STATE OF NEVADA
Department of Administration
Division of Human Resource Management

CLASS SPECIFICATION

TITLE	GRADE	EEO-4	CODE
CHIEF IT MANAGER	**45***	**A**	**7.901**
IT MANAGER III	**44***	**A**	**7.902**
IT MANAGER II	**43***	**A**	**7.906**
IT MANAGER I	**42***	**A**	**7.904**

SERIES CONCEPT

Information Technology (IT) Managers are responsible for planning, organizing, directing, and controlling the IT activities, in one or more IT specialization areas, of the State, a department, or a division.

Develop, maintain, and enforce operational standards in accordance with departmental and State policies to ensure operating specifications are met.

Develop physical and logical safety and security procedures for operating conditions and disaster recovery by analyzing procedures utilized at other agencies and organizations, reviewing literature on safety and security procedures, following federal/State guidelines, and consulting with subject matter experts.

Assess the effectiveness of current information systems technology resources and capacity analysis and initiate actions to reduce utilization, increase capacity, or address system replacement needs, if necessary.

Recommend or select hardware by reviewing system-generated reports, system logs, utilization reports, vendor presentations, and technical hardware manuals.

Design physical layout and installation requirements in response to the purchase of new equipment; analyze hardware technical manuals, floor space layouts, environmental requirements, and electrical requirements.

Evaluate and maintain inventory control, e.g., computer supplies, tape library, departmental equipment, and other items.

Write requests for proposals which detail proposed systems and serve as a reference document for system development, personnel, and IT management by utilizing information gathered and subsequent analysis relating to hardware, software, and personnel requirements including systems objectives, data security provisions, primary outputs, implementation plans, comprehensive cost estimates, time schedules, migration plans, and integration of multiple technologies.

Develop, examine, and evaluate contracts for purchases of materials and services.

Develop and monitor IT budgets by reviewing past expenditure patterns, current funding levels, projected personnel and equipment needs, and demands for additional services by clients/users.

Present and justify agency or division-wide IT budgets for review and approval and testify before Executive and Legislative groups as required.

Provide project management to ensure that projects are completed by the scheduled due date in accordance with project specifications and requirements and within the project budget; analyze personnel, hardware and software requirements, and all costs associated with the project; establish delivery dates, conduct periodic project

* **Reflects a 1-grade, special salary adjustment granted by the 2017 Legislature to improve recruitment and retention.**

SERIES CONCEPT (cont'd)

reviews, provide training for project team members, supervise installation of the system, provide regular project status reports to senior management; and determine training required prior to installation.

Participate in State IT activities and policy-making activities and/or serve on various ad hoc committees and work groups as needed.

Maintain current knowledge of technological trends and advancements in the IT field and security management practices, laws, policies, and ethics.

Develop organizational structure, staffing patterns, and resource allocation to meet agency or division-wide goals and objectives.

Supervise subordinate managers, supervisors, and staff, including hiring, determining workload, delegating assignments, training, monitoring and evaluating performance, and taking disciplinary action.

Resolve problems presented by subordinate staff, users, and clients regarding work processes, policies, procedures, and methods.

Perform related duties as assigned.

Additional description for Information Security positions: administer security policies, security operations, and/or maintain oversight of information systems and data within the assigned area of information security responsibility. Incumbents work with management and technical staff to develop a comprehensive information security program for integrated IT systems within the State or agency and are responsible for seven or more of the following ten security domain areas:

- Access control – centralized / decentralized / remote / federated
- Application/system development security – validation / verification / guidelines
- Continuity of operations/disaster recovery planning – business recovery
- Cryptography – transport / storage / authentication / non-repudiation
- Information security management – awareness / policies / risk management / procedural standards
- Operational security (OPSEC) – threats / hostile code / techniques
- Physical technical security – access systems / structural / environmental controls
- Security architecture and models – methods / security operational standards
- Security law, investigation and ethics – cyber crime / incident response / security regulation
- Telecommunications/network security – enclave / monitoring / virtual private network / firewall / prevention

****

ALLOCATION OF POSITIONS

Positions are allocated to a level within this series by a review of the totality of the duties assigned. Duties are evaluated based on the following established classification factors:

- Nature and complexity of work performed
- Knowledge, skills and abilities required
- Supervisory/managerial responsibility
- Independence/supervision received
- Scope of responsibility/consequence of error
- Authority to take action/decision-making
- Personal contacts necessary to complete work.

ALLOCATION OF POSITIONS (cont'd)

In relation to these factors, classifiers will evaluate the scope and complexity of the IT functions for which the position has management responsibility; the breadth/diversity of IT services managed; responsibility for managing vendor contracts to include development of the project, scope of work, budget and schedule control, approval of changes, and evaluation of deliverables; complexity of the infrastructure to include multiple system and development platforms, databases, and operating systems, in-house vs. outside support, geographic dispersion vs. concentration, and interface with internal and external entities; the number and level of subordinate managers, supervisors, and professional staff and the development/implementation of policies and work plans; the latitude to exercise initiative and discretion in managing staff and activities; the criticality of systems operations/results of failure in relation to legal, fiscal, and physical consequences; the financial and organizational actions for which the position has final decision-making authority; and the personal contacts with management internally and with external organizations to negotiate solutions to complex problems, resolve disputes, and justify actions/requests.

With regards to the consequence of error factor, IT initiatives (projects or major work products) for each class are judged (either critical, high, significant, or moderate) on four factors and their effects on the State, department, or citizens: financial risk (monetary impact of mistakes); legal/physical risk (legal risk or physical harm impact of mistakes); positive/negative consequences; and the effect of a sharp reduction or elimination of funding.

Critical – federal and/or State financial or legal/physical (injury risk) costs and penalties; has an effect on citizens and State government; the effect of sharp or eliminated funding for an initiative is not mitigated by the ability to fall back on legacy systems (manual processing is always an option).

High – likely federal and/or State financial or legal/physical (injury risk) costs and penalties; has an effect on citizens and most of State government; the effect of sharp or eliminated funding for an initiative is mitigated by the ability to fall back on legacy systems judged to be inadequate for growth within a few years (manual processing is always an option).

Significant – limited federal and/or State financial or legal/physical (injury risk) costs and penalties; may have an effect on citizens and has an effect on several State departments; the effect of sharp or eliminated funding for an initiative is mitigated by the ability to fall back on legacy systems judged to be inadequate for long term growth (manual processing is always an option).

Moderate – limited State financial or legal/physical (injury risk) costs and penalties; may have an effect on citizens and has an effect on one or several State departments; the effect of sharp or eliminated funding for an initiative is mitigated by the ability to fall back on legacy systems (manual processing is always an option).

Benchmark descriptions have also been provided at each level for purposes of position comparison.

****

CLASS CONCEPTS

Chief IT Manager: Under general administrative direction, incumbents perform IT managerial duties and interact with internal and external management levels as well as executives and officials to negotiate solutions to major or controversial issues within policy guidelines. Incumbents supervise a staff of lower level IT Managers and IT professionals on a regular and recurring basis and IT Technicians and support staff as required. Incumbents perform one of the following roles:

1) Incumbents direct and manage IT functions for a department or division with direct responsibility for an annual IT operation and maintenance budget and development projects' funds. Incumbents plan and implement IT initiatives, where the responsibility for failure falls on the incumbent, with a critical level of financial risk, critical level of legal or physical risk, and at least high positive or negative consequences to State government and citizens. Sharply reducing or eliminating funding for these initiatives would have at least a high negative effect on the populace the initiative is intended to serve; or

CLASS CONCEPTS (cont'd)

Chief IT Manager (cont'd)

2) The incumbent works under the direction of the Nevada State Chief Information Officer (CIO) and manages the State's information security program. The incumbent provides co-leadership to the State Security Committee in planning, developing, and implementing information security initiatives at the statewide level; or

3) Incumbents work under the direction of the director or executive of an agency that is excluded from Department of Information Technology oversight as established in NRS 242.111 and manage the agency's information security program. Incumbents provide co-leadership to the State Security Committee in planning, developing, and implementing information security initiatives at the statewide/multi-agency/agency level.

Examples of Chief IT Manager positions include:

In the Welfare and Supportive Services Division of the Department of Health and Human Services, the incumbent reports to the division administrator and manages the Information Systems subdivision. The incumbent directly supervises an IT Manager III and two IT professionals (one of whom is a supervisor), and indirectly supervises 29 IT professionals, eight IT Technicians, 21 support staff positions, and 11 contractors. This position is responsible for IT initiatives that involve potential conflicts with federal financial regulations and penalties, potential conflicts with federal and State laws and risks to families, and eliminating funding would necessitate continued usage of a legacy system for public assistance processing and reporting. The incumbent has direct authority for budgets for operations and maintenance in excess of $14 million and developmental projects in excess of $7 million.

In the Department of Information Technology, the incumbent reports to the deputy director and manages the Communications Division. The incumbent directly supervises three IT Manager I's and one IT Technician and indirectly supervises 17 IT professionals, three IT Technicians, and 15 support staff positions. This position is responsible for IT initiatives that involve financial risk related to potential outage of the State's communication system, public safety and health risks involving legal and physical risks of potential communications outages, and eliminating funding would harm efforts to support growing law enforcement communications needs. The incumbent has direct authority for budgets for operations and maintenance in excess of $21 million and developmental projects.

IT Manager III: Under administrative direction, incumbents perform IT managerial duties and interact with internal and external management levels as well as executives and officials to solve problems involving conflict or controversy requiring interpretation/application of policy. Incumbents supervise a staff of IT professionals on a regular and recurring basis and lower level IT Managers, IT Technicians, and support staff as required. Subordinates may include Master IT Professional II's. Incumbents perform one of the following roles:

1) Incumbents direct and manage IT functions within or for a department or division with direct or indirect responsibility for an annual IT operation and maintenance budget or funds on a regular and recurring basis and development projects' funds as required. Incumbents plan and implement IT initiatives, where the responsibility for failure falls on the incumbent, with a critical level of financial risk, at least high level of legal or physical risk, and at least high positive or negative consequences to State government and citizens. Sharply reducing or eliminating funding for these initiatives would have at least a significant negative effect on the populace the initiative is intended to serve; or

2) Incumbents work under the direction of a Chief IT Manager, or director of a large department and manage the department's information security program. Positions at this level are wholly dedicated to information security. Incumbents maintain departmental adherence to security policies and must serve as the department's representative on the State Security Committee.

CLASS CONCEPTS (cont'd)

IT Manager III (cont'd)

Examples of IT Manager III positions include:

In the Health Division of the Department of Health and Human Services, the incumbent reports to the financial executive officer and manages the division's IT functions. The incumbent directly supervises five IT professionals (two of whom are supervisors), one IT Technician (who is a supervisor), and one support staff position and indirectly supervises four IT professionals and eight IT Technicians. This position is responsible for IT initiatives that involve federal and State financial regulations and penalties and potential lost revenues, potential conflicts with federal laws and the risk of exposure of citizens' health data, and elimination of funding would result in downgrades of planned initiatives. The incumbent has indirect responsibility for funds for operations and maintenance and developmental projects.

In the Motor Vehicle Information Technology Division of the Department of Motor Vehicles, the incumbent reports to the division administrator and manages the Network subdivision. The incumbent directly supervises three IT professionals (all of whom are supervisors) and indirectly supervises seven IT professionals. This position is responsible for IT initiatives that involve financial risk of potential delayed collection of revenues for the State, legal risk due to potential exposure of citizens' identities, and elimination of funding could cause loss of service and denied law enforcement access to driver and vehicle records. The incumbent has direct authority for budgets for operations and maintenance in excess of $8 million and developmental projects.

IT Manager II: Under general direction, incumbents perform IT managerial duties and interact with internal management levels or external peers and higher supervisory levels to solve problems involving conflict or controversy requiring interpretation/application of policy. Incumbents supervise a staff of IT professionals on a regular and recurring basis and lower level IT Managers, IT Technicians, and support staff as required. Subordinates may include Master IT Professional II's.

Incumbents direct and manage IT functions within or for a department or division with direct or indirect responsibility for an annual IT operation and maintenance budget or funds on a regular and recurring basis and developmental projects' funds as required. Incumbents plan and implement IT initiatives, where the responsibility for failure falls on the incumbent, with at least a high level of financial risk, at least a high level of legal or physical risk, and at least significant positive or negative consequences to State departments and citizens. Sharply reducing or eliminating funding for these initiatives would have at least a significant negative effect on the populace the initiative is intended to serve.

In the Office of the Controller, the incumbent reports to the Deputy Controller and manages IT functions for the agency. The incumbent directly supervises seven IT professionals (one of whom is a supervisor) and one IT Technician and indirectly supervises two IT Technicians. This position is responsible for IT initiatives that involve financial risk of potential failure of the department's financial and billing system, legal risk of potential improperly routed transactions and debt collections, and elimination of funding would result in a reduction in available historical data and require users to access microfiche. The incumbent has direct authority for budgets and operations and maintenance in excess of $300,000 and developmental projects in excess of $100,000.

In the Motor Vehicle Information Technology Division of the Department of Motor Vehicles, the incumbent reports to the division administrator and manages the Applications subdivision. The incumbent directly supervises six IT professionals (four of whom are supervisors) and indirectly supervises 21 IT professionals. This position is responsible for IT initiatives that involve financial risk of potential misinterpretation of user requirements for taxes and fees, legal risk due to potential misinterpretation of law, and elimination of funding would affect the ability to prevent voter fraud and register new voters. The incumbent has indirect responsibility for funds for operations and maintenance and developmental projects.

CLASS CONCEPTS (cont'd)

IT Manager I: Under limited supervision, incumbents perform IT managerial duties and interact with others at similar levels or external peers and higher supervisory levels for the purpose of answering questions requiring explanations or interpretations of standard procedures and solving problems involving some conflict and requiring interpretation/application of policy. Incumbents supervise a staff of IT professionals on a regular and recurring basis and IT Technicians and support staff as required. Subordinates may include IT Professional IV's or Master IT Professionals.

Incumbents direct and manage IT functions within or for a department or division with direct or indirect responsibility for an annual IT operation and maintenance budget or funds on a regular and recurring basis and developmental projects' funds as required. Incumbents plan and implement IT initiatives, where the responsibility for failure falls on the incumbent, with at least a significant level of financial risk, at least a significant level of legal or physical risk, and at least moderate positive or negative consequences to State departments and citizens. Sharply reducing or eliminating funding for these initiatives would have at least a significant negative effect on the populace the initiative is intended to serve.

Examples of IT Manager I positions include:

In the Communications Division of the Department of Information Technology, the incumbent reports to a Chief IT Manager and manages the Network Engineering subdivision. The incumbent directly supervises six IT professionals (four of whom are supervisors) and indirectly supervises six IT professionals, three IT Technicians, and one support staff position. This position is responsible for IT initiatives that involve financial risk due to potential problems with transactional systems used by State departments, legal risk due to a potential compromise of the SilverNet, and elimination of funding could harm communications on the SilverNet. The incumbent has direct authority for a budget for operations and maintenance in excess of $500,000.

In the Department of Taxation, the incumbent reports to the deputy director and manages IT functions for the department. The incumbent directly supervises two IT professionals (both of whom are supervisors), one IT Technician, and five support staff positions (one of whom is a supervisor) and indirectly supervises six IT professionals, one IT Technician, eight support staff positions, and one contractor. This position is responsible for IT initiatives that involve financial risk due to potential delayed collection of taxes, legal risk due to potential insufficient notification and collection of interest and penalties, and elimination of funding would harm the department's ability to collect taxes. The incumbent has direct authority for a budget for operations and maintenance in excess of $3 million.

****

MINIMUM QUALIFICATIONS

SPECIAL REQUIREMENTS:

- Pursuant to NRS 284.4066, some positions in this series have been identified as affecting public safety. Persons offered employment in these positions must submit to a pre-employment screening for controlled substances.
- Some positions are subject to call-out or call-back.
- Some positions require specialized certification that will be identified at the time of recruitment.
- Some positions require statewide travel.

INFORMATIONAL NOTES:

- Some positions require an applicant to undergo a background investigation prior to appointment. These positions will be identified at the time of recruitment.

MINIMUM QUALIFICATIONS (cont'd)

<u>INFORMATIONAL NOTES</u>: (cont'd)

For Information Security Positions Only:

* International Information Systems Security Certification Consortium, Inc (ISC^2) – Certified Information System Security Professional (CISSP) is equivalent to three years of experience.
* Information Systems Audit and Control Association (ISACA) – Certified Information Security Manager (CISM) is equivalent to two years of experience.
* Global Information Assurance Certification (GIAC) – GIAC Security Expert (GSE) is equivalent to two years of experience.
* Other nationally recognized information security certifications may be substituted for up to one year of experience.
* Chief IT Manager – CISSP and CISM certification must be obtained within 12 months of appointment and maintained as a condition of continued employment.
* IT Manager III – Nevada Information Security Professional (NISP) or CISSP certification must be obtained within 12 months of appointment and maintained as a condition of continued employment.

CHIEF IT MANAGER

EDUCATION AND EXPERIENCE: Bachelor's degree from an accredited college or university with major course work in computer science, management information systems, or closely related field and eight years of progressively responsible professional IT experience which involved strategic planning, project management, quality assurance, and computer operations, systems administration, network administration, database administration, applications analysis and development, or information security. Five years of this experience must have been in a supervisory or project manager capacity; **OR** one year of experience as an IT Manager III in Nevada State service; **OR** an equivalent combination of education and experience as described above. *(See Special Requirements and Informational Notes)*

ENTRY LEVEL KNOWLEDGE, SKILLS, AND ABILITIES (required at time of application):
Detailed knowledge of: strategic planning. **Ability to:** define complex problems, select the best course of action, assess costs, and present alternatives to high levels of government; *and all knowledge, skills and abilities required at the lower levels*.

Additional Entry Level Knowledge, Skills, and Abilities Required for Information Security Positions:
Detailed knowledge of: eight of the ten information security domains. **Ability to:** analyze data, solve problems and make appropriate decisions within eight of the ten domains; plan, organize, and manage the functional core components for information security including disaster prevention/recovery, assessment and awareness, and technical security administration and accreditation; *and all knowledge, skills and abilities required at the lower levels*.

FULL PERFORMANCE KNOWLEDGE, SKILLS, AND ABILITIES (typically acquired on the job):
Detailed knowledge of: Nevada Revised Statutes pertaining to information systems, services and security; organizational regulations, policies and procedures and State administrative processes.

IT MANAGER III

EDUCATION AND EXPERIENCE: Bachelor's degree from an accredited college or university with major course work in computer science, management information systems, or closely related field and seven years of progressively responsible professional IT experience which involved strategic planning, project management, quality assurance, and computer operations, systems administration, network administration, database administration, applications analysis and development, or information security. Four years of this experience must have been in a supervisory or project manager capacity; **OR** one year of experience as an IT Manager II in Nevada State service; **OR** two years of experience as an IT Professional IV in Information

MINIMUM QUALIFICATIONS (cont'd)

IT MANAGER III (cont'd)

EDUCATION AND EXPERIENCE: (cont'd)
Security in Nevada State service for Information Security positions; **OR** an equivalent combination of education and experience as described above. *(See Special Requirements and Informational Notes)*

ENTRY LEVEL KNOWLEDGE, SKILLS, AND ABILITIES (required at time of application):
Detailed knowledge of: budget preparation and control; project management; quality control. **Working knowledge of:** strategic planning; *and all knowledge, skills and abilities required at the lower levels.*

Additional Entry Level Knowledge, Skills, and Abilities Required for Information Security Positions:
Detailed knowledge of: current information security trends and technology; current principles, theories, practices and procedures of information security management; methods and techniques used to safeguard against accidental or unauthorized modification, destruction or disclosure of data to meet security needs. **Working knowledge of:** seven of the ten security domains; business practices and principles common to a large, complex organization. **Ability to:** select the best course of mitigation actions for security issues with respect to public and private sector information.

FULL PERFORMANCE KNOWLEDGE, SKILLS, AND ABILITIES (typically acquired on the job):
Working knowledge of: Nevada Revised Statutes pertaining to information systems, services, and security; organizational regulations, policies, and procedures and Nevada State administrative processes.

IT MANAGER II

EDUCATION AND EXPERIENCE: Bachelor's degree from an accredited college or university with major course work in computer science, management information systems, or closely related field and six years of progressively responsible professional IT experience which involved strategic planning, project management, quality assurance, and computer operations, systems administration, network administration, database administration, or applications analysis and development. Three years of this experience must have been in a supervisory or project manager capacity; **OR** one year of experience as an IT Manager I in Nevada State service; **OR** an equivalent combination of education and experience as described above. *(See Special Requirements and Informational Notes)*

ENTRY LEVEL KNOWLEDGE, SKILLS, AND ABILITIES (required at time of application):
Detailed knowledge of: current computer technology and trends, including information management, communications, networking data administration, data processing, systems design, programming, operations, and controls; supervisory practices. **Working knowledge of:** budget preparation and control; project management; quality control. **General knowledge of:** strategic planning. **Ability to:** interpret current and/or proposed legislation to determine its intent and impact; plan, organize, coordinate and direct IT projects, initiatives, and strategies; *and all knowledge, skills and abilities required at the lower level.*

FULL PERFORMANCE KNOWLEDGE, SKILLS, AND ABILITIES (typically acquired on the job):
Working knowledge of: Nevada Revised Statutes pertaining to information systems, services, and security; organizational regulations, policies, and procedures and Nevada State administrative processes.

IT MANAGER I

EDUCATION AND EXPERIENCE: Bachelor's degree from an accredited college or university with major course work in computer science, management information systems, or closely related field and five years of progressively responsible professional IT experience which involved project management, quality assurance, and computer operations, systems administration, network administration, database administration, or applications analysis and development. Two years of this experience must have been in a supervisory or

MINIMUM QUALIFICATIONS (cont'd)

IT MANAGER I (cont'd)

EDUCATION AND EXPERIENCE: (cont'd)
project manager capacity; **OR** an equivalent combination of education and experience as described above. *(See Special Requirements and Informational Notes)*

ENTRY LEVEL KNOWLEDGE, SKILLS, AND ABILITIES (required at time of application):
Detailed knowledge of: the capabilities of various computer hardware and software products. **Working knowledge of:** current computer technology and trends, including information management, communications, networking data administration, data processing, systems design, programming, operations, and controls; supervisory practices. **General knowledge of:** budget preparation and control; project management; quality control. **Ability to:** administer multiple projects and allocate resources to each project; communicate effectively both orally and in writing; define complex problems, select the best course of action, assess costs and present alternatives; develop and implement procedures, formulate policies, and evaluate programs; establish work performance standards, review employee performance, and take appropriate action in order to optimize productivity; manage and administer change; train, supervise, and evaluate the performance of assigned personnel.

FULL PERFORMANCE KNOWLEDGE, SKILLS, AND ABILITIES (typically acquired on the job):
Detailed knowledge of: State regulations related to IT, purchasing, and personnel administration.

This class specification is used for classification, recruitment, and examination purposes. It is not to be considered a substitute for work performance standards for positions assigned to this series.

	7.901	7.902	7.906	7.904
ESTABLISHED:	12/17/03R	7/1/95P	11/1/66	7/1/87
	12/19/03PC	9/16/94PC		7/18/86PC
REVISED:			5/1/68	
REVISED:			7/1/87-12P	
			7/18/86PC	
REVISED:			7/1/95P	7/1/95P
			9/16/94PC	9/16/94PC
REVISED:		7/1/97LG	7/1/97LG	7/1/97LG
REVISED:		10/1/97UC		
REVISED:		7/17/00R		
		12/18/00UC		
REVISED:		12/19/03PC		
REVISED:	7/1/05LG	7/1/05LG		
REVISED:	8/11/06PC	8/11/06PC	8/11/06PC	8/11/06PC
REVISED:	7/1/17LG	7/1/17LG	7/1/17LG	7/1/17LG
REVISED:	8/28/17UC	8/28/17UC	8/28/17UC	8/28/17UC