Title	Computer Security incident response
Type	Standard
Related Policy	Information Technology Protection
Category	Security
Status	
Approved	
To Be Reviewed	
Scope	This standard is designed to improve the response time to data security incidents, to improve incident reporting and related communications, to mitigate any damages caused by incidents, and to improve overall data security systems.
Standard	Applies to the City of Albuquerque (CABQ) Information Technology Services (ITSD) and all systems and services for which it is responsible.
Definitions	**Information technology asset** -- a system or systems comprised of computer hardware, software, networking equipment, as well as any data on those systems. Such assets include but are not necessarily limited to desktop or laptop computers, servers, printers, telephones, pagers, radios, network lines, personal digital assistants, E-mail and Web-based services. **Abuse incident** -- an incident meeting one or more of the following conditions: • Any potential violation of Federal law, New Mexico law, City ordinance or City rule, regulation, Administrative Instruction or policy involving a City information technology asset. • A breach, attempted breach or other unauthorized access of a City information technology asset. This policy is intended to address incidents originating from or transiting the City's networks or by City employees or contractors. • Any conduct using in whole or in part a City information technology asset which could be construed as harassing, or in violation of City policies. • Evidence of tampering with City data or computer hardware. • Other incidents that could undermine or raise concern about the availability, stability, reliability or integrity of the City's information technology infrastructure. **Critical Incident Response Team** **Incident Manager** -- a City management-level Department staff member assigned by the Department Director/CIO or designee. Assumes

responsibility for and coordinates the investigation and resolution of an abuse incident. Responsible for maintaining custody of affected departmental information technology assets. Coordinates, as required, with Employee Relations, EAP, Legal, law enforcement or other agencies. Reports actions and findings to the Department Director.

Information Security Manager -- a management-level professional or technical staff member assigned by the Chief Information Officer. Performs initial assessment of an abuse incident and determines whether the incident warrants a formal response. Responsible for maintaining custody of affected centrally-managed information technology assets. Coordinates the provision of technical assistance to the Incident Manager. Coordinates the work of assigned Specialists. Reports actions and findings to the Chief Information Officer or designee.

Specialist -- A technical staff member (e.g., systems administrator, network engineer, or personal computer support technician) assigned by the Chief Information Officer to assist in the investigation and resolution of an abuse incident. Provides technical assistance to the Incident Manager as coordinated by the Information Security Manager. Reports actions and findings to the Information Security Manager.

An *incident* is any event that threatens the security, confidentiality, integrity, or availability of CABQ information assets (electronic or paper), information systems, and/or the networks that deliver the information. Any violation of computer security policies, acceptable use policies, or standard computer security practices is an incident. Incidents may include but are not limited to:

- Unauthorized entry
- Security breach or potential security breach
- Unauthorized scan or probe
- Denial of service
- Malicious code or virus
- Other violations of the CABQ IT Policies and Standards
- Networking system failure (widespread)
- Application or database failure (widespread)
- Others as defined by critical incident response team

Incidents such as those listed above vary in their impact on CABQ and in the degree of risk and vulnerability they pose.

Incidents may be identified through a variety of means, such as reports from staff, alerts from intrusion-detection, intrusion-prevention, and file-integrity monitoring systems.

A *security breach* is the unauthorized acquisition or access of computerized data that compromises the security, confidentiality or integrity of personal information. Security breach does not include good faith but unauthorized

acquisition or access of personal information by an employee for a legitimate business purpose.

For the purpose of this policy, *personal information* means an individual's first name or first initial and last name in combination with any one or more of the following data elements when either the name or the data elements are not encrypted or redacted or protected by another method that renders them unreadable or unusable by unauthorized persons:

- social security number;
- motor vehicle operator's license number or non-driver identification card;
- financial account number or credit or debit card number, if circumstances exist in which the number could be used without additional identifying information, access codes or passwords;
- account passwords or personal identification numbers or other access codes for a financial account.

Personal identifiable information does not include information that is made available to the general public.

Critical Incidents are defined as high impact and high risk; these include known or suspected security breaches, and the known or suspected compromise of protected information to individuals or entities outside the CABQ or to individuals or entities inside the CABQ without authorization. Critical incidents require the development and implementation of a formal incident response action plan by the critical incident response team.

Non-Critical Incidents are defined as medium, low or no risk; these may include good faith but unauthorized acquisition or access of personal information by an employee for a legitimate business purpose, breaches involving encrypted data, unauthorized scans or probes, or other non-critical or minor issues. Non-critical incidents do not require a formal incident response action plan but must have an appropriate response, as determined by the Security Administrator and Chief Information Officer (CIO) or designee for system incidents. Non-critical incidents involving security breaches require notification to the CABQ ITSD Security Administrator even though the misuse of personal information is determined to be not reasonably possible.

An incident is declared to be critical in one of the following ways:

- The ITSD Security Manager or designee, or CIO or designee, declares an incident to be critical.

ROLES AND RESPONSIBILITIES

A Critical Incident Response Team shall be established at the central facility; the membership of this team is documented in the Information Technology, Incident Management Standard. Overall membership should include:

- executive leadership

- ITSD Network Senior staff
- systems personnel
- facilities personnel
- security personnel

Participation by individual members may vary by incident as appropriate. Members of critical incident response teams are expected to respond immediately and fully when called upon. Responding to a critical incident, in general, takes precedence over all other work. If a member is unavailable at the time the team is assembled, a substitute member may be named by the executive leadership. Critical Incident Response Team members will receive periodic training to ensure all members are prepared to identify and efficiently respond to a potential incident.

Rationale

The City of Albuquerque relies extensively on its computing systems to meet its operational, financial, and informational requirements. It is essential that these systems and the data they process be operated and maintained in a secure environment.

The intent of this policy is to maintain accountability. Protection of City assets and accountability for their use shall override convenience in all circumstances.