

Technical Information Security Officer (TISO)

Een veilige, weerbare en toekomstbestendige digitale Hanze; dat is jouw missie als Technical Information Security Officer (TISO). Je vertaalt wet- en regelgeving, dreigingen en risico's naar praktische beveiligingsmaatregelen die bijdragen aan veilig onderwijs, onderzoek en bedrijfsvoering. Daarbij werk je nauw samen met collega's van informatiebeveiliging, privacy, architectuur, IT-beheer en datamanagement. Cybersecurity zien wij als een essentieel onderdeel van onze digitale dienstverlening en kwaliteitszorg.

Dit ga je doen

Je bent lid van het Privacy & Security team van de afdeling Generieke Diensten IT binnen het cluster Business, Support & IT. Samen met collega's werk je aan het versterken van de digitale weerbaarheid van de Hanze. Je draagt bij aan de verdere professionalisering van informatiebeveiliging en ondersteunt de uitvoering van het project Hanze Informatiebeveiliging. Je adviseert over technische informatiebeveiliging en helpt bij het implementeren van beveiligingsmaatregelen binnen onze onderwijs-, onderzoeks- en bedrijfsvoeringsprocessen. Daarbij werk je samen met beheerders, architecten, technisch specialisten, projectleiders, informatiemanagers en leveranciers.

- Samen met ICT-teams, proceseigenaren en projectleiders identificeer je risico's, kwetsbaarheden en dreigingen. Je vertaalt deze naar concrete en haalbare beveiligingsmaatregelen.
- Je adviseert over de toepassing van wet- en regelgeving en normenkaders zoals NIS2, ISO 27001 en NIST binnen de Hanze.
- Je ondersteunt projecten en verandertrajecten vanuit het principe Security by Design en Privacy by Design.
- Je beoordeelt technische ontwerpen, cloudoplossingen en architecturen op beveiligingsaspecten.
- Je stelt technische beveiligingsrichtlijnen, standaarden en procedures op en helpt deze te implementeren.
- Je voert risicoanalyses, kwetsbaarheidsanalyses en security-assessments uit en adviseert over passende beheersmaatregelen.
- Je begeleidt en coördineert penetratietesten en bewaakt de opvolging van bevindingen.
- Je ondersteunt bij security-incidenten, calamiteiten en herstelactiviteiten en levert een bijdrage aan business continuity en disaster recovery.
- Je monitort de effectiviteit van beveiligingsmaatregelen en rapporteert hierover aan management, projectteams en de CISO.
- Je draagt bij aan bewustwording rondom informatiebeveiliging en bent een vraagbaak voor collega's binnen de Hanze.
- Je signaleert ontwikkelingen op het gebied van cybersecurity en vertaalt deze naar verbeteringen voor de organisatie.

Hier ga je werken

Je komt te werken binnen het cluster Business, Support & IT. Binnen dit cluster staan optimale processen, digitale vernieuwing en betrouwbare dienstverlening centraal. We bieden service, advies en ondersteuning op het gebied van student- en HR-administratie, Finance, IT, International Office, Privacy & Security en Mediatheekdiensten.

Het leveren van kwalitatief hoogwaardige, veilige en efficiënte dienstverlening staat hierbij centraal. Naast het borgen van continuïteit in de dienstverlening werken we voortdurend aan het verbeteren van processen rondom onderwijs, onderzoek en bedrijfsvoering. Cybersecurity speelt daarbij een steeds belangrijkere rol.

Dit vragen we van jou

Je weet hoofd- en bijzaken te onderscheiden, schakelt gemakkelijk tussen strategie en uitvoering en voelt je thuis in een complexe organisatie. Je bent analytisch sterk, neemt initiatief en weet anderen mee te nemen in jouw adviezen. Daarnaast houd je van samenwerking, investeer je in relaties en weet je collega's te inspireren en te overtuigen. Verder beschik je over uitstekende communicatieve vaardigheden, zowel mondeling als schriftelijk.

Verder:

- je hebt minimaal een afgeronde hbo-opleiding op het gebied van Informatica, Cyber Security, Information Security Management, Integrale Veiligheid of een vergelijkbare richting. En je hebt werkervaring in een soortgelijke functie;
- je hebt kennis van en ervaring met het opstellen, implementeren en toetsen van technische beveiligingsmaatregelen en kennis van normenkaders en wet- en regelgeving zoals NIS2, ISO 27001/27002 en NIST;
- je hebt ervaring met cloud- en/of on-premise infrastructuren, bij voorkeur binnen Microsoft 365 en Azure;
- je hebt kennis van Identity & Access Management, vulnerability management, endpoint security en netwerkbeveiliging;
- je weet hoe je met ITIL- en Agile/Scrum-werkwijzen moet omgaan;
- je beschikt bij voorkeur over één of meer van de volgende certificeringen: CISSP, CISM, CISA of vergelijkbaar.

Mocht je niet volledig aan het profiel voldoen maar wel enthousiast zijn over deze functie, dan nodigen we je van harte uit om te solliciteren. We zijn benieuwd naar jouw verhaal.

Dit krijg je ervoor terug

Een uitdagende functie met directe impact op de digitale veiligheid van onderwijs, onderzoek en bedrijfsvoering.

- Een dienstverband van 0,8 tot 1,0 fte. Startdatum is zo spoedig mogelijk.
- In eerste instantie een jaarcontract, met uitzicht op verlenging.
- Schaal 10 (min. € 3.639,- en max. € 5.699,-), conform cao-hbo. Het salaris is bruto per maand bij een fulltime dienstverband. Inschaling vindt plaats in de functie Medewerker Informatievoorziening E of D. De uiteindelijke inschaling binnen de functie wordt vastgesteld op basis van relevante werkervaring, kennis, vaardigheden en competenties.
- Een vakantie-uitkering van 8% en een structurele eindejaarsuitkering van 8,3%.
- Maximaal 53 verlofdagen op jaarbasis, en daarnaast kun je gebruik maken van duurzame inzetbaarheidsuren en thuiswerkfaciliteiten.
- De mogelijkheid om je voortdurend te professionaliseren via onze Hanze PL Academy.

Nieuwsgierig naar meer?

Wil je meer weten over deze functie? Neem dan contact op met Ellen Ramaker, manager ICT Infrastructuur, via 050-5956726 of e.j.ramaker@pl.hanze.nl. Tijdens de herfstvakantie per mail bereikbaar, je wordt na de vakantie teruggebeld. Let op! Dit e-mailadres niet gebruiken voor je sollicitatie. Klik daarvoor op de sollicitatiebutton.

Word jij onze nieuwe collega?

Stuur dan je cv en motivatie via de sollicitatiebutton.

- Sluitingsdatum is **1 november 2026**.
- Gesprekken zijn op **vrijdagochtend 6 november 2026**.
- Wij vragen nieuwe medewerkers om bij indiensttreding een Verklaring Omtrent het Gedrag (VOG) aan te vragen. De kosten worden door de Hanze vergoed.

Acquisitie naar aanleiding van deze vacature wordt niet op prijs gesteld