Title	**Computer Abuse Incident Reporting and Response - Definitions**
Type	Standard
Related Policy	Computer Abuse Incident Reporting and Response
Category	Security
Status	Approved
Approved	01/09/2013
Revised	12/25/2012
To Be Reviewed	06/18/2017
Scope	Applies to all City information technology assets.
Standard	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. **Incident Manager** -- a City management-level Department staff member assigned by the Department Director. 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.

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.

Rationale

Due to a variety of issues, including the safety and privacy of City employees, it is imperative that a formal reporting and response policy be followed when responding to incidents of City computer abuse.

City computer abuse may constitute violations of: the City Employee Code of Conduct, City Personnel Rules and Regulations Section 301.15; the City Internet Usage Policy, Administrative Instruction 8-12; Guidelines for City E-Mail Services, Administrative Instruction 8-13; other City computing policies as approved by the Information Services Committee or issued by the Chief Information Officer; or other City ordinances or New Mexico or Federal law, including but not limited to the Federal Computer Fraud and Abuse Act (18 USC §1030 et seq), Electronic Communications Privacy Act (18 USC §2501 et seq), and Digital Millennium Copyright Act (17USC §512 et seq).