Information Security Officer

Job Overview: Information Security officer is responsible for protecting an organization's computer systems and networks from cyber threats, unauthorized access, and data breaches. Analyzing security risks, implementing security measures, and monitoring systems to ensure confidentiality, integrity, and availability of data.

- **Policy Development**: implement and maintain information security policies, procedures, and guidelines.
- **Security Monitoring**: Monitor and respond to security alerts and incidents from intrusion detection systems, firewalls, and other security tools.
- **Incident Response**: Investigate security breaches, identify vulnerabilities, and lead the response to security incidents
- **Risk Assessment**: Conduct regular security assessments, including vulnerability scanning and penetration testing, to identify and mitigate potential security risks. Assess current technology architecture for vulnerabilities, weaknesses and for possible upgrades or improvement.
- **Security Architecture**: implement secure network and system architectures, ensuring proper configuration of firewalls, encryption, access controls, and other security measures. Implement and oversee technological upgrades, improvements and major changes to the information security environment.
- **User Awareness Training**: Conduct security awareness training for staff to educate them about potential cyber threats and how to mitigate them. Provide training to information security personnel during onboarding.
- **Compliance:** Provide insights and metrics to the ISGC on the information security compliance posture and its potential impact on ADNTC's objectives. Communicate information security goals and new programs effectively with the ISGC.
- **Disaster Recovery**: Work on disaster recovery and business continuity plans to ensure data is backed up and can be restored in the event of an attack or system failure.
- **Security Audits**: Assist in internal and external security audits, ensuring compliance with security controls.
- **Collaboration**: Work with cross-functional teams including IT, legal, and compliance departments to ensure an integrated approach to security across the organization. Ensure the consistent application of policies and standards across all technology projects, systems and services
- Proven experience in information security, network security, or IT operations.
- Strong knowledge of security frameworks, risk management principles, and best practices (e.g., NESA, ISO 27001).
- Experience with security tools such as SIEM (Security Information and Event Management), firewalls, IDS/IPS (Intrusion Detection/Prevention Systems), and encryption technologies.

- Proficiency with incident response methodologies, and handling security incidents and breaches.
- Experience in performing vulnerability assessments and penetration testing.
- Familiarity with network protocols, operating systems (Linux, Windows), and database security.
- Understanding of regulatory compliance requirements related to data security and privacy (e.g., GDPR, HIPAA).
- Strong problem-solving and analytical skills, with the ability to think critically under pressure.
- Excellent communication skills to work with technical and non-technical stakeholders
-

Preferred Qualifications:
Certifications such as CISSI (Certified Information Systems Security Implementer), CISM (Certified Information Security Manager), CEH (Certified Ethical Hacker), or CompTIA Security+.
Experience with cloud security (e.g., AWS, Azure).
Familiarity with security automation tools and scripting languages (e.g., Python, PowerShell).