

Information Security Policy Manual

THIS PAGE INTENTIONALLY LEFT BLANK

Table of Contents

0.	Executive Summary	4
1.0	Policy:	5
1.1	Program Policy:	5
1.2	Scope of Policy:	5
1.3	Issue-Specific Policy:	5
1.3.1	<u>Use of OAG Information Resources:</u>	5
1.3.2	<u>Classification of Information (Data) Assets:</u>	5
1.3.3	<u>Information Asset Protection:</u>	5
1.3.4	<u>Access to OAG Information Assets:</u>	6
1.3.5	<u>Data Integrity:</u>	6
1.3.6	<u>E-Mail:</u>	6
1.3.7	<u>Copyright:</u>	6
1.3.8	<u>Personal Hardware and Software:</u>	6
1.3.9	<u>Shareware and Freeware:</u>	6
1.3.10	<u>Asset Protection:</u>	7
1.3.11	<u>Voice/Phone Mail:</u>	7
1.3.12	<u>Data Encryption and Key Management:</u>	7
1.3.13	<u>Security Awareness:</u>	7
1.3.14	<u>Risk Analysis and Risk Management:</u>	8
1.3.15	<u>Contingency Planning:</u>	8
1.3.16	<u>Termination and Transfers:</u>	8
1.3.17	<u>Bulletin Board Access:</u>	8
1.3.18	<u>Internet Policy:</u>	8
1.3.19	<u>Passwords:</u>	9
1.3.20	<u>Security Breaches:</u>	9
1.3.21	<u>Data Communications Systems:</u>	9
1.3.22	<u>Dial-Up Access:</u>	9
1.3.23	<u>User Identification:</u>	9
1.3.24	<u>Warning Statements:</u>	10
1.3.25	<u>System Development and Testing:</u>	10
1.3.26	<u>Statement of Responsibility:</u>	10
1.3.27	<u>Automatic Suspension / Deletion of User ID's:</u>	10
1.3.28	<u>Physical Security:</u>	10
1.3.29	<u>Positions of Special Trust:</u>	10

0. Executive Summary

The Office of Attorney General [OAG] has a commitment to the citizens of Texas to ensure that the information entrusted to them will be reasonably secure and protected. Unauthorized use of any kind must not be tolerated and such use should be punishable to the fullest extent of the law. An effective information security program takes a lot of work, commitment and cooperation among the employees of OAG. We are all involved in the well-being of this strategic effort. The Information Security Officer for your division (i.e., CSD or A&L) may be contacted for further information as required.

Purpose

The intent of the *OAG Information Security Policy Manual* is threefold:

- 2) comprehensive documentation of the current information security and contingency planning policies as determined by management;
- 3) education for the users on the proper usage of OAG information assets; and
- 4) legal ramifications of the misuse of information assets.

The Challenging OAG Environment

Information asset protection and contingency planning are becoming two of the more complex challenges of the modern automated environment. Our automation systems consist of large central databases, over one hundred (100) Local Area Networks (LAN) and one of the largest Wide Area Networks (WAN) in the State of Texas. Our network is now tied to the Internet, and other State and federal agencies as required.

Information Asset Protection and Disclosure

As technology becomes more prolific, the chance of OAG information assets becoming destroyed, modified or disclosed, either intentionally or inadvertently, becomes more prevalent. The Texas Administrative Code I TAC 201.13 (b) indicates a required classification and ownership methodology under the Texas Public Information Act.

Security Awareness Program

A comprehensive security awareness program has been established for all OAG personnel. It is incumbent upon each OAG employee, consultant or contractor to be familiar with the *Information Security Policy Manual* and associated procedures in his or her respective area.

Contingency Planning

Finally, the OAG is charged with providing a comprehensive contingency plan and disaster recovery procedures for all data center, and field operations. Information security "ownership," classification, access and controls, resulting risk assessment and criticality analyses are used as a basis for business resumption planning.

1.0 Policy

1.1 Program Policy:

Information and information resources residing in the Office of the Attorney General (OAG) are strategic and vital assets belonging to the people of Texas. These assets require a degree of protection commensurate with their value. Measures will be taken to protect these assets against accidental or unauthorized disclosure, modification or destruction, as well as to assure the security, reliability, integrity and availability of information.

1.2 Scope of Policy:

This policy applies to all information resources that are used by or for the OAG. It applies to information processing systems throughout their life cycle. This policy also applies to all users (manager, employees, contractors, etc.) of OAG information assets.

1.3 Issue-Specific Policy:

The following are the policies that cover specific issues as they relate to the security of information within the OAG.

1.3.1 Use of OAG Information Resources:

State information resources will be used only for official State purposes. Compliance with this policy will be monitored via periodic maintenance, scheduled and random audits. The individual user of OAG information resources shall have no expectation of privacy for information contained within or processed by an OAG information resource.

1.3.2 Classification of Information (Data) Assets:

All information processed by or for the OAG is of value and therefore will be classified. The OAG has three levels of data classification. They are confidential, sensitive and unclassified. Further detailed descriptions of these classifications can be found in the "Information Classifications" section of the Information Security Procedure Manual.

1.3.3 Information Asset Protection:

Information which is confidential or sensitive will be protected from unauthorized access or modification. Data which is essential to critical State functions must be protected from loss, contamination or destruction. The expense of security safeguards will be appropriate to the value of the assets being protected.

1.3.4 Access to OAG Information Assets:

Access to OAG information resources must be strictly controlled. State law requires that State owned information resources be used only for official State purposes. Read access to OAG information is on a need-to-know basis. When access by the user requires the use of a password, or other security measure, that security measure must be kept confidential by the intended user.

1.3.5 Data Integrity:

The integrity of data, its source, its destination and processes applied to it must be assured. The creation or modification of OAG information may only be performed by authorized personnel. Each user will be individually accountable for his/her actions when handling, processing, or otherwise using OAG information.

1.3.6 E-Mail:

Electronic mail (e-mail) is a form of communication which uses information assets. However, as with the use of phones (excluding long distance) employees may use the e-mail system for communicating with OAG employees on non official business provided such communication does not disrupt or interfere with official State business, is kept to a minimum duration and frequency, and is not political in nature.

1.3.7 Copyright:

OAG information assets shall not be used to produce illegal copies of copyrighted information. Illegal copies of software shall not be loaded or

executed on OAG information systems. Regular audits will be conducted to search for unauthorized software installed on machines.

1.3.8 Personal Hardware and Software:

No personal programs of any kind are to be loaded onto any State computer. Hardware provided by the user may not be used at the OAG or connected to the OAG's networks.

1.3.9 Shareware and Freeware:

Shareware and freeware will not be loaded or otherwise used on OAG systems unless specifically approved by the Information Resource Manager.

1.3.10 Asset Protection:

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

1.3.11 Voice/Phone Mail:

Voice or phone mail is a form of communication which uses information assets. However, employees may use the voice mail system for communicating with other OAG employees and personal business provided such communication does not disrupt or interfere with official State business, is kept to a minimum duration and frequency, and is not political in nature.

1.3.12 Data Encryption and Key Management:

It is not a requirement at this time for agencies to use data encryption techniques for storage and transmission of data. However, those agencies who choose to employ data encryption shall adopt the data encryption standard, also referred to as the DES algorithm, which is defined in the Federal Information Processing Standard Publication 46-2 (FIPS PUB 46-2). Any use of encryption by OAG staff must be approved in advance by their

Division Director. For systems employing encryption as described, procedures shall be prescribed for secure handling, distribution, storage and construction of DES key variables used for encryption and decryption. Protection of the key shall be at least as stringent as the protection required for the information encrypted with the key. Copies of the FIPS PUB 46-2 are available from the Information Security Officer (ISO).

1.3.13 Security Awareness:

The OAG will provide an ongoing awareness and training program in information security and in the protection of State information resources for all personnel whose duties bring them into contact with confidential or sensitive data. New employee orientation will be used to establish security awareness and inform new employees and contractors information security policies and procedures. Information security programs must be responsive and adaptable to changing vulnerabilities and technologies affecting State information resources.

1.3.14 Risk Analysis and Risk Management:

Risks to information resources must be managed. The OAG will perform a comprehensive risk analysis of all information processing systems on a periodic basis. Risk analysis results will be presented to the owner of the information resource for risk management.

1.3.15 Contingency Planning:

All information resources determined by agency management to be essential to the agency's critical mission and functions, shall have a written and cost-effective contingency plan. The contingency plan shall be tested and updated annually to assure that it is valid and current. Backups of data and software will be maintained to mitigate the impact of such a disaster. A disaster declaration will be issued by the Attorney General in the event that a disaster destroys or makes inoperable a significant portion of the processing capability of the OAG. This declaration will authorize the Information Resource Manager to make timely decisions in the recovery of the information assets.

1.3.16 Termination and Transfers:

Computer user identifications (User ID's) for employees that have terminated employment with the OAG must be removed from the computer system immediately following termination notification. If the agency is terminating the employee, the ID should be removed prior to or at the same time of the employee being notified of the termination. For employees transferring to another position and/or section within the OAG, the user ID should also be removed immediately.

1.3.17 Bulletin Board Access:

Users of OAG information assets are authorized to access electronic bulletin boards in performance of their duties, but they remain responsible for ensuring that all security precautions and policies are followed. Policies 1.3.6 & 1.3.7 on personal software and freeware and shareware still apply to anything that is downloaded from bulletin boards (including Texas State bulletin boards).

1.3.18 Internet Policy:

The OAG has provided e-mail access to the Internet for all employees. Employees should use caution and are responsible for his or her actions when using this medium. Web browser access should be limited to those areas relevant to your job functions. Web access to non-job related sites represents an unauthorized use of government time, property and facilities. Employees violating this policy are subject to disciplinary action, up to and including dismissal from the Agency.

CAVEAT: The OAG has implemented reasonable security measures to protect staff when using the Internet. However, the OAG cannot guarantee the security when using this system. Therefore, confidential and sensitive information will not be transferred using this medium.

1.3.19 Passwords:

Systems which use passwords, shall follow the OAG guidelines based upon the federal standard on password usage contained in the Federal Information Processing Standard Publications 112 (FIPS PUB 112), which specifies minimum criteria and provides guidance for selecting additional password security criteria, when appropriate. Copies of FIPS PUB 112 are available

from the Information Security Officer. Disclosure of an individual's password or use of an unauthorized password or access device may be punishable under both State and Federal law.

1.3.20 Security Breaches:

Any event which results in loss, disclosure, unauthorized modification, or unauthorized destruction of information resources constitutes a security incident or breach. Users should report any security breaches immediately to the ISO, who will promptly investigate the incident. If criminal action is suspected, the agency must contact the appropriate local law enforcement and investigative authorities immediately.

1.3.21 Data Communications Systems:

Network resources (LAN-WAN-Mainframe) that access confidential or sensitive information will assume the security level of that information for the duration of the session. All network components under State control must be identified and restricted to their intended use.

1.3.22 Dial-up Access:

For services other than those authorized for the public, authorized users of dial-up access shall be positively and uniquely identifiable and their identity authenticated to the systems being accessed.

1.3.23 User Identification:

Except for public users of systems where such access is authorized, or for situations where risk analysis demonstrates no need for individual accountability of users, each user of a multiple-user automated system shall be assigned a unique personal identifier or user identification.

1.3.24 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:

- (i) unauthorized use is prohibited;
- (ii) usage may be subject to security testing and monitoring; and
- (iii) abuse is subject to criminal prosecution.

1.3.25 System Development and Testing:

Security needs must be considered and addressed in all phases of development or acquisition of new information processing systems.

Test functions shall be kept either physically or logically separate from production functions.

1.3.26 Statement of Responsibility:

All OAG personnel shall be required to provide written acknowledgment that they have received, read and understand the Information Security Policy Manual.

1.3.27 Automatic Suspension / Deletion of User ID's:

Mainframe, LAN and Remote Access ID's will be monitored for usage. Unused ID's pose a security threat and will be subject to suspension after 30 days and deletion after 60 days, without notice to the user.

1.3.28 Physical Security:

Management reviews of physical security measures will be conducted annually, and when significant modifications are made to the facilities or security procedures.

Physical access to mainframe computer and file server rooms will be restricted to authorized personnel. Authorized visitors will be required to record their visits via a sign-in / sign-out log.

1.3.29 Positions of Special Trust:

The OAG will establish procedures for reviewing information resource functions to determine which positions require special trust or responsibilities.





ATTORNEY GENERAL OF TEXAS GREG ABBOTT

My Account Logout

Agreements

Statement

OFFICE OF THE ATTORNEY GENERAL: AUTOMATED COMPUTER SYSTEM ACCESS STATEMENT OF RESPONSIBILITY

General Information:

All information maintained in the files and records of the Child Support Division are privileged and confidential. The unauthorized use or release of the information can result in criminal prosecution and civil liability. Only authorized personnel may add, modify and/or delete information.

Statements:

I understand that the information concerning any person, customer or client that may come to my knowledge while using the computer system of the TxCSDU or TXCSES or any other OAG computer shall be held in strictest confidence and may not be disclosed except as used exclusively for purposes directly connected with the administration of programs under Title IV-A, IV-D and XIX of the federal Social Security Act and the OAG Confidentiality Policy and Procedures.

Notwithstanding the above, I understand that I may not disclose to any individual or agency any federal tax return or return information. I further understand that it is unlawful to offer or receive anything of value in exchange for federal tax return or return information. Such unauthorized disclosure or exchange is punishable by fine up to \$5,000, or imprisonment up to 5 years, or both, under Internal Revenue Code 7213 and 7213 A. Accessing federal tax information without a "need to know" is a federal misdemeanor punishable by not more than one year imprisonment, or a \$1000 fine or both, plus costs of prosecution, under 7213 A, Internal Revenue Code. I also understand that I may be civilly liable for damages of not less than \$1000 per violation, together with costs of prosecution under Section 7431 of the Internal Revenue Code.

I also understand that I may not release information to any committee or legislative body (federal, state, or local) that identifies by name or address any such applicant or recipient of services. Use of such information by a local government or component thereof for any other purpose, including but not limited to, collecting a fee is prohibited.

I understand that I may not perform any work, review, update or otherwise act to obtain information upon my own, or any relative's, friend's, or business associate's child support case, regardless if the case is open or closed. My failure to comply with the OAG Confidentiality Policy will result in immediate termination of my computer access. I also understand that a violation will be reported to my supervisor or other appropriate personnel in my agency for disciplinary action, which may include termination and/or referral for prosecution.

In addition, if applicable, I understand that the computer password(s) I receive or devise is confidential, and must not be disclosed to anyone. I understand that it is my responsibility to safeguard such password(s) by not allowing it to be viewed by anyone. I understand that I am responsible for computer transactions performed through misuse of my password(s).

I agree I will not load unauthorized software, personal computer programs, shareware or freeware of any kind onto the OAG computer equipment without the express written approval of the Office of the Attorney General, Information Resource Manager or designee, or the contract manager or designee. I understand that use of a password not issued or devised specifically for me is expressly prohibited and is a violation of state and federal law.

I also understand that failure to observe the above conditions may constitute a "breach of computer security" as defined in the TEXAS PENAL CODE, CHAPTER 33, Section 33.02 (b), and that such an offense may be classified as a felony. Similar federal statutes may also be applicable.

I certify that I understand that any copyrighted material, including but not limited to commercial computer software, which may be made available to me for use by the OAG is protected by copyright laws and is not to be copied for any reason without written permission from the owner of the copyright and the OAG.

By agreeing to this statement I certify that I:

- agree to abide by all written conditions imposed by the OAG regarding information security;
- understand my responsibilities as described above;
- have received, read and understand the OAG security information policy manual; and
- if applicable, I have read all applicable software licenses and agree to abide by all restrictions.

I Agree

I Disagree

[Portal Tips](#) | [Accessibility](#) | [Privacy & Security Policy](#)



ATTORNEY GENERAL OF TEXAS GREG ABBOTT

My Account Logout

Agreements

Policy

When you register for the OAG Portal Service, we may ask you to give us certain identifying information ("Registration"), such as your name, address, and e-mail or the company's name and address and the company representative's name and e-mail address. This information will be used solely for Child Support IV-D purposes.

You agree to provide true, accurate, current and complete information about yourself. You also agree not to impersonate any person or entity, misrepresent any affiliation with another person, entity or association, use false headers or otherwise conceal your identity from the OAG for any purpose.

For your protection and the protection of our other members and Web site users, you agree that you will not share your Registration information (including passwords, User Names, and screen names) with any other person for the purpose of facilitating their access and unauthorized use of OAG Portal Services. You alone are responsible for all transactions initiated, messages posted, statements made, or acts or omissions that occur within any OAG Portal Service through the use of Registration information. Your failure to honor any portion of this agreement can result in termination of access to Portal Services.

I Agree

I Disagree

[Portal Tips](#) | [Accessibility](#) | [Privacy & Security Policy](#)

Data Integrity Procedures Changes to Case Information

Before updating member/ case information, such as home address, phone number, etc., verify the caller's identity. Ask the caller for the following identifiers:

- Name
- Date of Birth
- Home address

If there is any doubt about the caller's identity after these identifier's have been obtained, ask for the children names and date of birth.

When pertinent information is unavailable on registry-only (RO) cases, county staff are prevented from verifying a caller's identity. Once all attempts to verify the caller's identity have been exhausted, instruct the caller to take one of the following actions in order to have the member/case information updated on TXCSESWeb:

• **Mail:**

- a copy of a photo ID
- information to be updated
- proof/verification of the information to be updated (ie., home address, SSN card, drivers license, etc.) to the county address

• **FAX:**

- a photo ID
- information to be updated
- proof/verification of the information to be updated (ie., home address, SSN card, drivers license, etc.) to the county FAX number

• **E-mail the information** to be updated with a scanned copy of the proof/verification information to be updated (ie., home address, SSN card, drivers license, etc.) to the county email address

• **In Person (District Clerk Office or Domestic Relations Office):**

- a photo ID
- information to be updated
- proof/verification of the information to be updated (ie., home address, SSN card, drivers license, etc.)

• **Visit the local child support office** that is assigned to work the RO case and provide:

- a photo ID
- information to be updated
- proof/verification of the information to be updated (ie., home address, SSN card, drivers license, etc.)

**CERTIFICATION REGARDING LOBBYING
DEPARTMENT OF HEALTH AND HUMAN SERVICES
ADMINISTRATION FOR CHILDREN AND FAMILIES**

**PROGRAM: CHILD SUPPORT ENFORCEMENT PROGRAM PURSUANT TO TITLE IV-D
OF THE SOCIAL SECURITY ACT OF 1935 AS ADMINISTERED BY THE OFFICE OF THE
ATTORNEY GENERAL OF TEXAS**

PERIOD: September 1, 2007 - August 31, 2009

Certification for Contracts, Grants, Loans and Cooperative Agreements

The undersigned certifies, to the best of his or her knowledge and belief, that:

- (1) No Federal appropriated funds have been paid or will be paid by or on behalf of the undersigned, to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an office or employee of Congress, or an employee of a Member of congress in connection with the awarding of any Federal contract, the making of any Federal grant, the making of any Federal loan, the entering into of any cooperative agreement, and the extension, continuation, renewal, amendment, or modification of any Federal contract, grant, loan, or cooperative agreement.
- (2) If any funds other than Federal appropriated funds haven been paid or will be paid to any person for influencing or attempting to influence an office or employee of any agency, a Member of congress, an officer or employee of Congress, or an employee of Member of Congress in connection with this Federal contract, grant, loan, or cooperative agreement, the undersigned shall complete and submit standard Form LLL, "Disclosure Form to Report Lobbying," in accordance with its instructions.
- (3) The undersigned shall require that the language of this certification be included in the award documents for all subawards at all tiers (including subcontracts, subgrants, and contracts under grants, loans, and cooperative agreements) and that all subrecipients shall certify and disclose accordingly.

This certification is a material representation of fact upon which reliance was placed when this transaction was made or entered into. Submission of this certification is a prerequisite for making or entering into this transaction imposed by Section 1352, Title 31, U.S. Code. Any person who fails to file the required certification shall be subject to a civil penalty of not less than \$10,000 and not more than \$100,000 for each such failure.

Signature

Date

Agency/Organization

Date

United States Internal Revenue Service Requirements for the Safeguarding of Federal
Tax Information Including Federal Tax Returns and Return Information

#.1. PERFORMANCE

#.1.1. In performance of this contract, the contractor agrees to comply with and assume responsibility for compliance by his or her employees with the following requirements:

#.1.2. All work will be done under the supervision of the contractor or the contractor's employees.

#.1.3. Any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material will be treated as confidential and will not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Disclosure to anyone other than an officer or employee of the contractor will be prohibited.

#.1.4. All returns and return information will be accounted for upon receipt and properly stored before, during, and after processing. In addition, all related output will be given the same level of protection as required for the source material.

#.1.5. The contractor certifies that the data processed during the performance of this contract will be completely purged from all data storage components of his or her computer facility, and no output will be retained by the contractor at the time the work is completed. If immediate purging of all data storage components is not possible, the contractor certifies that any IRS data remaining in any storage component will be safeguarded to prevent unauthorized disclosures.

#.1.6. Any spoilage or any intermediate hard copy printout that may result during the processing of IRS data will be given to the agency or his or her designee. When this is not possible, the contractor will be responsible for the destruction of the spoilage or any intermediate hard copy printouts, and will provide the agency or his or her designee with a statement containing the date of destruction, description of material destroyed, and the method used.

#.1.7. All computer systems processing, storing, or transmitting Federal tax information must meet the requirements defined in IRS Publication 1075. To meet functional and assurance requirements, the security features of the environment must provide for the managerial, operational, and technical controls. All security features must be available and activated to protect against unauthorized use of and access to Federal tax information.

#.1.8. No work involving Federal tax information furnished under this contract will be subcontracted without prior written approval of the IRS.

#.1.9. The contractor will maintain a list of employees authorized access. Such list will be provided to the agency and, upon request, to the IRS reviewing office.

United States Internal Revenue Service Requirements for the Safeguarding of Federal Tax Information Including Federal Tax Returns and Return Information
#.1.10. The agency will have the right to void the contract if the contractor fails to provide the safeguards described above. (NOTE TO DRAFTER: Include any additional safeguards that may be appropriate.)

#.2. CRIMINAL/CIVIL SANCTIONS

#.2.1. Each officer or employee of any person to whom returns or return information is or may be disclosed will be notified in writing by such person that returns or return information disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any such returns or return information for a purpose or to an extent unauthorized herein constitutes a felony punishable upon conviction by a fine of as much as \$5,000 or imprisonment for as long as 5 years, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized further disclosure of returns or return information may also result in an award of civil damages against the officer or employee in an amount not less than \$1,000 with respect to each instance of unauthorized disclosure. These penalties are prescribed by IRC sections 7213 and 7431 and set forth at 26 CFR 301.6103(n)-1.

#.2.2. Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing by such person that any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of the contract. Inspection by or disclosure to anyone without an official need to know constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as \$1,000 or imprisonment for as long as 1 year, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized inspection or disclosure of returns or return information may also result in an award of civil damages against the officer or employee [United States for Federal employees] in an amount equal to the sum of the greater of \$1,000 for each act of unauthorized inspection or disclosure with respect to which such defendant is found liable or the sum of the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure plus in the case of a willful inspection or disclosure which is the result of gross negligence, punitive damages, plus the costs of the action. These penalties are prescribed by IRC section 7213A and 7431.

#.2.3. Additionally, it is incumbent upon the contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to contractors by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a contractor, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is prohibited, willfully discloses the material in

United States Internal Revenue Service Requirements for the Safeguarding of Federal Tax Information Including Federal Tax Returns and Return Information
any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than \$5,000.

#.3. INSPECTION

#.3.1. The IRS and the Agency shall have the right to send its officers and employees into the offices and plants of the contractor for inspection of the facilities and operations provided for the performance of any work under this contract. On the basis of such inspection, specific measures may be required in cases where the contractor is found to be noncompliant with contract safeguards.

____ COUNTY

INCIDENT RESPONSE PLAN

Adopted _____, 2008

SAMPLE

Overview..... 3
Incident Response Team..... 3
Incident Response Team Roles and Responsibilities..... 4
Incident Contact List..... 5
 OAG Contact Information 5
 County Contact Information 5
ATTACHMENTS
Incident Identification..... 6
Incident Survey 7
Incident Containment..... 8
Incident Eradication..... 9

SAMPLE

_____ County Incident Response Plan

Overview

Pursuant to the 2009 SCR/LCS Contract # _____, § _____, this Incident Response Plan is designed to provide a general guidance to county staff, both technical and managerial, to:

- enable quick and efficient recovery in the event of security incidents which may threaten the confidentiality of OAG Data;
- respond in a systematic manner to incidents and carry out all necessary steps to handle an incident;
- prevent or minimize disruption of mission-critical services; and,
- minimize loss or theft of confidential data.

The plan identifies and describes the roles and responsibilities of the Incident Response Team and outlines steps to take upon discovery of unauthorized access to confidential data. The Incident Response Team is responsible for putting the Plan into action.

Incident Response Team

The Incident Response Team is established to provide a quick, effective and orderly response to any threat to confidential data. The Team's mission is to prevent a serious loss of information assets or public confidence by providing an immediate, effective and skillful response to any unexpected event involving computer, information systems, networks or databases. The Team is responsible for investigating suspected security incidents in a timely manner and reporting findings to management and the appropriate authorities as appropriate.

Incident Response Team Roles and Responsibilities

Position	Roles and Responsibilities
Chief Information Security Officer (CISO)	<ul style="list-style-type: none"> • Immediately report incident directly to OAG CISO and OAG Contract Manager pursuant to § • Determine nature and scope of the incident • Contact members of the Incident Response Team • Determine which Team members play an active role in the investigation • Escalate to executive management as appropriate • Contact other departments as appropriate • Monitor and report progress of investigation to OAG CISO pursuant to § • Ensure evidence gathering and preservation is appropriate • Prepare and provide a written summary of the incident and corrective action taken to OAG CISO pursuant to §
Information Technology Operations Center	<ul style="list-style-type: none"> • Central point of contact for all computer incidents • Notify CISO to activate Incident Response Team • Complete Incident Identification form (Attachment One) and Incident Survey (Attachment Two) and forward to County CISO
Information Privacy Office	<ul style="list-style-type: none"> • Document the types of personal information that may have been breached • Provide guidance throughout the investigation on issues relating to privacy of customer and employee personal information • Assist in developing appropriate communication to impacted parties • Assess the need to change privacy policies, procedures and/or practices as a result of the breach
Network Architecture	<ul style="list-style-type: none"> • Analyze network traffic for signs of external attack • Run tracing tool and event loggers • Look for signs of firewall breach • Contact external internet service provider for assistance as appropriate • Take necessary action to block traffic from suspected intruder • Complete Incident Containment Forms (Attachment Three), as appropriate, and forward to County CISO
Operating Systems Architecture	<ul style="list-style-type: none"> • Ensure all service packs and patches are current on mission-critical computers • Ensure backups are in place for all critical systems • Examine system logs of critical systems for unusual activity • Complete Incident Containment Forms (Attachment Three), as appropriate, and forward to County CISO
Business Applications	<ul style="list-style-type: none"> • Monitor business applications and services for signs of attack • Review audit logs of mission-critical servers for signs of suspicious activity • Contact the Information Technology Operations Center with any information relating to a suspected breach • Collect pertinent information regarding the incident at the request of the CISO
Internal Auditing	<ul style="list-style-type: none"> • Review systems to ensure compliance with information security policy and controls • Perform appropriate audit test work to ensure mission-critical systems are current with service packs and patches • Report any system control gaps to management for corrective action • Complete Incident Eradication Form (Attachment Four) and forward to County CISO

Incident Contact List

OAG Contact Information

Position	Name	Phone Number	Email address
OAG Chief of Information Security Officer	Walt Fultz		
OAG SCR/LCS Contract Manager	Allen Broussard		

County Contact Information

Position	Name(s)	Phone Number	Email address
Chief of Information Security Offices			
County SCR/LCS Contract Manager			
Information Technology Operations Center			
Information Privacy Office			
Network Architecture			
Operating Systems Architecture			
Business Applications			
Internal Auditing			

SAMPLE

Incident Identification

Date Updated: _____

General Information

Incident Detector's Information:

Name: _____	Date and Time Detected: _____
Title: _____	_____
Phone: _____	Location Incident Detected From: _____
Email: _____	_____
Detector's Signature: _____	Date Signed: _____

Incident Summary

Type of Incident Detected:

- Denial of Service
- Malicious Code
- Unauthorized Use
- Unauthorized Access
- Espionage
- Other
- Probe
- Hoax

Incident Location: _____

Site: _____

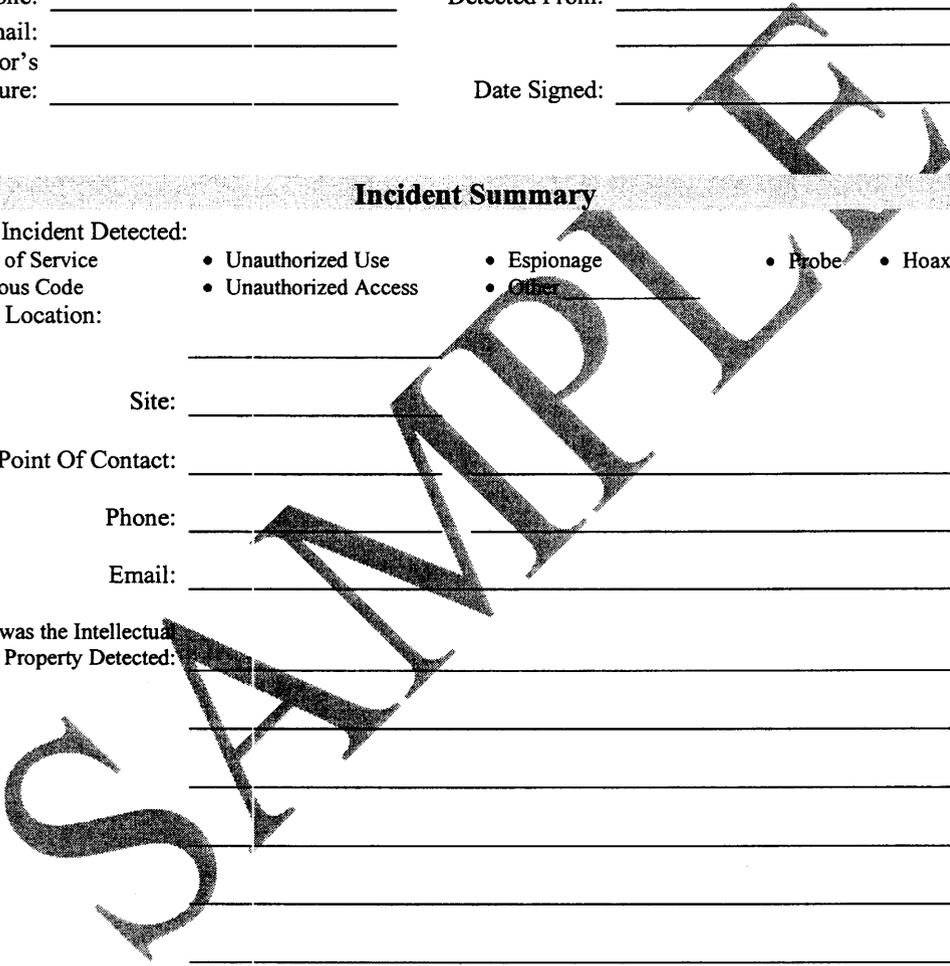
Site Point Of Contact: _____

Phone: _____

Email: _____

How was the Intellectual Property Detected: _____

Additional Information: _____



Incident Survey

Date Updated: _____

Location(s) of affected systems: _____

Date and time incident handlers arrived at site: _____

Describe affected information system(s): _____

Is the affected system connected to a network? YES NO

Is the affected system connected to a modem? YES NO

Describe the physical security of the location of affected information systems (locks, security alarms, building access, etc.):

Incident Containment

Date Updated: _____

Isolate Affected Systems:

CISO approved removal from network? **YES** **NO**

If YES, date and time systems were removed: _____

If NO, state reason: _____

Backup Affected Systems:

Successful backup for all systems? **YES** **NO**

Name of person(s) performing backup: _____

Date and time backups started: _____

Date and time backups complete: _____

SAMPLE

Incident Eradication

Date Updated: _____

Name of person(s) performing forensics on systems:

Was the vulnerability identified: YES NO

Describe: _____

SAMPLE