

CLARK COUNTY SCHOOL DISTRICT

CLASSIFICATION TITLE: Computer Forensic Investigator

CLASS CODE: 1650

PAY GRADE: 62

GENERAL DESCRIPTION OF DUTIES

Under direction and guidance, using advanced knowledge of computing hardware and software, information security, networking technologies and protocols, provides computer forensic services, including digital evidence preservation and analysis. Provides forensic case support, analysis and assistance with other investigative goals. Makes recommendations to implement internal controls and procedures in order to safeguard the Clark County School District. Routinely performs computer and network forensic investigations in support of both internal and criminal investigations and intrusion incidents.

SPECIFIC DUTIES AND RESPONSIBILITIES

ESSENTIAL JOB FUNCTIONS:

The list of essential functions, as outlined herein, is intended to be representative of the tasks performed within this classification. It is not necessarily descriptive of any one position in the class.

Performs computer and network forensic examinations and investigations in support of internal investigations and intrusion incidents, with responsibilities including, but not limited to digital evidence preservation, analysis, data and tape recovery, electronic mail extraction and database examination.

Creates and maintains forensic processes and procedures based on industry best practices.

Develops and maintains the necessary documentation to support the forensic and investigative processes and procedures.

Participates in the design, build-out and maintenance of a forensics lab; assesses and troubleshoots a variety of technical issues and supports a computer forensic lab in a technically secure environment.

Performs network intrusion examinations and investigations.

Installs and maintains forensic hardware and software.

Researches and develops evidence collection, protection, and analysis techniques for company-owned and maintained hardware and software.

Coordinates with internal support organizations in the development of additional evidence collection methods, technologies, and processes that support the need to detect and respond to unauthorized or unintentional activities.

Provides technology advisory services in an effort to help enhance forensic engagements.

Exercises a solid knowledge of computing hardware and software, and a good understanding of information security, networking technologies and protocols.

Communicates in both verbal and written forms, and provides thorough case documentation.

Maintains advanced computer forensic certifications and keeps current with related technologies; researches and develops new computer forensic tools and methodologies.

ESSENTIAL JOB FUNCTIONS: (continued)

Processes and interprets a wide variety of computer querying languages.

Conforms to safety standards as prescribed.

Performs related duties as assigned.

KNOWLEDGE, SKILLS AND ABILITIES:

Knowledge of forensic programming languages.

Knowledge of Microsoft, Macintosh, Linux and Solaris computer operating systems and software.

Knowledge of current forensic software and methodology.

Knowledge of applicable laws and codes.

Knowledge of current case law and trends that could effect the outcome of an investigation.

Ability to administer complex investigations that synthesize criminal/penal codes, NRS, school district policies and administrative due-process procedures.

Ability to obtain and maintain advanced forensic training certifications.

Ability to evaluate and test new techniques and technologies pertaining to forensic investigations and incident responses.

Ability to process and interpret computer query languages.

Ability to maintain complex data and prepare complex reports.

Ability to read and interpret complex materials.

Ability to analyze and interpret forensic metadata.

Ability to debug computer hardware and software.

Ability to work flexible hours or shifts and be on 24-hour call, if needed.

Ability to work cooperatively with employees, vendors and the public.

Ability to recognize and report hazards and apply safe work methods.

Ability to maintain confidentiality of information.

Ability to learn and apply school rules, regulations and procedures.

Ability to exercise judgment as to when to act independently and when to refer situations to an administrator.

Ability to demonstrate well developed organization skills.

Ability to work well either alone or in a team environment.

Ability to maintain a positive attitude with good interpersonal skills.

Ability to demonstrate initiative.

EXAMPLES OF ASSIGNED WORK AREAS:

Clark County School District Police Department, as well as travel to schools and other district office settings, utilizing the following equipment (illustrative, not inclusive): Various computers, printers, modems, telephones, fax machines, punch-down tools, digital multi-meters, data system and communication test equipment, and hand and power tools used in taking apart and assembling computer equipment.

Strength: Sedentary to medium – exert force 20-50 lbs. occasionally, 10-25 lbs. frequently or up to 10 lbs. constantly.

Physical Demands: Frequent climbing, reaching, handling, fingering, talking and hearing. Mobility to work in a typical office setting and use standard office equipment, stamina to remain seated and maintain concentration for an extended period of time. Hearing and speech to communicate in person or over the telephone. Vision: Frequent near acuity and occasional far acuity. Vision to read printed materials and VDT screens and other monitoring devices.

Environmental Conditions: Climate-controlled office setting and exposure to moderate noise intensity levels.

MINIMUM TRAINING AND EXPERIENCE:

Proof of documentation for all minimum qualifications, as cited below, is required at time of application.

1. High school graduation or other equivalent (e.g., GED, college, technical, trade school transcript, foreign equivalency, etc.).
2. Four (4) years experience performing computer forensic examinations, which includes three (3) years experience performing intrusion investigations and incident responses.
3. Two hundred (200) hours of Forensic Analysis courses.
4. EnCase Analysis certificate must be in possession at time of application/Request for Placement in the Qualified Selection Pool (QSP) and must be maintained for the duration of the assignment.
5. AccessData certificate must be in possession at time of application/Request for Placement in the Qualified Selection Pool (QSP) and must be maintained for the duration of the assignment.
6. Valid Nevada Class C Driver License. Must be maintained for the duration of the assignment. Copy of driving history issued by the Department of Motor Vehicles is required at the time of application and/or QSP placement request **and** at the time of interview, prior to approval of final selection.
7. Law enforcement, information and network security, and forensic investigation knowledge and experience is preferred, but not required.
8. Qualified applicants must pass extensive background investigation by School Police.

Clark County School District is an Equal Opportunity Employer. In compliance with the American with Disabilities Act, Clark County School District will provide reasonable accommodations to qualified individuals with disabilities.

Individuals with a disability who require reasonable accommodation(s) during any step of the screening process or who have questions about qualifications should notify a representative in Support Staff Personnel. Notification may be made in person, in writing, or by calling: (702) 799-5334 (V) or (702) 799-0217 (TDD).

06/05/06