware. Users shall not alter, disable, bypass, or adjust any settings or configurations for OAG malware protection software in any manner.

### **5.19. Intrusion Detection**

Intrusion detection techniques will be deployed wherever possible in order to safeguard against unauthorized attempts to access, manipulate, or disable OAG networks. Intrusion detection activities may be conducted only by specially-trained personnel within the OAG using techniques approved by the appropriate ISO.

## **5.20. Internal Electronic Investigations**

All internal electronic investigations must be authorized by, and conducted under the supervision of, the appropriate ISO unless otherwise approved by the First Assistant Attorney General. No other investigation is authorized on OAG systems or networks. Any unauthorized electronic investigation or monitoring discovered on OAG systems or networks will be reviewed by the Information Security Division and may result in disciplinary action up to and including termination of employment.

## **5.21. Screen Savers**

To reduce the likelihood of unauthorized access to OAG data, systems and networks, all OAG workstations, including laptop computers, must be configured to activate password-protected screensavers after no more than fifteen minutes of user inactivity. An employee should not leave his or her workstation unless the password-protected screensaver has been activated or, if possible, the workstation has been secured by a locked door.

## **5.22. User Passwords**

Systems that use passwords shall follow the standards on password usage prescribed by DIR found at <http://www2.dir.state.tx.us/security/policy/Pages/policy.aspx>. This document specifies minimum criteria and provides guidance for selecting additional password security criteria. Disclosure of an individual's password or use of an unauthorized password or access device may result in disciplinary action up to and including termination of employment.

## **5.23. Administrator Passwords**

All system administrators will maintain and use both a standard user password and a system administrator password ("super user" password). The system administrator password will be used only for system administrator activities. All common applications and system activities (email, calendar, etc.) must be accessed by the system administrator only with their standard user password.

## **5.24. System Log On & Re-Boot**

All OAG workstations, including laptop computers, must be connected to the OAG network at least once weekly in order to receive appropriate application updates and security patches. Additionally, all systems must be re-booted (shut down and restarted) at least once a week to ensure these updates and patches are installed appropriately.

## **5.25. System Settings**

All OAG systems are specifically configured to ensure that users have the appropriate ability to perform assigned tasks. Users shall not modify, change or attempt to change any system settings. If additional user access, permissions or system setting changes are required, then a request for the modification must be approved by the user's manager and submitted to the appropriate IT Division for handling.

## **5.26. Control of Peripherals**

A peripheral device is any device attached to a computer in order to expand its functionality, such as USB flash drives, CD burners, or PCMCIA card slots. The ability to use peripheral

devices may be controlled on some OAG systems; users are not authorized and should not attempt to change control settings in order to use peripheral devices on these systems. Adding or deleting peripherals on these systems may only be accomplished by IT personnel.

### **5.27. Security Breaches**

A security breach is defined as any event which results in loss, disclosure, unauthorized modification, or destruction of information resources. Users shall immediately report all actual or suspected security breaches to their Division Chief and the ISO responsible for their division. The responsible ISO will promptly report the suspected or actual security breach to the appropriate IT Director and IRM. Depending on the nature of the information involved, additional procedures may be required in accordance with the Sensitive Personal Information Privacy Policy.

### **5.28. Dial-up Access**

For dial-up access to OAG systems other than access authorized for the public, information security protocols shall be employed to positively and uniquely identify authorized users and authenticate user access to the requested system. All modems used for dial-up access to OAG systems must be authorized by the appropriate IT Director and ISO.

### **5.29. Purchasing/Development Pre-Approval**

All OAG purchases, acquisitions, or developments of information technology services, equipment or software must be reviewed and pre-approved by the appropriate ISO to determine whether the purchase may negatively impact OAG information technology security. All purchases of information technology security products, or products with information technology security functionality or impact, must be approved by the IRM and appropriate ISO prior to the issuance of a purchase order.

### **5.30. Contract Security Provisions**

All third-party contracts must contain appropriate language to ensure the security of OAG information to which the third-party may have access, even if such access is limited to encrypted data. This language must state in clear and unambiguous terms the security requirements placed on the third-party involved, and their responsibilities for security under the contract. It must also clearly state OAG's authority to audit their security procedures for appropriateness during the length of the contract.<sup>xii</sup>

All contracts to which the OAG is a party and that affect OAG information technology security must be reviewed and approved by the appropriate ISO prior to execution in order to ensure that appropriate security controls are included.

### **5.31. System Development, Acquisition and Testing**

Data and network security requirements must be considered and addressed in all phases of the development or acquisition of new information processing systems. Before being placed into use, all new systems must be properly tested in order to ensure compatibility with OAG information systems and the OAG computing environment. During system testing, test functions shall be

kept either physically or logically separate from production functions in order to safeguard OAG data and information technology systems.

## **6. Exception, Waiver and Modification**

### **6.1. Waivers and Exceptions**

Waivers and exceptions to the existing information security policies and procedures are strongly discouraged because they may pose an unacceptable risk to protected OAG data and systems. Prior to implementation, all exceptions or waivers of existing security policies or procedures must be reviewed and approved by the IRM, appropriate IT Director, appropriate ISO, and reported to the Records Management Officer.

- A waiver is a variance of a control standard that is limited to a specific period of time and to a specific system in order to allow IT personnel to perform an approved change or modification to OAG systems.
- An exception is an indefinite variance from a control standard supported by a valid and ongoing business justification.

### **6.2. Modification or Significant Changes to Procedures**

All changes in the procedures to protect OAG IT systems and data must be reviewed by the appropriate IT Director and approved by the appropriate ISO prior to implementation. If immediate changes to procedures are required to meet an emergency situation, A&L and/or CS ISO, and the Records Management Officer must be informed as soon as possible thereafter.

### **6.3. Executive Management Waiver**

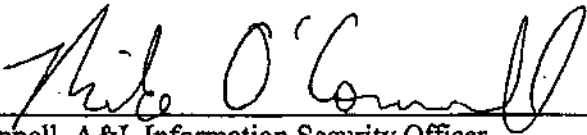
Notwithstanding any provisions to the contrary contained herein, waivers, exceptions and modifications to the information security policies and procedures may be authorized in writing at the discretion of the First Assistant Attorney General.

## 7. Document Acceptance and Release Notice

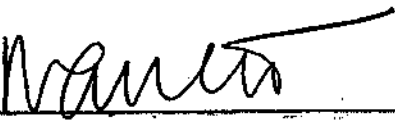
This is Version 4.2 of the OAG Information Security Division Security Policy Manual.

The OAG Information Security Division Security Policy Manual is a managed document. Changes will be issued only as a complete replacement document. Recipients should remove superseded versions from circulation. This document is authorized for release after all signatures have been obtained.

Please submit all requests for changes to the owner/author of this document.

OWNER:  DATE: April 5, 2011  
Mike O'Connell, A&L Information Security Officer

OWNER:  DATE: April 5, 2011  
Kathleen Donaho-Jaeger, CSD Information Security Officer

EXECUTIVE SPONSOR:  DATE: April 5, 2011  
Diane B. Smith, Deputy for Administration and Information Resources Manager

## 8. References

- 
- <sup>i</sup> Tex. Gov't Code § 2054.003(7).
  - <sup>ii</sup> 1 TAC § 202.20.
  - <sup>iii</sup> 1 TAC § 202.1
  - <sup>iv</sup> 1 TAC § 202.21.
  - <sup>v</sup> 1 TAC § 202.21.
  - <sup>vi</sup> 1 TAC § 202.21.
  - <sup>vii</sup> 1 TAC § 202.27.
  - <sup>viii</sup> *See generally*, 1 TAC Chapter 202.
  - <sup>ix</sup> 1 TAC § 202.21.
  - <sup>x</sup> 1 TAC § 202.1.
  - <sup>xi</sup> 1 TAC § 202.26.
  - <sup>xii</sup> 1 TAC § 202.25(6)(B).