MARION COUNTY BOARD OF COMMISSIONERS

Board Session Agenda Review Form

Meeting date: Jul 18, 2018

Department: Business Services

Agenda Planning Date: Jul 12, 2018

Time required: 5 Min.

□ Audio/Visual aids

Contact: Colleen Coons-Chaffins, Business Services Director

Phone: 503-373-4426

Department Head Signature:

TITLE

Recommendation to adopt and establish two classifications; Information Technology Security Analyst, and Information Technology System Architect.

Issue, Description & Background

At the request of the Information Technology Department, human resources (HR) has completed two job assessments based upon the business needs of the department. As the county does not currently have existing job classifications that met the business needs of the department, two new classifications have been developed: Information Technology Security Analyst and Information Technology System Architect. These classifications have specialized functions that are not well defined in any other classification. From a recruitment standpoint, these new classifications are a more accurate reflection of the scope of duties.

Financial Impacts:

Impacts to Department & External Agencies

Options for Consideration:

1. Approve recommendation; 2. Do not approve recommendation

Recommendation:

1. In Unit 13, Non-Represented, Non-Supervisory, adopt and establish the classification Information Technology Security Analyst, pay grade 13.G33 AK ($40.95 / $7,098.00 - $54.85 / $9,507.33) based on internal equity. Under FLSA positions in this classification are exempt from overtime.

2. In Unit 13, Non-Represented, Non-Supervisory, adopt and establish the classification Information Technology System Architect, pay grade 13.G32 AK ($38.90 / $6,742.67 - $52.16 / $9,041.06) based on internal equity. Under FLSA positions in this classification are exempt from overtime.

3. Approve recommendation beginning of first pay period following approval by the Board.

List of attachments:

Personnel Findings and Recommendation Report

Presenter:

Scott Emry, Information Technology Director

Copies of completed paperwork sent to the following: (Include names and e-mail addresses.)

MARION COUNTY BOARD OF COMMISSIONERS

Board Session Agenda Review Form

Copies to:	Jan Fritz, Deputy County Administrative Officer; jfritz@co.marion.or.us Colleen Coons-Chaffins; Business Services Director; ccoonschaffins@co.marion.or.us Jane Vetto, County Counsel; JVetto@co.marion.or.us HR Processing; HRProcessing@co.marion.or.us; HR Comp & Class; HRCompClass@co.marion.or.us INFORMATION TECHNOLOGY Scott Emry, IT Director; SEmry@co.marion.or.us Cynthia Klein, Administrative Assistant; cklein@co.marion.or.us

MARION COUNTY HUMAN RESOURCES

Personnel Findings and Recommendation Report

Date: Jul 11, 2018

To: Jan Fritz, Personnel Officer

From: Colleen Coons-Chaffins, Business Services Director

Re: Recommendation to adopt and establish two classifications; Information Technology Security Analyst, and Information Technology System Architect.

Background Information: At the request of the Information Technology Department, human resources (HR) has completed (2) job assessments based upon the business needs of the department. As the county does not currently have existing job classifications that met the business needs of the departments (2) new classifications have been developed: Information Technology Security Analyst and Information Technology System Architect. These classifications have specialized functions that are not well defined in any other classification. From a recruitment standpoint, these new classifications are a more accurate reflection of the scope of duties.

Discussion: Functions performed by classification:

Information Technology Security Analyst

GENERAL STATEMENT OF DUTIES Plan, organize, manage, and administer information security programs, operations, and functions; develop and implement program and strategic planning; implement and assist in the development of information security program policies, procedures, and business practices; evaluate goals, objectives, priorities, and activities to improve performance and outcomes; recommend and establish administrative controls and improvements; develop procedures to implement new and/or changing regulatory requirements; serve as an advisor to the management team.

SUPERVISION RECEIVED Works under general supervision of the IT Director who assigns work, establishes goals, and reviews the results obtained for overall effectiveness through the analysis of work products, observations, and meetings.

SUPERVISION EXERCISED The employee does not typically supervise, but facilitates and leads representatives from county departments and coordinates with IT Department personnel to achieve the objectives of the Information Security Program plan.

Information Technology System Architect

GENERAL STATEMENT OF DUTIES Uses business strategy to lead, define, and coordinate technical solutions architecture that meets operational objectives. The position serves as the senior most technical expert for creating an integrated user experience across a broad set of technologies. Strategically design and implement information systems that support core organizational functions, and assure their effective and efficient operational availability. Gains organizational commitment for all systems and software plans, as well as evaluating and selecting all technologies required in delivering on those plans. In addition, provides technical leadership across the organization, from strategic decision making down to the project planning level. Responsible for defining the system architecture processes, standards and governance, as well as leading the integration of those processes with related business, IT processes and standards.

SUPERVISION RECEIVED Works under general supervision of the IT Director who assigns work, establishes goals, and reviews the results obtained for overall effectiveness through the analysis of work products, observations, and meetings.

SUPERVISION EXERCISED Works independently under broad direction and occasional supervision, and may act as technical lead in providing work direction on large-scale, complex projects.

In determining if these classifications are appropriately compensated HR conducted a market review in accordance with county personnel rules and HR practices. This review identifies which pay grade will bring each classification closest to the mean (0%) of market comparables within the county's current pay structure; in addition to these market findings, funding and internal equity are also considered when establishing pay grades.

Recommendation: 1. In Unit 13, Non-Represented, Non-Supervisory, adopt and establish the classification Information Technology Security Analyst, pay grade 13.G33 AK ($40.95 / $7,098.00 - $54.85 / $9,507.33) based on internal equity. Under FLSA, positions in this classification are exempt from overtime.

2. In Unit 13, Non-Represented, Non-Supervisory, adopt and establish the classification Information Technology System Architect, pay grade 13.G32 AK ($38.90 / $6,742.67 - $52.16 / $9,041.06) based on internal equity. Under FLSA, positions in this classification are exempt from overtime.

3. Approve recommendation

I concur with the findings of the Human Resources Department and approve the actions detailed above.

Jan Fritz

Jan Fritz, Personnel Officer

7/12/18

Date

Copies to:
Copy of completed paperwork sent to the following: (Include names and e-mail addresses.)

Jan Fritz, Deputy County Administrative Officer; jfritz@co.marion.or.us
Colleen Coons-Chaffins, Business Services Director; ccoonschaffins@co.marion.or.us
Jane Vetto, County Counsel; JVetto@co.marion.or.us
HR Comp & Class; HRCompClass@co.marion.or.us
HR Processing; hrprocessing@co.marion.or.us

INFORMATION TECHNOLOGY
Scott Emry, IT Director; SEmry@co.marion.or.us
Cynthia Klein, Administrative Assistant; cklein@co.marion.or.us

Marion County
OREGON

Information Technology Security Analyst

Class Code 000
Bargaining Unit: 13
Non-Supervisory

FLSA: Exempt **EEOC**: 02 Professionals **Department**: Information Technology

GENERAL STATEMENT OF DUTIES

Plan, organize, manage, and administer information security programs, operations, and functions; develop and implement program and strategic planning; implement and assist in the development of information security program policies, procedures, and business practices; evaluate goals, objectives, priorities, and activities to improve performance and outcomes; recommend and establish administrative controls and improvements; develop procedures to implement new and/or changing regulatory requirements; serve as an advisor to the management team.

SUPERVISION RECEIVED

Works under general supervision of the IT Director who assigns work, establishes goals, and reviews the results obtained for overall effectiveness through the analysis of work products, observations, and meetings.

SUPERVISION EXERCISED

The employee does not typically supervise, but facilitates and leads representatives from county departments and coordinates with IT Department personnel to achieve the objectives of the Information Security Program plan.

DISTINGUISHING CHARACTERISTICS

Develops and maintains the framework for the organization's IT information security program. Evaluates and recommends new information security technologies and counter-measures against threats to information or privacy. Identifies information technology security initiatives and standards for the enterprise. Manages the development, implementation, and maintenance of information security policy, standards, guidelines, and procedures. Sets the access and authorization controls for everyday operations, as well as emergency procedures for data. Sets the standards for access controls, audit trails, event reporting, encryption, and integrity controls. Keeps abreast of latest security and legislation, regulations, advisories, alerts and vulnerabilities pertaining to IT assets.

EXAMPLES OF DUTIES (Duties may include, but are not limited to the following)

1. Develops and implements an ongoing risk management program targeting information security and privacy matters; determines the methods for vulnerability detection and remediation, and oversees ongoing vulnerability testing. Leads the information technology security assessments to identify risk due to changes or modifications to the computing environment. Directs the security assessments/audits to identify vulnerabilities in security program and policies. Controls testing of security procedures, mechanisms and measures. Collaborates with federal and state auditors, and subject matter experts for

satisfactory completion of compliance and program audits of the information security program.

2. Designated leader of security incident reporting and official responses to security incidents (breaches) responds to potential policy violations or complaints from external parties. Leads the oversight and activities for intrusion detection and response. Ensures the internal control systems are monitored and that appropriate access levels are maintained.
3. Acts as the Marion County's designee representing the Information Technology department on information security matters. Oversee the investigation and documentation of security breaches, misuse of computer resources, internet access, and other violations of information security policies, standards, and personnel rules governing use of technology by employees; develops after-action reports and testify in administrative or judicial proceedings.
4. Serves as the contact point for external auditors, survey requests, etc. and on security/privacy matters. Initiates, facilitates, and promotes activities to create information security awareness and training throughout the organization.
5. Plan, organize, manage, and administer information security programs, operations, and functions; develop and implement program and strategic planning; implement and assist in the development of program policies, procedures, and business practices; evaluate goals, objectives, priorities, and activities to improve performance and outcomes; recommend and establish administrative controls and improvements; develop procedures to implement new and/or changing regulatory requirements.
6. Work with internal stakeholders to enact, monitor and administer enterprise information security policies and standards; conduct the information security risk assessment program; coordinate contingency plan tests on a regular basis.
7. Provide expert guidance and reporting on information security issues to other departments, the general public, and/or outside agencies; represent the county to the public, elected officials, other agencies, governments, and organizations including making presentations, participating in meetings, and interacting with emergency services community; act as representative on committees, interagency task forces, and special projects.
8. Respond and resolve confidential and sensitive inquiries; investigate non-conformance and recommend corrective actions as necessary.
9. Analyze and review federal, state, and local laws, regulations, policies, and procedures in order to ensure compliance; conduct analysis on best practices and trends, and formulate and implement recommendations.
10. Develop, administer, assist, and monitor information security budgets; develop justifications for budgetary recommendations and/or adjustments; participate in forecasting additional funds for resources; identify, obtain, and manage funding from information security grants and interagency partnerships.
11. Attends and participates in professional meetings and stays abreast of new trends and innovations in the field of information security.
12. Actively participates in maintaining a safe and respectful working environment.
13. Perform other duties as assigned.

EXPERIENCE AND TRAINING

1. Bachelor's degree from a four-year accredited college or university with major coursework in Computer Science, Information Technology or a related field; AND
2. Five (5) or more years of progressive experience in computing and information security, including experience with Internet technology and security issues; OR
3. Any satisfactory equivalent combination of nine (9) years or more of education, training, and/or experience relevant to the position.

PREFERENCES

- Certified Information Systems Security Professional (CISSP), or formal security certifications from (ISC)², GIAC, CompTIA, ISACA.
- Information security principles and practices, including any of the following: security risk assessment standards, risk assessment methodologies, and vulnerability assessments.
- Senior level knowledge of mainstream operating systems and a wide range of security technologies, such as network security appliances, identity and access management (IAM) systems, anti-malware solutions, automated policy compliance tools, and desktop security software.

KNOWLEDGE, SKILLS AND ABILITIES

Knowledge of technology hardware and software which includes, but is not limited to systems, application languages, server based systems, cloud computing, personal computers, local and wide area network configurations and management, information/data management software and state-of-the-art system development and maintenance technologies; local, state, and federal laws, rules, policies, and regulations affecting information security and related technology and systems; strategic planning, preparation, and projection; and effective leadership and organizational communication principles and practices. Working knowledge of prevailing industry security standards and Common Body of Knowledge gained by way of CISSP, SANS, and/or CISA Certification(s).

Skills and abilities to manage and oversee comprehensive information security programs; lead diverse technologies, employees, and customer groups; communicate effectively in writing and orally, including the ability to make public or staff presentations; establish and maintain effective working relationships with a variety of individuals and groups, including customers in high-stress situations; and assist in confidential investigations. Skill in identifying information security problem areas, formulating diagnoses, and proposing practical solutions. Deep understanding of network infrastructure, including routers, switches, firewalls, and the associated network protocols and concepts. Ability to establish and maintain effective working relationships with employees, systems users, outside consultants and vendors.

The IT Security Analyst classification may require specific knowledge, experience, or skill sets based upon the technology, regulations, and business needs of the assigned county department. This may include experience with specific types of information system technology, complex database management systems or various business application areas relevant to the departmental business function [e.g., various engineering application systems; health care related services and insurance/client billing systems; and protective services confidential database systems].

ADOPTED
REVISED
MR

Information Technology System Architect

Class Code 000
Bargaining Unit: 13
Non-Supervisory

FLSA: Exempt **EEOC**: 02 Professionals **Department**: Information Technology

GENERAL STATEMENT OF DUTIES

Uses business strategy to lead, define, and coordinate technical solutions architecture that meets operational objectives. The position serves as the senior most technical expert for creating an integrated user experience across a broad set of technologies. Strategically design and implement information systems that support core organizational functions, and assure their effective and efficient operational availability. Gains organizational commitment for all systems and software plans, as well as evaluating and selecting all technologies required in delivering on those plans. In addition, provides technical leadership across the organization, from strategic decision making down to the project planning level. Responsible for defining the system architecture processes, standards and governance, as well as leading the integration of those processes with related business, IT processes, and standards.

SUPERVISION RECEIVED

Works under general supervision of the IT Director who assigns work, establishes goals, and reviews the results obtained for overall effectiveness through the analysis of work products, observations, and meetings.

SUPERVISION EXERCISED

Works independently under broad direction and occasional supervision, and may act as technical lead in providing work direction on large-scale, complex projects.

DISTINGUISHING CHARACTERISTICS

The IT System Architect is part of the Information Technology (IT) team responsible for establishing and implementing the strategic direction of the division and defines solutions that meet the business needs of end-user departments. The role of the IT System Architect demands deep and broad technical skills in multiple technical domains such as applications, server, cloud-based computing, storage, database, network, and security.

EXAMPLES OF DUTIES (Duties may include, but are not limited to the following)

1. Leads the development, implementation, and communication of architecture roadmap strategies, relevant policies, and standards that support IT department goals and objectives.
2. Consults with senior management staff in county departments regarding systems needs and information management opportunities.
3. Ensure that proposed and existing systems architectures are aligned with organizational goals and objectives.
4. Provide architectural expertise, direction, and assistance to others.

5. Develop, document, and communicate plans for investing in systems architecture, including analysis of cost reduction opportunities.
6. Conduct research on emerging technologies in support of systems development efforts, and recommend technologies that will increase cost effectiveness and systems flexibility.
7. Serves as the primary internal resource to senior technical staff and management regarding systems architecture issues; monitors and analyzes systems performance and evaluates costs, specifications, and organizational policies to recommend system performance tuning.
8. Document the organization's existing systems architecture and technology portfolio; make recommendations for improvements and/or alternatives.
9. Research complex technology products and services, prepare procurement specifications, evaluate vendor proposals and ensure compliance with standards and architectural plans.
10. Confers with vendors to determine suitability of products and services; makes recommendations for new products and services to IT management staff.
11. Consults with senior staff in preparing detailed specifications for countywide systems, diagrams, and network charts to implement new or existing systems.
12. Develop, document, communicate, and enforce processes and procedures for standardizing software, systems, and development and implementation methodologies.
13. Where applicable, design, develop, and oversee implementation of end-to-end integrated systems.
14. May share on-call duties with other staff members and respond in a timely manner 24 hours per day when problems arise.
15. Share knowledge and information with management, customers, and co-workers via written and verbal reports, presentations, training, and informal communication.
16. Maintain and improve technical knowledge including current and emerging technologies and best practices.
17. May schedule, assign, coordinate, monitor, and review the work of assigned staff.
18. Perform other duties as assigned.

EXPERIENCE AND TRAINING

1. Bachelor's degree from a four-year accredited college or university with major coursework in Computer Science, Information Technology or a related field; AND
2. Six (6) or more years of professional experience in one or more of the following disciplines: Technical Architecture, System Development, Business Analysis or Data Architecture; OR
3. Any satisfactory equivalent combination of ten (10) years or more of education, training, and/or experience relevant to the position.

PREFERENCES

Demonstrable experience with:

- Proficiently translating complex business issues into readily understood concepts for staff, management, and the public
- Developing assets such as enterprise applications and solution integration with focus on performance, scalability, re-use, source control, continuous building/integration
- Certification in Application Development or Application Architecture

KNOWLEDGE, SKILLS AND ABILITIES

Knowledge of principles, practices, and techniques of management of information systems; Information security, system integration, data and analytics, infrastructure application and program design, software systems development, business process design, and application portfolio management; Microsoft Active Directory environments with an understanding of ActiveSync; Network and security architectures and topologies including routers and switches, reverse proxies, firewalls, load balancers, SSL accelerators. Knowledge of architectural frameworks such as TOGAF, NIST-EA, Zachman; expertise in using industry standard notations for documenting business processes for use in architectural designs.

Current technologies of an information technology services department; Principles and practices of strategy formulation, program planning, and project management; Principles, practices, and applications of enterprise security practices and technical solutions; Advanced server platforms, virtualization technologies, systems and application software, and database administration; Compliance requirements for security and licensing within the services provided by the county departments; Techniques of analysis and programming of systems applications; Principles and practices for meeting quality standards for customer service; and Contracting for information services including contract negotiations and performance monitoring.

Skills and abilities to use logic and reasoning to identify and evaluate alternative solutions, conclusions, and approaches to problems; Identify complex problems and review related information to develop and evaluate different approaches and implement solutions; Negotiate and reach consensus on complex or contentious issues; Use professional judgment and decision-making to evaluate costs and benefits to potential solutions and choose the most appropriate one; Leverage and apply existing IT architectural solutions to business requirements; Apply knowledge and skills across a broad range of information technology disciplines, including application, data, infrastructure, and security domains; Analyze and summarize complex technical and organizational issues with ability to summarize life cycle cost-benefit summaries and risk analysis; Think creatively to develop, design, or create new applications, ideas, systems, or products; Develop long and short-range plans to meet established goals; Assist IT leadership staff in responding to operational issues in emergencies; Analyze situations accurately and adopt an effective course of action; Evaluate the effectiveness and efficiency of various computer applications and alternative systems; and Establish and maintain cooperative working relationships with individuals and groups who come from diverse backgrounds and represent members of the public, coworkers, and/or vendors. Read and understand information and ideas presented in writing or through spoken words. Communicate information and ideas orally and in writing so that others will understand.

The IT System Architect classification may require specific knowledge, experience, or skill sets based upon the technology, regulations, and business needs of the assigned county department. This may include experience with specific types of information system technology, complex database management systems or various business application areas relevant to the departmental business function [e.g., various engineering application systems; health care related services and insurance/client billing systems; and protective services confidential database systems].

ADOPTED
REVISED
MR