Department of the Premier and Cabinet

Cyber Security Executive

Guideline to support implementation of Western Australian Cyber Security Policy clause 1.2 (Cyber Security Executive)

2024

Contents

Leading the development, implementation and updating of the entity business continuity plan

Ensures oversight of the inventory of the entity’s ICT environment, including critical databases and information assets

Ensures that physical and digital access to

an entity's personnel security activities aimed at mitigating the risk of unauthorised access to information at all stages of employment (pre-engagement, engagement, separation)

the employees' use of social media in the context of WA government advice on the use of social media

other activities as indicated by other whole-of-government or Commonwealth information security guidance on personnel risks.

The Cyber Security Executive oversees the process of recruiting adequately qualified cyber security operational staff to be employed at the entity.

Threat Detection

The Cyber Security Executive oversees threat detection activities and alignment with DGov's WASOC for their entity and is responsible for oversight of:

Continuous monitoring, analysis and triage of

Reporting of cyber security incidents to DGov's WASOC within 24 hours of detection.

Personnel Training

The Cyber Security Executive oversees the development and operation of their organisation's cyber security awareness training program. They should be able to foster positive security culture, where everyone understands importance of cyber security within the entity.

The Cyber Security Executive oversees the development and deployment of cyber security awareness training for all entity staff, as well as additional tailored cyber security training for staff in specialist positions, such as cyber security specialists, executives, finance/payroll staff or staff with access to personal and sensitive information.

Capability Profile

While it is recognised that not all individuals will meet all requirements, the following criteria represent a list of desirable qualifications and experience for a person in a Cyber Security Executive role.

It is recommended that a Cyber Security Executive be appointed at Tier 3 (Level 9) role. If you are considering appointing a cyber security executive at a lower tier, please discuss with DGov (cyber.policy@dpc.wa.gov.au)

10 to 15 years of experience in organisational and business strategy, IT strategic

T

Assistance

If you require assistance developing an Executive Job Description Form (JDF) please contact cyber.policy@dpc.wa.gov.au.

Additional Resources