ATTACHMENT G

WILLIAMSON COUNTY

INCIDENT RESPONSE PLAN

Adopted _____, 2012

Williamson County
Incident Response Plan

Overview

Pursuant to Contract #13-C0099, § 6.4.1.1, 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)	• Immediately report incident directly to OAG CISO and OAG Contract Manager • 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 • Ensure evidence gathering and preservation is appropriate • Prepare and provide a written summary of the incident and corrective action taken to OAG CISO
Information Technology Operations Center	• 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	• 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	• 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	• 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	• 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	• 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	Willie Harvey	512-936-1320	willie.harvey@texasattorneygeneral.gov
OAG Contract Manager	Allen Broussard	512-460-6373	allen.broussard@texasattorneygeneral.gov

County Contact Information

Position	Name	Phone Number	Email address
Chief of Information Security Officer			
County Contract Manager			
Information Technology Operations Center			
Information Privacy Office			
Network Architecture			
Operating Systems Architecture			
Business Applications			
Internal Auditing			

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 Information

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: _____

[redacted]

CISO approved removal from network? YES NO

If YES, date and time systems were removed: _____

If NO, state reason: _____

_____

_____

[redacted]

Successful backup for all systems? YES NO

Name of person(s) performing backup: _____

_____

Date and time backups started: _____

Date and time backups complete: _____

Office of the Attorney General – Child Support Division

Certificate of Destruction for Contractors and Vendors

ATTACHMENT H

Hard copy and electronic media must be sanitized prior to disposal or release for reuse. The OAG tracks, documents, and verifies media sanitization and disposal actions. The media must be protected and controlled by authorized personnel during transport outside of controlled areas. Approved methods for media sanitization are listed in the NIST Special Publication 800-88, Guidelines for Media Sanitization. http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf

Contact Name	Title	Company Name and Address	Phone

You may attach an inventory of the media if needed for bulk media disposition or destruction.

Media Type				Media Title / Document Name			
	HARD COPY		ELECTRONIC				
Media Description (Paper, Microfilm, Computer Media, Tapes, etc.)							
Dates of Records							
Document / Record Tracking Number		OAG Item Number		Make / Model		Serial Number	

Item Sanitization		CLEAR	Who Completed?		Who Verified?	
		PURGE	Phone		Phone	
		DESTROY	DATE Completed			
Sanitization Method and/or Product Used →						
Final Disposition of Media		Reused Internally			Destruction / Disposal	
		Reused Externally			Returned to Manufacturer	
		Other:				

Comments:

If any OAG Data is **retained**, indicate the type of storage media, physical locations(s), and any planned destruction date.

Description of OAG Data Retained and Retention Requirements:

Proposed method of destruction for OAG approval:	Type of storage media?	
	Physical location?	
	Planned destruction date?	

Within five (5) days of destruction or purging, provide the OAG with a signed statement containing the date of clearing, purging or destruction, description of OAG data cleared, purged or destroyed and the method(s) used.

Authorized approval has been received for the destruction of media identified above and has met all OAG Records Retention Schedule requirements including state, federal and/or internal audit requirements and is not pending any open records requests.

Records Destroyed by:			Records Destruction Verified by:	
Signature	Date		Signature	Date

Be sure to enter name and contact info for who completed the data destruction and who verified data destruction in the fields above.

Send the signed Certificate of Destruction to:

OAG: Child Support Division, Information Security Office, PO Box 12017, Austin, TX 78711-2017

Office of the Attorney General – Child Support Division

Certificate of Destruction for Contractors and Vendors **ATTACHMENT H**

INSTRUCTIONS FOR CERTIFICATE OF DESTRUCTION

Hard copy and electronic media must be sanitized prior to disposal or release for reuse. The OAG tracks, documents, and verifies media sanitization and disposal actions. The media must be protected and controlled by authorized personnel during transport outside of controlled areas. Approved methods for media sanitization are listed in the NIST Special Publication 800-88, Guidelines for Media Sanitization. http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf

IRS Publication 1075 directs us to the FISMA requirements and NIST guidelines for sanitization and disposition of media used for federal tax information **(FTI)**. These guidelines are also required for sensitive or confidential information that may include personally identifiable information **(PII)** or protected health information **(PHI)**. NIST 800-88, Appendix A contains a matrix of media with minimum recommended sanitization techniques for clearing, purging, or destroying various media types. This appendix is to be used with the decision flow chart provided in NIST 800-88, Section 5.

There are two primary types of media in common use:

- **Hard Copy**. Hard copy media is physical representations of information. Paper printouts, printer and facsimile ribbons, drums, and platens are all examples of hard copy media.
- **Electronic (or soft copy).** Electronic media are the bits and bytes contained in hard drives, random access memory (RAM), read-only memory (ROM), disks, memory devices, phones, mobile computing devices, networking equipment, and many other types listed in NIST SP 800-88, Appendix A.

1. For media being reused within your organization, use the **CLEAR** procedure for the appropriate type of media. Then validate the media is cleared and document the media status and disposition.

2. For media to be reused outside your organization or if leaving your organization for any reason, use the PURGE procedure for the appropriate type of media. Then validate the media is purged and document the media status and disposition. Note that some **PURGE** techniques such as degaussing will typically render the media (such as a hard drive) permanently unusable.

3. For media that will not be reused, use the **DESTRUCTION** procedure for the appropriate type of media. Then validate the media is destroyed and document the media status and disposition.

4. For media that has been damaged (i.e. crashed drive) and can not be reused, use the **DESTRUCTION** procedure for the appropriate type of media. Then validate the media is destroyed and document the media status and disposition.

5. If immediate purging of all data storage components is not possible, data remaining in any storage component will be protected to prevent unauthorized disclosures. Within twenty (20) business days of contract expiration or termination, provide OAG with a signed statement detailing the nature of OAG data retained type of storage media, physical location, planned destruction date, and the proposed methods of destruction for OAG approval.

6. Send the signed Certificate of Destruction to:

OAG: Child Support Division
Information Security Office
PO Box 12017
Austin, TX 78711-2017

FAX to: 512-460-6070

or send as an email attachment to:

Willie.Harvey@cs.oag.state.tx.us

Final Distribution of Certificate	Original to:	Willie Harvey, Information Security Officer 512-460-6764
	Copy to:	1. Your Company Records Management Liaison - or - Information Security Officer 2. CSD Contract Manager