Universiteit Leiden

Statement informatieveiligheid

De Universiteit Leiden hecht grote waarde aan de kwaliteit en betrouwbaarheid van informatie in het tijdperk van digitalisering en ketenintegratie. Informatie is één van de belangrijkst bedrijfsmiddelen voor de domeinen Onderzoek, Onderwijs en de Bedrijfsvoering. Toegankelijke en betrouwbare informatie is namelijk essentieel voor een universiteit.

Als toonaangevende universiteit streven wij ernaar om een veilige en betrouwbare informatievoorziening te bieden aan studenten, onderzoekers, medewerkers (waaronder docenten) en (keten)partners.

Het 'Strategisch beleid informatiebeveiliging' vormt de leidraad voor het borgen van adequate informatieveiligheid binnen de Universiteit Leiden. Onze visie op informatieveiligheid is gebaseerd op het besef van de groeiende dreiging van cybercriminaliteit en statelijke actoren, evenals de toenemende afhankelijkheid van digitale processen en systemen. We erkennen dat succesvolle onderwijs- en onderzoeksactiviteiten steeds meer afhankelijk zijn van goed beveiligde informatie, nieuwe technologieën en computersystemen.

Belangrijke doelen van ons informatiebeveiligingsbeleid zijn het waarborgen van de betrouwbaarheid en continuïteit van onderwijs-, onderzoeks- en bedrijfsvoeringsprocessen, het bieden van een veilige leer-, onderzoeks- en werkomgeving en het beheersen van informatiebeveiligingsrisico's door passende beheersmaatregelen te treffen.

Wij hanteren vijf beleidsprincipes:

1. *Informatiebeveiliging is risicogestuurd*
   We baseren de maatregelen op de mogelijke veiligheidsrisico's van onze informatie, processen en IT-faciliteiten.

2. *Informatiebeveiliging is een verantwoordelijkheid van iedereen*
   Iedereen is en voelt zich verantwoordelijk voor een juist en veilig gebruik van middelen en bevoegdheden. Beleid en technische maatregelen zijn niet voldoende om risico's op het terrein van informatiebeveiliging uit te sluiten. De mens zelf creëert de grootste risico's. We werken daarom voortdurend aan het vergroten van het beveiligingsbewustzijn om kennis van risico's te verhogen en veilig en verantwoord gedrag aan te moedigen

3. *Informatiebeveiliging is een continu proces*
   Informatiebeveiliging zit in het DNA van al onze werkzaamheden. Informatiebeveiliging is een continu proces, waarbij we steeds kijken naar mogelijke verbeteringen. Dit gebeurt onder andere door jaarplannen, controles en bijsturing.

4. *Security by Design*
   Informatiebeveiliging is vanaf de start een integraal onderdeel van ieder project of iedere verandering m.b.t. informatie, processen en IT-faciliteiten.

5. *Security by Default*
   Gebruikers hebben alleen toegang tot informatie en IT-faciliteiten die zij nodig hebben voor hun werkzaamheden. Het openstellen van informatie is een bewuste keuze.

Om de effectiviteit van het informatiebeveiligingsbeleid te waarborgen, worden regelmatig controles, assessments en audits uitgevoerd. Hierbij evalueren we de naleving van het beleid en rapporteren we hierover aan het College van Bestuur. De Chief Information Security Officer (CISO) beoordeelt jaarlijks ook de effectiviteit van het informatiebeveiligingsmanagementproces en adviseert het College van Bestuur op basis van verzamelde gegevens en informatie.

Wij nodigen u uit om het volledige 'Strategisch beleid informatiebeveiliging' te lezen, waar onze visie, doelen, uitgangspunten en verantwoordelijkheden in zijn beschreven. Samen streven we naar een veilige, betrouwbare en toekomstbestendige Universiteit Leiden waarin de privacy en rechten van onze studenten, docenten, onderzoekers, medewerkers en andere betrokkenen worden gewaarborgd.

Voor eventuele vragen inzake dit beleid kan contact opgenomen worden via security@BB.leidenuniv.nl