Chief Information Security Officer

Soort functie:	Vaste medewerker	**Locatie:**	regio Mechelen
Duur:		**Referentie:**	201806851

Omschrijving:

The chief information security officer (CISO) is the head of ICT security, designing and driving the corporate ICT security strategy and coordinating the implementation of the ICT security strategy locally and centrally, to protect the business from security threats and cyber-hacking. The ICT security strategy should comply to all ISO and other standards and regulations. This is a senior role within the company and reports directly to the Corporate Director ICT (CIO) of the company and is part of the Corporate Management Team ICT.
He coaches local ICT staff responsible in their respective operational entities for the implementation of corporate ICT security strategy.

The day-to-day
- Creating and implementing a strategy for the deployment of information security technologies
- Performing ICT security risk assessments and reporting on ways to minimize threats
- Monitoring security vulnerabilities and hacking threats in network and host systems
- Tracking latest ICT security innovations and keeping abreast of latest cyber security technologies
- Advise the local ICT staff in ensuring business continuity
- Communicating with key stakeholders about ICT security threats
- Implementing an effective process for the reporting of security incidents
- Overseeing the investigation of reported security breaches
- Developing strategies to handle security incidents and trigger investigations
- Managing the ICT security team (decentralized organization, centrally managed), security experts and advisors
- Complying with the latest regulations and compliance requirements
- Championing and educating the organization about the latest security strategies and technologies

Key responsibilities
- Overlook the daily operation and implement the ICT security strategy
- Conduct a continuous assessment of current ICT security practices and systems and identify areas for improvement
- Run security audits and risk assessments
- Deliver new security technology approaches and implementing next generation solutions
- Oversee the management of the decentralized ICT security staff, giving leadership to the team and developing staff
- Ensure compliance and governance is met
- Drive change projects and building new ICT capabilities
- In close collaboration with the local ICT departments develop and implement business continuity plans to ensure service is continuous when a change program is introduced or a security breach occurs or in the event that the disaster recovery plan needs to be triggered
- Define strategies and selection of ICT solutions to minimize the risk of cyber-attacks and to protecting the intellectual property of the organization at all times
- Define systems to reviewing, analyze and deliver data information
- Communicate digital program and strategy to a range of stakeholders
- Manage the ICT security budget and communicating this with the appropriate parties
- Report to the ICT Management board and being an active member of the senior management team

Key skills

- Digital leadership skills – capable of empowering and leading a decentralized ICT team to meet business and ICT security goals
- Solid people management skills – providing direction, monitoring performance, motivating staff and building a positive working environment
- Ability to adapt to a fast-moving ICT landscape and keep pace with latest thinking and new security technologies
- A passion for technology and security safeguarding with a desire to deliver
- Thrives on change, showing an impressive ability to drive the ICT security strategy forward
- Analytical mind capable of managing numerous information sources and providing data analysis reports to senior management
- Strong customer focus – able to meet the demands of internal and external customers
- Excellent communication skills – providing verbal and written communication that is outstanding to both direct reports and senior management as well as other stakeholders
- Flexible and adaptable – capable of changing direction where required and showing flexibility to meet new demands
- Forms business partnerships that help drive the IT security strategy forward
- Can make decisions that are well informed and timely
- Creative thinking – able to look at alternatives and consider new ways of thinking to problem solve
- Multi-tasking – can manage several concurrent projects and prioritize demands

Vereisten:

Qualifications
A Masters' degree is a minimum in computer science or in a related area or extensive relevant experience. A Master's degree in business administration is highly desirable.

Relevant experience
- This level of seniority demands around a decade of proven IT security experience
- Change management and business process experience is ideal together with a proven track record of driving large-scale change programmes
- Experience of managing a team
- A proven record of dealing with complex projects and meeting conflicting demands

Hours
This is a senior level position with an attractive salary package on offer. Working hours are typically contracted as a normal working week – Monday to Friday 9:00am to 5:00pm - but a CISO is expected to work extended hours to match the peaks and troughs of project flows, typically when a new system is implemented, to ensure business continuity.

Start: 2018-07-31 22:00:00