# Technical Services – CSOF5

Role summary for potential applicants

|  |  |
| --- | --- |
| Advertised Job Title**:** | O365 Security Engineer |
| Reference Number**:** | 58951 |
| Classification**:** | CSOF5 |
| Salary Range: | $97,276 - $105,571 plus up to 15.4% superannuation |
| Location**:** | Yarralumla, ACT; North Ryde, NSW; Clayton, VIC |
| Tenure: | Indefinite |
| Relocation assistance**:** | Will be provided to the successful candidate if required. |
| Applications are open to: | Australian Citizens Only |
| Functional Area**:** | Technical Services |
| % Client Focus - Internal: | 80% |
| % Client Focus - External: | 20% |
| Reports to the: | IT Security Manager |
| Number of Direct Reports: | 0 |

|  |
| --- |
| **Role Overview:** |
| Cyber Security Services is responsible for the provision of cyber security detection and prevention capabilities across the CSIRO corporate and scientific enterprise.  This position will directly support CSIRO’s migration to cloud based collaborative solutions in particular Office 365 and Azure. This position will work at the direction of the Security Architect actioning on their designs, with the guidance of the Security Architect support the project team along the journey of designing and building an accreditable Unclassified DLM instance of Office 365.  The incumbent will be responsible for representing Cyber Security Services working with immediate team members as well as teams across IMT and CSIRO business units to help promote cyber education and awareness, sustain effective and efficient secure systems and services, and promote cyber security as an enabler of CSIRO business, science and innovation.  Contributing to the quality of the service delivered to clients while playing a vital part in evolving strategic, tactical, and operational service direction. The incumbent will also be expected to demonstrate subject matter expertise through analytical investigation of complex and ambiguous problems as well as the application of adaptive and innovative solutions.  The incumbent will positively reinforce Cyber Security Services capacity and activities initially supporting complex enterprise scale Office 365 and Identity Access Management projects.  **Security Clearance**: This is a security assessed position and successful applicants will be required to obtain and maintain a security clearance of NV1 (SECRET). |
| **Duties and Key Result Areas:** |
| * Deliver security engineering expertise to Office 365 and Identity Access Management projects along with providing effective risk management support. * Define, design and implement appropriate controls to mitigate against the risks of cyber-attacks and mitigate vulnerabilities across the digital services and enterprise applications. * Analyse and resolve complex technical and cyber security issues. * Conduct scoping and security assessment of new on premise and cloud based systems, applications, and major updates. * Review and perform high quality modification of local IT Security policies and operational documentation including playbooks, SOPs, processes, and solution designs. * Contribute to the design, installation, configuration, monitoring, and management of cyber security capabilities and tools. * Develop and apply automation to simplify sophisticated processes where required through programming and scripting. * Other duties as directed. |

|  |
| --- |
| **Selection Criteria:** |
| *Please include a statement in your application addressing the selection criteria. Under CSIRO policy only those who meet all essential criteria can be appointed.*  ***Pre-Requisites:***   * **Education/Qualifications:** Diploma or degree in information technology, or equivalent relevant work experience. * **Security clearance:** currently hold or have the ability to obtain a security clearance of Negative Vetted 1.   ***Essential Criteria:***   1. A Minimum of 2 years experience working in a similar role. 2. Experience in the design, delivery and support of cloud environments and Identity & Access Management solutions (Microsoft Office 365, Azure Active Directory, AWS, Google) and secure integration with on premise infrastructure. 3. Sound understanding of Modern Authentication Protocols, DNS, Active Directory, Exchange, Networking, Security Enclave design, and Data Classification. 4. Experience in reviewing and securing physical (endpoints, servers, appliances), virtual (VDI, VMWare), and cloud based enterprise technologies. 5. Experience in conducting threat risk assessments and auditing through understanding of the latest threats and mitigation strategies. 6. Excellent interpersonal, collaboration, and communication skills along with the ability to apply initiative, autonomy, and team work. 7. Experience in the implementation of security controls, risk frameworks, and standards (ISO 27001, ASD Information Security Manual, and NIST).   **Desirable Criteria:**   1. Relevant certification in information security (e.g. CISSP, CEH, OSCP). 2. Relevant certification in cloud technologies (e.g. Microsoft, AWS, CCSP). 3. Experience with cloud security architecture and design using Cloud Access Security Brokers. 4. Sound knowledge of privacy compliance and adherence to the Australia Privacy Principles. 5. Experience working in a large complex environment.   **As Australia’s Innovation Catalyst, CSIRO has strategic actions underpinned by behaviours aligned to**:   * Excellent science * Inclusion, trust & respect * Health, safety & environment * Delivery on commitments.   **In your application and at interview you will need to demonstrate alignment with these behaviours.**  ***Other special requirements:***  This is a security assessed position and successful applicants will be required to obtain and maintain a security clearance of NV1 (SECRET). |

|  |
| --- |
| **Other Information:** |
| **How to Apply**  Please apply for this position online at <https://jobs.csiro.au/> and enter requisition number **58951.**  Please upload your Cover letter and CV (Maximum 2MB) as one document. You may also be required to respond to some on-line screening questions.  If you experience difficulties applying online call 1300 984 220 for assistance. Outside Australian business hours please email: [csiro-careers@csiro.au](mailto:csiro-careers@csiro.au).  **Referees**: Please provide contact details of two previous supervisor or academic/professional referees in your resume/CV. We will ask your permission before making contact.  **Contact:** If after reading the position details above you require more information please contact:  **Alfred Dera**via email: [Alfred.Dera@csiro.au](mailto:Alfred.Dera@csiro.au) or phone: **+61 2 9490 8956**  Please do not email your application directly to Mr Dera. Applications received via this method may not be considered by the selection panel.  **About CSIRO**  Australia is founding its future on science and innovation. Its national science agency, the Commonwealth Scientific and Industrial Research Organisation (CSIRO) is a powerhouse of ideas, technologies and skills for building prosperity, growth, health and sustainability. It serves governments, industries, business and communities across the nation.  Find out more! [www.csiro.au](http://www.csiro.au).    We work flexibly at CSIRO, offering a range of options for how, when and where you work. Talk to us about how this role could be flexible for you.  Find out more! [CSIRO Balance](https://www.csiro.au/en/Careers/A-great-place-to-work/Work-life-balance)  **CSIRO Information Management and Technology (IMT)** is committed to introducing and maintaining up-to-date, quality information services in support of CSIRO’s strategic objectives. Ongoing business engagement maintains strong connections between IMT and CSIRO’s research areas so that our services are closely aligned with CSIRO’s strategic objectives, and forms the basis for IMT's annual Operational Plans. |