PEA Job Description

1. Position Identification

<table>
<thead>
<tr>
<th>Position Number</th>
<th>992126, 992127</th>
</tr>
</thead>
<tbody>
<tr>
<td>Position Title:</td>
<td>Information Security Analyst</td>
</tr>
<tr>
<td>Department:</td>
<td>University Systems</td>
</tr>
<tr>
<td>Reports to:</td>
<td>Manager, Information Security Office</td>
</tr>
<tr>
<td>Number of Direct/Indirect Reports</td>
<td>Direct 0</td>
</tr>
<tr>
<td>Classification Level</td>
<td>SG 10</td>
</tr>
<tr>
<td>Last Updated</td>
<td>May 2018</td>
</tr>
</tbody>
</table>

2. Position Summary

University Systems (http://www.uvic.ca/systems/) serves a diverse client base including students, faculty and world-renowned researchers. We consist of three major units: Academic & Administrative Services, Infrastructure Services, and UVic Online, all working together to provide computing, communications and technology in support of the university's learning, teaching, research and administrative activities. We support high profile research projects and work as part of the BCNET consortium. We exist in a complex work environment where we must effectively navigate complex, cutting edge and ever-changing technology, and information security and privacy issues in order to be the best information systems organization in the Canadian university system.

Reporting to the Manager, Information Security Office, the Information Security Analyst assists in the monitoring and enforcement of information security policy and practice to ensure the confidentiality, integrity, and availability of the University's Information Resources. As a member of the Information Security Office, the Information Security Analyst supports day-to-day operations; analyzes and consults on security matters; responds to operational security issues; serves as a resource on security-related projects or projects with a security component; and leads select information security projects. In fulfilling the responsibilities and expectations of the role, this position promotes good information security practice to the University community. The Information Security Analyst is a trusted resource, providing guidance to technical staff and staff in units within the University, as well as collaborating closely with technical staff. This role uses their knowledge of moderately complex information security and systems-related experience to analyze and solve problems. Senior Information Security Analysts, the Manager, Information Security Office, and other senior leaders within University Systems provide guidance and direction on the resolution of more complex issues.

3. Key Responsibilities and Expectations

<table>
<thead>
<tr>
<th>Key Responsibilities</th>
<th>Expectations</th>
</tr>
</thead>
</table>
| Security Analysis/Consulting (15%) | • As part of a team, perform periodic security audits or reviews of existing systems; recommend methods for vulnerability detection and remediation; verify that issues identified are resolved in a timely manner.  
• Provide security audits or reviews of new systems prior to implementation; act as a security resource on projects with a security component.  
• Work with the University Privacy Office to ensure information security helps protect stakeholders’ privacy. |
- Work with Identity and Access Management personnel to promote appropriate access for users and systems.
- Assess vulnerabilities in systems and make recommendations for remediation.
- Work with technical and non-technical staff in other campus units in the completion of security analysis and consulting activities.

**Participate in Security Projects (35%)**

- Identify gaps in the existing information security; posture and research, plan, and execute additional projects to secure University Information Resources.
- Project areas may include replacement of existing/aging security infrastructure, development of additional security services, implementation of new security monitoring hardware and software.

**Security Operations (35%)**

- Respond to information security incidents, alleged policy violations, or complaints from internal and external parties; involves interaction with various groups within University Systems and across campus, the Information Security team, subject-matter experts and various external resources.
- Incident response may be required on a daily basis, is often of an urgent nature, and is important for preventing major breaches.
- Participates in day-to-day operational security activities, including security investigations, monitoring security services (intrusion prevention, firewall, anti-virus, endpoint protection, data loss prevention, disk encryption, system logs, security incident and event management)
- Interpret highly-technical information and perform log manipulation in order to analyze events and identify security issues.

**Security Awareness (15%)**

- Keep current with the latest security and privacy legislation, regulations, advisories, alerts, and vulnerabilities pertaining to the University.
- Ensure the appropriate staff across the University are aware of relevant security issues pertaining to their environments and information resources under their custody and control.
- Document standards, procedures, and best practices; Advocate good security practice across the University.
- Develop and deliver information security training materials and presentations to peers and university staff campus-wide.
- Participate in the higher educational security community (REN-ISAC, Educause, BCNET, CUCCIO, CCRIC etc.) through the exchange and contribution of information, and may attend conferences and make presentations.

**4. Classification Factors:**

**Problem-Solving:**

- Use investigative and analytical skills, prior experience, and a broad and deep technical understanding and knowledge of information security, UVic systems and business operations, to detect, analyze and assess the risk and impact of vulnerabilities, and to devise and recommend solutions to manage or eliminate vulnerabilities and mitigate risk.
• Periods of intense focus are often involved, and an immense body of knowledge covering networks, operating systems, applications, security is required.
• Significant technical troubleshooting and analysis required in often in highly stressful or time sensitive environments.
• Discretion is required as activities may involve highly-confidential or personally identifiable information.

**Responsibility for Financial & Material resources:**

• No direct responsibility for financial resources.
• Indirect financial impact through project management, project participation, risk mitigation, and incident response.
• Formulate and support recommendations requiring detailed specifications to Manager and/or Systems Leadership on the development, replacement, implementation, and support of university information systems.
• Shares responsibility for the confidentiality, integrity, and availability of the University's Information Resources.

**Responsibility for Human Resources:**

• Supervision provided by the Manager, Information Security Office; priority and direction established by Manager.
• Receives guidance from Manager and Senior Information Security Analysts on projects or trouble-shooting of operational security issues.
• Indirect supervision and guidance may be given to junior staff and/or co-op students.
• Mentors and trains staff on information security concepts.

**Impact of Decisions and Actions:**

• Responsible for correctly identifying security operational issues and incidents, which may have an immense impact on risk.
• Contributes to the overall reduction of information security risks to individuals and the University.
• Contributes to delivery of technical services to faculty, staff, and students in support of academic course work, administration, and research activities.
• Reduces the likelihood and impact of a security or privacy breach that may have financial and reputational implications to the University.

**Independence:**

• Formulate supportable recommendations to Manager and recommendations to other units, teams, and senior technical staff, usually through formal reports, meetings, and presentations
• When responding to urgent threats or incidents, makes collaborative decisions for containment or risk/impact-reduction purposes.
• Collaborate with Manager, other units, teams and senior technical staff in the monitoring, and enforcement of information security policy and practice.
• Informed guidance received from Manager and Senior Information Security Analysts.
• Actions and decisions guided by policy existing policy, procedures and practices.

5. **Summary of qualifications:**

This position requires a Bachelor's degree in a technical discipline (Computer Science or Computer Engineering preferred) and 3-5 years' experience working in an enterprise networking environment, and 1-3 years' experience in an information security-related function,

An equivalent combination of education, training and experience would be considered.
Essential knowledge and experience requirements include:

- Good understanding of TCP/IP and related network protocols.
- Broad knowledge of N-tier computing environments (web applications, database, networking, firewall, etc.)
- Basic scripting/programming knowledge (e.g. shell scripts, Perl, Ruby, Python, SQL)
- Broad knowledge of Windows, Mac, and Linux operating system environments
- Working knowledge of and experience in the environment of information security
- Experience with common open source security tools (Nessus, nmap, Wireshark, Snort, Metasploit, etc.)
- Experience with security services, such as Disk Encryption, Antivirus and Endpoint Protection, Intrusion Detection/Prevention and Firewalls, Desktop Management, Security Event and Incident Management, and Data Loss Prevention, is strongly desired.
- Experience in securing remote-access and mobile computing environments.

Essential competencies include:

- Demonstrate the highest standards of ethical conduct in ensuring the confidentiality, integrity, and availability of information resources.
- Demonstrated trust from peers and supervisors in regards to working with highly-confidential and personally identifiable information.
- Ability to communicate complex technical concepts to a non-technical audience through written and verbal communication.
- Ability to work both collaboratively in a team environment as well as independently.

The following criteria are considered an asset:

- Cybersecurity industry certifications such as GIAC, CISSP, ISACA, CEH or OSCP
- Experience with public sector privacy legislation and regulations (PIPEDA, FIPPA)
- Experience working in a post-secondary education environment or comparable size/complex organization
- Experience in delivering training and awareness to end users, and being a spokesperson or ambassador for information security issues.

<table>
<thead>
<tr>
<th>Employee’s Signature:</th>
<th>Date:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Manager's/Supervisor’s Signature</th>
<th>Date:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>