Candidate Information Pack

Lead System Administrator - CYBER

Executive Level 1

Position details

Title	Lead System Administrator - Cyber
Classification	EL1
Location	Canberra
Salary Range	$145,137 - $169,572
Contact	Recruitment Phone: (02) 6261 1849
Closing Date and Time	Monday 13 April 2026 at 23:59 AEST

About ASIS

The Australian Secret Intelligence Service (ASIS) is Australia's overseas intelligence collection agency. We are Australia's experts at collecting highly sensitive information – secret intelligence – from sources overseas to keep Australia and our region safe and prosperous.

Our work spans continents and cultures. As a tech-powered and data-driven organisation, we use covert techniques and cutting-edge technology to put us in the right rooms, next to the right people, with the right access to the intelligence we need. We are tasked to collect intelligence – it might be political, military or economic information – deliberately withheld from the Australian Government that might present threats to or opportunities for Australia.

From graduates to career changers, we come from every corner of the country and all walks of life, with backgrounds from all around the world.

Regardless of our ethnicity, experiences and education, we're bound by a shared commitment to something bigger: building a better future for those who come after us. We seek to reflect the community we serve, and welcome applications from Aboriginal and Torres Strait Islander peoples, women, people with a disability, neurodiverse, people from culturally and linguistically diverse backgrounds and those who identify as LGBTQIA+.

It's a mission owned by everyone, with opportunities for all.

The role

The Lead System Administrator specialising in Cybersecurity plays a crucial role in engineering and maintaining our robust ICT infrastructure. In this hands-on leadership position, the Lead System Administrator will design, architect, and implement secure and scalable cybersecurity solutions tailored to our organisation's needs.

The Lead System Administrator - Cyber will apply their deep technical expertise to drive the administration and optimization of cutting-edge cybersecurity tools, ensuring our systems remain secure, resilient, and operationally efficient. They will lead the configuration, monitoring, and maintenance of security solutions to protect sensitive data and mitigate risks. Furthermore, they will share their expertise in mentoring and coaching junior team members whilst collaborating with cross-functional teams to drive capability engineering initiatives, system upgrades, testing, and maintenance efforts.

Role responsibilities

Under broad direction, the Lead System Administrator - Cyber will be responsible for the following key duties:

- **Design and Architecture**:
  - Lead the design and architecture of cutting-edge cybersecurity tools and solutions tailored to our organisation's needs.
  - Develop security strategies and roadmaps to enhance our overall security posture.
- **Technical Leadership**:
  - Provide technical guidance and mentorship to the system administration team.
  - Collaborate with cross-functional teams to drive cybersecurity initiatives, upgrades, testing, and maintenance efforts.
- **Security Operations**:
  - Oversee the administration and optimization of cybersecurity platforms to support our Security Operation Centre and ensure operational integrity.
- **Mentorship and Development**:
  - Mentor and coach junior team members, fostering their professional growth and development.
  - Conduct regular training sessions and knowledge-sharing activities to enhance the team's cybersecurity skills.
- **Stakeholder Communication**:
  - Effectively communicate complex technical concepts to both technical and non-technical stakeholders.

    - Collaborate with internal teams and external partners to align security efforts with business objectives.
- **Policy and Procedure Development**:
    - Develop and maintain cybersecurity policies, procedures, and standards whilst ensuring compliance with regulatory requirements and industry best practices.

Core skills

We encourage applicants with the following skills and attributes to apply:

- Demonstrated ability to design and deploy complex ICT infrastructure in enterprise or government environments both on-premise and cloud.
- Ability to develop and implement ICT system administration policies, strategies, and continuous improvement initiatives.
- Strong background across various system and applications used by cybersecurity teams (SIEM, AV/IDS, vulnerability management tools).
- Demonstrated ability to work across a full project lifecycle in collaborative teams.
- Strong leadership, mentorship, and ability to communicate effectively with technical and non-technical stakeholders.
- Demonstrated expertise in designing and architecting cybersecurity solutions.
- Ability to solve complex problems and make strategic decisions.
- Proficiency in various cybersecurity tools and technologies.
- Strong proficiency in Microsoft and Linux operating systems
- Technical skills across virtualisation, network fundamentals, cross-domain or multi-domain solutions, programming/scripting is desirable.

Education/Qualification/Experience requirements

The following education, qualifications and/or experience will be highly regarded:

- Proven experience in enterprise or government ICT environments, with a strong background in cybersecurity.
- Extensive experience in Operating Systems and Applications Patch Management processes.
- 6+ years of experience as a System Administrator.
- Professional certifications will be highly regarded.
- Bachelor's degree in Computer Science or Information Technology (not essential).
- Cloud experience is desirable.

Benefits of working at ASIS

ASIS employees enjoy access to generous workplace terms and conditions. Benefits include but are not limited to:

- Competitive salary plus 15.4% superannuation
- A variety of leave options including 22 days paid annual leave per year
- Paid leave between Christmas and New Year
- Domestic Relocation assistance for new staff to Canberra
- Health and wellbeing initiatives
- Salary packaging arrangements
- Learning and development opportunities including access to study assistance
- A variety of support services including but not limited to Employee Assistance Program (EAP) and a Staff and Family Support Office.

Whilst ASIS officers are not able to work from home due to the classified nature of our work, staff have access to a range of flexible working arrangements. These include part time hours, condensed hours and/or flexible start/finish times to support other responsibilities.

ASIS conditions of service are similar to those applying for the Australian Public Service, for a full list of benefits and conditions see asis.gov.au

Eligibility

To be eligible for a role you must:

- Be an Australian citizen
- Be assessed as suitable to hold and maintain a TOP SECRET-Privileged Access security clearance
- For more information on eligibility please see the Protective Security Policy Framework which is publicly accessible at protectivesecurity.gov.au, section 12 provides information on Eligibility and suitability

How to apply

Click on “Apply Now” on our website on the role/s that you are applying for. You will be required to submit the following:

- 800-word pitch outlining your skills and experience for the role
- A current CV, no more than 2 pages in length, outlining your employment history, academic qualifications and relevant training that you may have undertaken

- Details of two referees, which must include a current supervisor

Applicants are encouraged to consider the Integrated Leadership System (ILS) capabilities when preparing their application. For more information on the ILS, and tips for applying for jobs in Australian Public Service, please visit the APSC website found at www.apsc.gov.au.

All applications for employment with ASIS are handled in the strictest confidence. It is essential you maintain a similar level of confidentiality and that you do not discuss your application with anyone.

Important:

If you are currently living overseas and wish to apply for a role with ASIS, please note that we cannot contact you until you return to Australia. Every part of the recruitment process, including contacting you, must be done while you are in Australia.

If you have no plans to return to Australia in the foreseeable future, we recommend you wait until you return before submitting an application.

Reasonable adjustments

ASIS is committed to fostering a diverse and inclusive environment for candidates to participate in all stages of the selection process. Please let us know if you require any additional assistance or reasonable adjustments during any stage of the recruitment process and we will work with you to manage this throughout. If you are successful in gaining employment, reasonable adjustments can also be made available to you in performing your role.

Recruitment process – what happens next

We thank all applicants for their interest in a role with ASIS. Please be advised that our selection process is rigorous and extensive and that we do not provide feedback to unsuccessful applicants. **If you progress from application, you will receive an SMS requesting you to complete online testing – please ensure that you complete this testing or your application will not progress further.**

All selection process decisions are merit based and candidates must be prepared to undergo various selection stages throughout the process.

A merit pool will be established for candidates who are suitable for this round and will remain valid for 18 months.