OKLAHOMA COUNTY

INCIDENT RESPONSE PLAN

Information Technology Operations

Aligned with CJIS Security Policy | NIST SP 800-53 | CIS Controls v8

Document ID:	IT-POL-IRP-001
Version:	1.0
Effective Date:	[Date of BOCC Resolution]
Last Reviewed:	[Date]
Classification:	Internal Use
Document Owner:	Director of MIS
Approved By:	Board of County Commissioners — Resolution No. [____]

CONFIDENTIAL — FOR OFFICIAL USE ONLY

Table of Contents

1. Purpose

This Incident Response Plan (IRP) establishes the procedures, roles, and communication protocols for detecting, reporting, containing, eradicating, recovering from, and documenting information security incidents affecting Oklahoma County IT systems and data.

This policy is adopted under the authority of the Oklahoma County Information Technology Governance Charter (IT-GOV-CHARTER-001), as approved by the Board of County Commissioners. It is binding on all County offices, departments, and agencies as defined in the Governance Charter.

This plan operationalizes the incident response framework defined in the Information Security Policy (IT-POL-ISP-001) and applies to all security events affecting County information assets.

> ***Framework Alignment:*** *NIST SP 800-53: IR-1 (Incident Response Policy and Procedures) | NIST SP 800-61 Rev. 2 (Computer Security Incident Handling Guide) | CIS Control 17 | CJIS Security Policy 5.3*

2. Scope

This plan applies to all information security incidents affecting Oklahoma County IT resources, including:

- Systems, networks, and data managed by MIS (shared infrastructure)
- Systems managed by departmental IT operations (County Clerk, Assessor, Sheriff, Treasurer, Court Clerk) when the incident affects shared infrastructure or other County Offices
- Cloud services, remote access systems, and mobile devices used to access County resources
- Third-party and vendor systems that connect to or process County data

Departmental IT Offices are responsible for incident response on their own isolated systems, but must notify MIS immediately when an incident could affect shared infrastructure, involves CJI, or impacts other County Offices.

> ***Framework Alignment:*** *NIST SP 800-61: Section 2 (Organizing a Computer Security Incident Response Capability)*

3. Definitions

Term	Definition
Security Event	Any observable occurrence in a system or network that may indicate a security issue. Not all events are incidents.
Security Incident	A security event that has been confirmed to violate County policy, compromise security controls, or pose a threat to the confidentiality, integrity, or availability of County data or systems.
Data Breach	A confirmed incident in which sensitive, protected, or confidential data has been accessed, disclosed, or exfiltrated by an unauthorized party.

Term	Definition
Incident Commander (IC)	The individual with overall authority and responsibility for managing an incident from detection through closure.
Incident Response Team (IRT)	The group of personnel activated to respond to, contain, and remediate a security incident.
Containment	Actions taken to limit the scope and impact of an incident and prevent further damage.
Eradication	Removal of the root cause of the incident from all affected systems.
Recovery	Restoring affected systems and data to normal operations with confidence that the threat has been eliminated.
Post-Incident Review (PIR)	A structured review conducted after incident closure to document lessons learned and improve future response.
Indicator of Compromise (IOC)	Technical evidence that a security breach has occurred (malicious IPs, file hashes, registry changes, etc.).

4. Incident Response Team

4.1 IRT Composition

Role	Assigned To	Responsibilities
Incident Commander	MIS Operations Manager	Overall incident authority; makes containment/escalation decisions; coordinates resources; authorizes communications
Lead Investigator	Senior Security Analyst	Leads technical analysis, forensics, and evidence preservation; determines root cause; recommends containment and eradication actions
Security Analyst	Junior Security Analyst	Supports investigation; monitors SIEM/EDR during incident; documents technical findings in real time
Infrastructure Lead	SE III (assigned by domain)	Executes containment and recovery actions on affected systems; implements firewall rules, isolates systems, restores from backup
Communications Lead	Director of MIS, MIS Operations Manager, and/or County Manager	Manages all internal and external communications; coordinates with County PIO if needed
CJIS Liaison	LASO (Sheriff's Office)	Activated for incidents involving CJI; coordinates CJIS incident reporting to the State CSA
Legal / Insurance Liaison	Director of MIS	Engages County legal counsel and cyber insurance carrier when warranted; authorizes law enforcement notification
Departmental IT Liaison	Affected Office's IT lead	Activated when incident affects departmental systems; provides department-specific context and coordinates departmental recovery

4.2 IRT Activation

The IRT is activated when a reported security event is confirmed or strongly suspected to be a security incident at severity P1, P2, or P3. Activation authority:

- **P1 (Critical) - MIS Operations Manager activates the full IRT immediately; Director of MIS is notified within 30 minutes** P1 (Critical):

- **P2 (High) - MIS Operations Manager activates core IRT (Investigator, Infrastructure Lead) within 1 hour** P2
- **P3 (Medium) - Senior Security Analyst leads response with support as needed; MIS Operations Manager notified**
- **P4 (Low) - Handled through normal security operations; no IRT activation required**

Framework Alignment: *NIST SP 800-61: Section 2.4 (Incident Response Team Structure) | CJIS Security Policy 5.3*

5. Incident Response Lifecycle

Oklahoma County follows the NIST SP 800-61 incident response lifecycle:

5.1 Phase 1: Preparation

Preparation activities are ongoing and ensure the County is ready to respond effectively:

- Maintain and test incident response tools, playbooks, and contact lists
- Ensure SIEM, EDR, and DLP platforms are operational and generating alerts
- Conduct incident response tabletop exercises at least annually
- Maintain current on-call rotation schedules and emergency contact information for all IRT members
- Maintain relationships with external resources: cyber insurance carrier, legal counsel, law enforcement (FBI, OSBI), and State CJIS Systems Agency
- Ensure forensic tools and evidence preservation procedures are documented and accessible

5.2 Phase 2: Detection and Analysis

Detection sources include but are not limited to:

- SIEM alerts and correlation rules
- EDR endpoint alerts and behavioral detections
- DLP policy violations
- Firewall and IDS/IPS alerts
- User reports of suspicious activity, phishing, or system anomalies
- Vulnerability scan findings indicating active exploitation
- External notifications (law enforcement, vendors, threat intelligence feeds)

Upon detecting a potential incident, the following analysis steps are performed:

1. Initial triage: Determine if the event is a confirmed incident or a false positive
2. Severity classification: Assign a severity level (P1–P4) using the matrix in the Information Security Policy
3. Scope assessment: Identify affected systems, users, data, and network segments
4. Evidence preservation: Begin logging all actions; capture system state, logs, memory dumps, and network captures as appropriate

5. Document the initial findings in the MIS' ITSM as an Incident ticket (linked to any related Change Requests)

Evidence preservation is critical. Do not reboot, reimage, or modify affected systems until the Senior Security Analyst has confirmed that volatile evidence has been captured or that evidence preservation is not required.

5.3 Phase 3: Containment

Containment actions are taken to limit the impact and prevent further spread. The strategy depends on the incident type:

Containment Strategy	When Used	Actions
Network Isolation	Active intrusion, lateral movement, malware propagation	Isolate affected VLANs/subnets; block malicious IPs at firewall; disable affected switch ports
Account Suspension	Compromised credentials, unauthorized access	Disable affected accounts in AD/Azure AD; force password reset; revoke active sessions and tokens
Endpoint Quarantine	Malware infection, compromised workstation	EDR quarantine; disconnect from network; preserve for forensic analysis
Service Isolation	Compromised application or cloud service	Disable service access; rotate API keys/credentials; block external connections
Full Network Disconnect	Ransomware or wiper malware actively spreading	Disconnect affected segments from County core network; MIS emergency disconnect authority per IT Governance Charter

All containment actions must be documented in the ITSM Incident ticket with timestamps, who performed the action, and the rationale.

5.4 Phase 4: Eradication

After containment, the root cause is identified and eliminated:

- Remove malware, backdoors, unauthorized accounts, and persistence mechanisms from all affected systems
- Patch the vulnerability that enabled the initial compromise
- Reset credentials for all accounts that may have been exposed, including service accounts
- Verify eradication through rescanning, log review, and EDR validation
- Confirm no additional IOCs are present on systems adjacent to affected hosts

5.5 Phase 5: Recovery

Recovery restores affected systems and services to normal operations:

6. Restore systems from verified clean backups if required
7. Rebuild compromised systems from known-good images if eradication cannot be fully confirmed
8. Gradually reconnect isolated systems to the network with enhanced monitoring

9. Validate system functionality and data integrity before returning to production
10. Monitor recovered systems for 30 days post-recovery for signs of re-compromise
11. Confirm with affected departments that their operations are restored

5.6 Phase 6: Post-Incident Activity

A Post-Incident Review is conducted for all P1, P2, and P3 incidents:

- The PIR meeting is convened within 5 business days of incident closure
- All IRT members and affected departmental representatives participate
- The PIR documents: timeline of events, root cause analysis, what worked well, what needs improvement, and specific action items with owners and deadlines
- PIR findings are reported to the IT Council at the next regular meeting
- Action items from PIRs are tracked in MIS' ITSM and reviewed monthly

Framework Alignment: *NIST SP 800-61: Sections 3.1–3.4 (Incident Handling) | CIS Controls 17.1–17.9*

6. Communication Procedures

6.1 Internal Communication

Audience	Trigger	Method	Timeline	Responsible
Director of MIS	All P1 and P2 incidents	Phone call + email	Within 30 minutes of IRT activation	Incident Commander
County Manager	P1 incidents; data breaches; incidents with legal/financial impact	Phone call from Director of MIS	Within 1 hour of P1 classification	Director of MIS
IT Council representatives	Incidents affecting their Office's systems	Phone + email	Within 2 hours for P1/P2; next business day for P3	Incident Commander
All County staff	Incidents requiring user action (password resets, phishing campaigns)	Email from MIS	As soon as practical	Communications Lead
Helpdesk / MIS team	All confirmed incidents	Internal briefing	Immediately upon confirmation	Incident Commander

6.2 External Communication

Audience	Trigger	Authorization Required	Method
Cyber insurance carrier	Any incident that may result in a claim; all P1 incidents	Director of MIS	Per policy terms — verify carrier hotline number
Law enforcement (FBI, OSBI, local)	Criminal activity suspected; ransomware; CJI breach	Director of MIS + County legal counsel	Direct contact

Audience	Trigger	Authorization Required	Method
State CJIS Systems Agency	Any incident involving CJI systems	LASO	Per CJIS reporting requirements
State Attorney General / Affected individuals	Confirmed data breach involving PII per Oklahoma Security Breach Notification Act	Director of MIS + County legal counsel	Written notification per statutory requirements
Media / Public	Incidents with public impact or media inquiries	County Manager + Director of MIS	Coordinated through County PIO if available; otherwise Director of MIS
Affected vendors / partners	Incident involving vendor systems or data	Incident Commander	Direct contact with vendor security team

No external communication about a security incident may be made without Director of MIS authorization. This includes conversations with media, social media posts, vendor notifications, and law enforcement contacts (except CJIS reporting by the LASO).

CJIS CJIS Security Policy 5.3: Security incidents involving CJI must be reported to the CJIS Systems Officer (CSO) through the LASO within the timeframe specified by the State CJIS Systems Agency. The LASO has independent authority to report CJI incidents without waiting for Director of IT authorization.

7. Incident Classification and Initial Response Playbooks

The following table provides initial response guidance by incident type. Detailed playbooks should be developed for each category as the program matures.

Incident Type	Initial Actions	Key Contacts
Ransomware	Isolate affected systems immediately; do NOT pay ransom without legal/insurance consultation; preserve encrypted files; activate full IRT; notify Director of MIS and insurance carrier	Incident Commander, Lead Investigator, Director of MIS, Insurance, Law Enforcement
Phishing Compromise	Disable compromised account; force password reset; check for mail forwarding rules; scan endpoint with EDR; search SIEM for lateral movement from compromised account	Senior Security Analyst, Systems Engineer III
Malware Infection	EDR quarantine endpoint; isolate from network; capture memory dump if possible; scan adjacent systems; check SIEM for C2 traffic	Senior Security Analyst, Systems Engineer III
Unauthorized Access	Disable compromised account(s); audit access logs; identify scope of access; check for data exfiltration; rotate affected credentials	Senior Security Analyst, Incident Commander
Data Breach / Exfiltration	Contain the exfiltration channel; identify what data was accessed; preserve evidence; engage legal counsel and insurance; prepare for notification obligations	Incident Commander, Director of MIS, Legal, Insurance, LASO (if CJI)
DDoS Attack	Engage ISP for upstream filtering; activate DDoS mitigation if available; identify attack vectors; document timeline	Systems Engineer III, Incident Commander

Incident Type	Initial Actions	Key Contacts
Insider Threat	Preserve evidence before alerting the individual; coordinate with HR and legal; restrict access discreetly; image workstation if warranted	Incident Commander, Director of MIS, HR, Legal
Physical Security Breach	Secure the area; assess what was accessed; check for device theft or tampering; review physical access logs; scan affected systems	Incident Commander, Systems Engineer III, Senior Security Analyst, Facilities

8. Evidence Handling and Preservation

8.1 Chain of Custody

- All digital evidence collected during an incident is documented with: what was collected, who collected it, when, where it was stored, and who has accessed it
- Evidence is stored in a secured, access-controlled location (physical or digital) separate from production systems
- Access to evidence is restricted to IRT members and authorized legal/law enforcement personnel
- Evidence logs are maintained in the MIS' ITSM tool and/or a dedicated evidence tracking document

8.2 Forensic Procedures

- Forensic imaging of affected systems follows industry-standard procedures (write-blockers for disk imaging, verified hash values)
- Volatile evidence (memory, network connections, running processes) is captured before any containment actions that would destroy it
- Forensic analysis is performed on copies, never on original evidence
- If the County does not have internal forensic capability for a specific incident, the Director of MIS authorizes engagement of external forensic resources (insurance carrier preferred vendor or contracted third party)

Framework Alignment: *NIST SP 800-86 (Guide to Integrating Forensic Techniques) | NIST SP 800-53: IR-4 (Incident Handling), AU-9*

9. Data Breach Notification

9.1 Determination

When an incident involves confirmed or suspected unauthorized access to personally identifiable information (PII), the following steps are taken:

12. The Senior Security Analyst assesses what data was accessed and the number of individuals affected
13. The Director of MIS engages County legal counsel to determine notification obligations under Oklahoma's Security Breach Notification Act and any other applicable laws

14. The cyber insurance carrier is notified to coordinate breach response services (forensics, notification, credit monitoring)

9.2 Notification Requirements

- Oklahoma law requires notification to affected individuals without unreasonable delay
- If more than a threshold number of individuals are affected, notification to the State Attorney General may be required
- CJI breaches require notification to the CJIS Systems Officer through the LASO
- Notification content and method are determined in coordination with legal counsel and the insurance carrier

Framework Alignment: *Oklahoma Security Breach Notification Act (24 O.S. § 163) | NIST SP 800-53: IR-6 (Incident Reporting)*

10. Incident Response Metrics

Metric	Definition	Target
Mean Time to Detect (MTTD)	Average time from incident occurrence to detection	Trending downward
Mean Time to Contain (MTTC)	Average time from detection to containment	P1: < 4 hours; P2: < 8 hours
Mean Time to Resolve (MTTR)	Average time from detection to full recovery	Tracked; trending downward
Incident Volume by Severity	Number of incidents per severity level per period	Tracked
PIR Completion Rate	Percentage of required PIRs completed within 5 business days	100%
Repeat Incident Rate	Percentage of incidents with same root cause recurring	< 5%
User Reporting Rate	Percentage of incidents initially reported by users vs. automated detection	Tracked

Framework Alignment: *NIST SP 800-61: Section 3.4 (Incident Handling Checklist and Metrics)*

11. Plan Testing and Maintenance

- **Tabletop Exercises - Conducted at least annually, simulating P1 and P2 scenarios with full IRT participation**
- **Functional Exercises - Conducted at least every two years, involving actual technical response actions in a test environment**
- **Contact List Validation - IRT contact information and escalation paths verified quarterly**
- **Plan Review - This IRP is reviewed at least annually and updated after every P1/P2 incident, organizational change, or significant infrastructure change**

- **External Coordination - Cyber insurance carrier contact information and claims procedures verified annually**

Framework Alignment: *NIST SP 800-53: IR-3 (Incident Response Testing), CP-4 (Contingency Plan Testing)*

12. Policy Administration

This plan is reviewed annually by MIS and the IT Council. Amendments follow the IT Governance Charter (Section 8) and require BOCC approval. Emergency updates to playbooks and contact lists may be made by the IT Operations Manager without BCC action, provided no substantive policy changes are involved.

13. Related Policies and Documents

Document	ID	Status
IT Governance Charter	IT-GOV-CHARTER-001	Pending
Information Security Policy	IT-POL-ISP-001	Pending
Acceptable Use Policy	IT-POL-AUP-001	Pending
Change Management Policy	IT-POL-CHG-001	Pending
Password and Access Management Policy	IT-POL-PAM-001	Pending
Business Continuity / Disaster Recovery Plan	IT-POL-BCDR-001	Planned
FBI CJIS Security Policy	External	Current Version
NIST SP 800-61 Rev. 2	External	Current Version
NIST SP 800-53 Rev. 5	External	Current Version
Oklahoma Breach Notification Act (24 O.S. § 163)	External	Current Version

Appendix A: Incident Response Contact List

This contact list must be verified quarterly and updated immediately when personnel changes occur.

Role	Name	Phone	Email	After-Hours
Incident Commander (IT Operations Manager)	[Name]	[Phone]	[Email]	[Cell]
Director of MIS	[Name]	[Phone]	[Email]	[Cell]
Senior Security Analyst	[Name]	[Phone]	[Email]	[Cell]
Junior Security Analyst	[Name]	[Phone]	[Email]	[Cell]
SE III	[Name]	[Phone]	[Email]	[Cell]
SE III	[Name]	[Phone]	[Email]	[Cell]

Role	Name	Phone	Email	After-Hours
SE III	[Name]	[Phone]	[Email]	[Cell]
LASO (Sheriff's Office)	[Name]	[Phone]	[Email]	[Cell]
County Manager	[Name]	[Phone]	[Email]	[Cell]
County Legal Counsel	[Name/Firm]	[Phone]	[Email]	[Cell]
Cyber Insurance Carrier	[Carrier Name]	[Claims Hotline]	[Email]	[24/7 Line]
FBI Cyber (OKC Field Office)		[Phone]		
OSBI Cyber		[Phone]		
State CJIS Systems Agency		[Phone]	[Email]	