Information Security Officer

Company Description

i3D.net is a leading provider of high-performance hosting and global infrastructure services. We offer a wide range of products and services including hosting, dedicated servers, cloud solutions, and more. With our global presence and state-of-the-art infrastructure, we serve clients in various industries including gaming, e-commerce, and enterprise businesses.

Job Description

The Information Security Officer (ISO) will be responsible for overseeing information security, cybersecurity and IT risk management programs based on industry-accepted information security and risk management frameworks, such as those from ISO 27001 and NIST-standards. The ISO works to improve the maturity level of information security, state of cybersecurity and IT risk best-practices across the company. The ISO is an integral part of the Security & Compliance team and reports directly to the Security & Compliance Manager.

Scope

The right candidate has an impeccable reputation and has no problem passing applicable background checks and providing the mandatory (Dutch) VOG-document as the candidate oversees an organization with multiple functional disciplines/occupations and may have to manage programs, regardless of size, that may have a critical impact on the company. Responsibility to formulate and administer policies and programs in all areas of Information security, including but not limited to human resources, development, project & service management and physical assets, and the ability to function with a high degree of autonomy. The Information Security Officer is accountable and the delivered work and leads our current certifications for ISO 27001 and NEN7510, including any future certifications. The ISO also negotiates and influences others to help them understand and accept new concepts, practices, and approaches in the field of information security.

Key Responsibilities

- Takes ownership towards the continuous development, implementation and updates of security and privacy policies, standards, guidelines, baselines, processes, and procedures in compliance with local, state, and federal regulations and standards for I3D.net information systems in our High-Level Structure Document (HLS).
- Be a sparring partner for your colleagues.
- Review and maintain our certifications e.g., ISO 27001 and NEN 7510.
- Proactive identification and mitigation of IT risks as well as responding to observations identified by third party auditors or examiners while assisting in the development of periodic reports and dashboards presenting the level of controls compliance and current IT risk posture.
- Assist managers and staff with the audits and facilitate management response and remediation efforts. Ensure overall IT compliance with regulatory requirements through proactive planning and communication, ownership, and relationships.
- Identify acceptable levels of residual risk and assist with action plans, policy, and procedural changes for risk mitigation. Provide strategic recommendations to key IT projects to help improve project results, quality of deliverables, risk optimization, security processes and compliance with regulations.
- Facilitate information systems security management education and training in regulatory and industry standards for all I3D.net employees.
- Collaborate with the Security Operations Center on security incidents and contribute to any investigations.
- Ability to work with local, state, and federal authorities requiring information and reports on security incidents to include police or other law enforcement agencies.
- Occasional travel to our other offices and owned datacenters may be required.

Interested?

Reach out to Arjan Koopen or Paul Hoogsteder, who are attending DENOG15 themselves or scan the QR code to see more information!