

Collin COUNTY

INCIDENT RESPONSE PLAN

Adopted _____, 2010

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

County Incident Response Plan

Overview

Pursuant to the 2009 SCR/LCS Contract # _____, § 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)	<ul style="list-style-type: none"> • 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	<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 Foulz	512-936-1320	walt.foulz@oag.state.tx.us
OAG SCR/LCS Contract Manager	Allen Broussard	512-460-6373	allen.broussard@cs.oag.state.tx.us

County Contact Information

Position	Name	Phone Number	Email address
Chief of Information Security Officer	Caren Skipworth	972-548-4501	cskipworth@co.collin.tx.us
County SCR/LCS Contract Manager	Hannah Kunkle	972-548-4320	hkunkle@co.collin.tx.us
Information Technology Operations Center	Caren Skipworth	972-548-4501	cskipworth@co.collin.tx.us
Information Privacy Office	Hannah Kunkle	972-548-4320	hkunkle@co.collin.tx.us
Network Architecture	Caren Skipworth	972-548-4501	cskipworth@co.collin.tx.us
Operating Systems Architecture	Caren Skipworth	972-548-4501	cskipworth@co.collin.tx.us
Business Applications	N/A	-	-
Internal Auditing	Jeff May	972-548-4644	jmay@co.collin.tx.us

Incident Identification

Date Updated: _____

General Information

Incident Detector's Information:

Name: _____	Date and Time Detected: _____
Title: _____	Location Incident Detected From: _____
Phone: _____	_____
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: _____

Incident Eradication

Date Updated: _____

Name of person(s) performing forensics on systems:

Was the vulnerability identified: YES NO

Describe: _____
