Position Description

Technology Security Specialist

The Cooperative Bank

Our purpose

Our long-term aspirations are to develop more long-term value-based relationships with our customers, and for our people to grow and develop so that they are better off working at the Co-operative.

Our values

Our values represent who we are, how we think, and how we behave to bring these to life every day. You'll demonstrate behaviours that define our core values and support an inclusive culture with a strong teamwork spirit.

About the team

The purpose of the security team is to safeguard the organization's technology infrastructure and data by implementing robust security measures and responding to security incidents. Their key accountabilities include managing security tools, ensuring compliance with regulatory requirements, and proactively addressing potential threats to maintain a secure environment for both customers and staff.

Purpose of this position

The purpose of the Technology Security Specialist role is to ensure the security and integrity of the organization's technology infrastructure and data. This involves managing and optimizing security tools, participating in the Bank' on-call roster, responding to security incidents, and facilitating the collection of security-related data. The role is crucial in protecting the organization from cyber threats, ensuring compliance with regulatory requirements, and maintaining a secure environment for both customers and staff.

Position reports to: Head of Development, Testing, and Security

Challenges and opportunities of this role

- **Dynamic Environment**: The role involves working within a small, dedicated security team, providing a unique opportunity to make a significant impact and drive security initiatives across a mix of technologies and infrastructure.
- **Impactful Contribution**: With a small team, the Technology Security Specialist will have a significant impact on the bank's security posture, directly influencing policies and procedures.
- **Cross-Platform Integration:** The opportunity to work on SOC/SIEM integration with sources from AWS and Imperva WAF, enhancing the bank's overall security infrastructure and gaining valuable cross-platform experience.

How you will contribute:

What you'll do	Success will mean
Manage and enhance security tools	
Manage and optimize Microsoft Purview, Entra ID, and Defender to ensure robust security measures are in place. Ensure tools are configured to detect unusual activity and potential threats. Share knowledge of how to use and administer security tools. Collaborate with third-party vendors and security providers to ensure tools remain fit for purpose.	• Security tools are effectively utilized, reducing vulnerabilities and enhancing overall security • Regular updates and improvements are implemented, keeping the tools aligned with the latest security standards • Service Hub and other staff are trained and confident in using these tools
Implement and optimise security solutions and enhance data protection measures	
Support the implementation and effective use of security solutions to protect the organization's infrastructure and data. Contribute to the ongoing review and improvement of security tools, so our people are aware of risks and understand how to deal with potential security threats. Contribute to the creation and regular review of policies and standards that support the Bank's security solutions.	• Security solutions are effectively supported and maintained, ensuring optimal performance • The team is well-supported in using these solutions to address security threats • Improved security operations and reduced response times • Data protection measures are comprehensive and effective, reducing the risk of data breaches • Enhanced policies and procedures are in place, ensuring compliance with regulatory requirements

What you'll do	Success will mean
Stay up to date with the latest security trends, threats, and technology solutions.	• Continuous improvement in data security practices and awareness
Monitor and respond to security events	
Participate in the Bank's on-call roster. Monitor, detect, and respond to security incidents in a timely and efficient manner to minimize impact. Contribute to the resolution of complex or high priority incidents, working with the Technology Systems and Security Architect to resolve these in a timely manner. Provide advice or training to Business Units across the Bank to ensure security best practices are followed.	• Quick identification and resolution of security incidents, minimizing potential damage • Improved incident response times and processes • Enhanced overall security posture through proactive threat management
Security data collection	
Assist in gathering and organizing security-related data for reporting and analysis. Contribute to regular security audits and assessments, so improvements can be made.	• Accurate and comprehensive data is collected and organized, supporting effective security reporting • Stakeholders have access to reliable data for informed decision-making • Continuous improvement in data collection processes and methodologies
Healthy and safe work environments	
Follow all health and safety policies, standards, emergency procedures and plans. Participate in health and safety activities, training and meetings as required. Reports hazards, near misses, injuries, incidents, and ideas for continuous improvement. Cease work if an unsafe situation arises and seek assistance.	• Having healthy and safe ways of working • All workers feel empowered to and aware of opportunities to participate in health and safety activities • Our people can easily report hazards, near misses, injuries, incidents, and ideas for continuous improvement • Workers stop work if they feel unsafe and connect with their people leader or other workers for assistance

Decision making and responsibilities

a) **Decisions and/or financial accountabilities:**
- Day-to-day operations and routine maintenance
- Incident response – identifying, assessing, and responding to security incidents in real time
- Data collection, collation, and reporting
- Policy implementation
- Providing training and support to Bank Staff

b) **Actions and decisions that are recommended to a higher level of management for approval:**
- Strategic changes
- Major incident escalation
- Tool acquisition
- Compliance & Legal issues
- Cross-functional initiatives

Qualifications and experience

- Role requires 2-3 years' experience in technology security roles such as IT Support Specialist, Network Administrator, or System Administrator
- Tertiary qualified in Information Technology or Cybersecurity, or equivalent industry experience
- Experience in the financial services industry is preferred

Skills and attributes

Technical Skills

- Proven experience as a Microsoft system administrator
- Strong knowledge of Microsoft Purview, Entra ID, and Defender
- Hands-on experience in monitoring, detecting, and responding to security incidents
- Familiarity with SOC/SIEM integration, especially with multiple sources of data
- Experience with a vulnerability management tool such as Qualys or Tenable
- Experience with AWS, Imperva WAF and Darktrace is a plus
- Understanding of security best practices and frameworks
- Excellent problem-solving and analytical skills
- Strong communication and teamwork abilities
- Familiarity with change control processes

Personality Attributes

- Detail-oriented analytical thinking
- Clear and effective verbal and written communication
- Active collaboration
- Team player
- Adaptability
- Discretion

Leadership Skills

You will be expected to demonstrate behaviours from our Leadership skills framework through your actions, the way you work and how you work with others.