PEA Job Description

1. Position Identification

<table>
<thead>
<tr>
<th>Position Number</th>
<th>991724</th>
</tr>
</thead>
<tbody>
<tr>
<td>Position Title</td>
<td>Senior Information Security and Research Data Protection 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  Indirect 1-2</td>
</tr>
<tr>
<td>Classification Level</td>
<td>SG 15</td>
</tr>
<tr>
<td>Last Updated</td>
<td>October 2019</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 Senior Information Security and Research Data Protection 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. The analyst will work closely with Compute Canada’s security team, which sets national standards for the federation. This position requires the Analyst to work closely with colleagues as well as technical, administrative (legal), and scientific staff to provide support for research computing, and works closely with the Research Computing Services team. The Analyst consults with users to carry out information security assessments in an effort to align research initiatives with appropriate information technology solutions, and assists researchers in developing comprehensive security-focused data management plans. The Senior Information Security and Research Data Protection Analyst works to ensure the operational security of research computing systems and services, and acts as both a trusted advisor/consultant and subject matter expert providing guidance to and collaborating with the research computing services team, technical staff and staff in various units throughout the university. This position requires extensive contact with faculty, staff, researchers and students campus-wide, as well as partner organizations. This role uses their knowledge of highly complex information security and systems-related experience to analyze and solve problems. 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>% of time</th>
<th>Expectations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Analysis/Consulting (50%)</td>
<td></td>
<td>• Work across the Compute Canada federation to develop security policies and solutions for the national Advanced Research Computing platform.</td>
</tr>
</tbody>
</table>


- Provide multi-level support as it pertains to information security issues for large, interdisciplinary research projects.
- Provide advice and expertise to researchers working with sensitive data in implementation and design of project architecture.
- Provides expertise to research groups on data sharing and transfer agreements by providing advice and direction to define security plans and data management plans to facilitate compliance with related requirements from third parties.
- Oversee and lead security audits and/or reviews of new and existing systems; assess and recommend methods for vulnerability detection and remediation.
- Collaborate with other university offices such as the University Privacy Office and Identity and Access Management personnel to ensure protection of stakeholders’ privacy and appropriate access for users and systems.
- Work with technical and non-technical staff in other campus units in the completion of security analysis and consulting activities.
- Provides advice to University Systems leadership team and other senior management on related security issues.

<table>
<thead>
<tr>
<th>Lead in Security Projects (20%)</th>
<th>Identify gaps in the existing information security; posture and research, plan, and execute additional projects to secure University Information Resources.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Project areas may include replacement of existing/aging security infrastructure, development of additional security services, implementation of new security monitoring hardware and software.</td>
</tr>
<tr>
<td></td>
<td>Consult with faculty, technical staff, and vendors in the design of research computing systems and storage used in data- and compute-intensive research, including the maintenance, administration of big data, databases, storage systems, compute systems, and cloud infrastructure.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Security Operations (20%)</th>
<th>Respond to incidents, alleged policy violations, or complaints; with various campus teams, subject-matter experts and external resources.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Participates in day-to-day operational security activities and monitors information security vulnerability and relevant software release notes to assess and advice priorities for patching,</td>
</tr>
<tr>
<td></td>
<td>Interpret highly-technical information and perform log manipulation in order to analyze events and identify security issues.</td>
</tr>
<tr>
<td></td>
<td>Advocates for the maintenance of appropriate security controls across all research computing technologies.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Security Awareness (10%)</th>
<th>Keep current with the latest security and privacy legislation, regulations, advisories, alerts, and vulnerabilities pertaining to the University</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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</td>
</tr>
<tr>
<td></td>
<td>Document standards, procedures, and best practices; Advocate good security practice across the University;</td>
</tr>
<tr>
<td></td>
<td>Participate in the higher educational security community (REN-ISAC, Educause, BCNET, CUCIO, CCRIC etc.) and research computing community (Compute Canada, Westgrid, etc.) through the exchange and contribution of information, and may attend conferences and make presentations.</td>
</tr>
</tbody>
</table>
• Provides information security training, expert liaison, technical and administrative advice for researchers and other university staff to further facilitate safe and secure handling of sensitive research data.

4. Classification Factors:

Problem-Solving:
• The analyst interprets and investigates alternative methods, regulatory requirements, and products innovatively to ensure technical solutions conform to regulatory, departmental and university practices and policies, as well as federation policies and practices. The analyst investigates the needs of the organization, the situation, and those involved and provides innovative approaches to meeting the business needs.
• This role identifies trends and exceptions, investigates to define problems more accurately, identifies relationships and linkages between components, identifies potential causes and effects, and escalate issues of an exceptional nature.
• Discretion is required as activities may involve highly-confidential, personally identifiable information, or sensitive research data
• Continuous learning and upgrading of skills is critical to the effectiveness of this role.

Responsibility for Financial & Material resources:
• No direct responsibility for financial resources.
• 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:
• This role provides indirect supervision and guidance to junior staff and/or co-op students.
• This role mentors and trains campus staff on information security concepts.

Impact of Decisions and Actions:
• This role analyzes and develops solutions to manage highly confidential research data and mitigate security vulnerabilities. The analyst collaborates nationally with Compute Canada’s security team to set national policies and standards for the federation.
• Errors in implementation and support leading to breaches of security involving research systems or data could compromise the privacy and confidentiality of research subjects as well as cause severe reputational damage to the University and could also feasibly terminate existing and future data sharing agreements and research partnerships with collaborators and providers locally, nationally, and internationally.

Independence:
• Reporting to the Manager, Information Security Office the analyst leads research development of computing security and research data protection practices within the University and contributes to the strategic planning processes and development of the unit’s work plans.

This role will lead and recommend the direction of policy development, procedure and practice in research data protection.

5. Summary of qualifications:
This position requires a Bachelor’s degree in a technical discipline (Computer Science or Computer Engineering preferred) and 5 years’ experience working in an enterprise networking environment, and 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, operating system environments
- Strong knowledge of the Linux operating system environment
- 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.
- A Cybersecurity industry certification such as GIAC, CISSP, ISACA, CEH or OSCP

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:

- Good knowledge of virtualized environments and cloud computing platforms such as OpenStack.
- Experience with High Performance Computing environments
- 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.
- Experience supporting the research community and working in environments involving multiple stakeholders.

Employee’s Signature:  
Date:

Manager’s/Supervisor’s Signature  
Date: