YAKIMA COUNTY, WASHINGTON
Class Specification
Class Title: Information Security Analyst

BAND: IT45			CLASS CODE: J23-3645	
DEPARTMENT: Information Technology	ACCOUNTABLE TO: Senior Director		JOB FAMILY: Information Technology	OVERTIME STATUS: Non - Exempt

JOB SUMMARY: Position is responsible for designing and implementing security systems to protect the County's workstations, servers, appliances, data, and networks from cyber attacks, and help set and maintain security standards.

DISTINGUISHING CHARACTERISTICS: The Information Security Analyst is a stand alone position. It differs from the Senior Technology Administrator in the level of responsibility for researching and implementing global operating systems and project management.

DUTY NO.	ESSENTIAL DUTIES: (These duties are a representative sample: (Position assignments may vary.)	BAND / GRADE
1.	Investigate security breaches and other cybersecurity incidents. Monitor the company's networks to keep an eye out for any security breaches and investigate it if one does occur. Document security breaches and assess the damage they cause.	C4
2.	Install security measures and operate software to protect systems and information infrastructure, including firewalls and data encryption programs. Recommend or fix detected vulnerabilities to maintain a high-security standard. Perform penetration testing.	B2
3.	Develop a security plan for best standards and practices for the company. Conduct frequent testing of simulated cyber attacks to look for vulnerabilities in the computer systems and take care of these before an outside cyber attack.	C4
4.	Research the latest in information technology security trends to keep up to date with the subject and use the latest technology to protect information. Research security enhancements and make recommendations to management. Stay up-to-date on information technology trends and security standards. Develop company-wide best practices for IT security.	B2
5.	Work with the Information Technology Services team or outside vendors to perform tests and uncover network vulnerabilities. Help colleagues install security software and understand information security management. Other duties as assigned.	C4

Knowledge: (Position requirements at entry):
Knowledge of:
- General computer operations
- Experience in information security or related field
- Experience with computer network penetration testing and techniques
- Understanding of firewalls, proxies, SIEM, antivirus, and IDPS concepts
- Ability to identify and mitigate network, server, and workstation vulnerabilities and explain how to avoid them
- Understanding of patch management with the ability to deploy patches in a timely manner while understanding business impact
- Customer service principles and techniques.

Class Title: Information Technology Security Analyst

Skills (Position requirements at entry):
Skills in:
- Using a personal computer and related software applications; operating basic office equipment
- Determining priorities and making critical decisions
- Developing projects
- Teaching and coaching others
- Developing, writing, applying, and implementing policies and procedures
- Resolving problems and conflicts
- Giving presentations, public speaking and facilitating meetings
- Researching and implementing compliance measures related to legislative requirements
- Good time management
- Establishing and maintaining effective working relationships with staff at all organizational levels, outside agencies, and with the public; and oral and written communication sufficient to exchange or convey information
- Business communication etiquette

Training and Experience (position requirements at entry):
Bachelor's Degree in Information Technology or Business AND 5years of large enterprise experience OR any equivalent combination of training and experience that would provide the required knowledge, skills and abilities to successfully perform the essential duties of the job.

Licensing Requirements (position requirements at entry):
Some positions may require a current Driver's license;
Successful completion of a criminal and / or financial background investigation and general employment verification.

Working Conditions: Position may have the potential exposure to the following:
Environment: work outside of standard business hours and multiple work locations;

Physical Demands: bending, carrying, handling, lifting, reaching, sitting, standing, walking, fingering, balancing, climbing, crawling, crouching, kneeling, hearing, smelling, talking, visual acuity.

Sedentary Work: Exerting up to 10 pounds of force occasionally and/or a negligible amount of force frequently or constantly to lift, carry, push, pull or otherwise move objects, including the human body. Sedentary work involves sitting, most of the time.

Intellectual Demands: ability to multitask, confidentiality, ability to work under pressure, ability to articulate and communicate in conversations, ability to follow written and verbal instruction.

Classification History:
New: 04/2022
Revised: 12/2022