Security Statement Universiteit Leiden

Hoe de Universiteit Leiden omgaat met security

In het kader van het onderwijs- en onderzoeksproces en bedrijfsvoering worden gegevens van studenten, medewerkers en relaties vastgelegd. In het privacy statement geven wij aan hoe de universiteit omgaat met het verzamelen en gebruiken van persoonsgegevens voor de verwerking van bovengenoemde processen. Dit security statement geeft informatie over hoe de Universiteit Leiden omgaat met informatiebeveiliging.

Uitgangspunt

De universiteit neemt veiligheid en privacy serieus en streeft ernaar om ervoor te zorgen dat gebruikersgegevens veilig worden verkregen en bewaard. Dit security statement is erop gericht om duidelijkheid te bieden over onze beveiliging zodat u er zeker van kunt zijn dat uw gegevens voldoende beschermd worden.

De Universiteit Leiden werkt met betrekking tot informatiebeveiliging conform de Code voor Informatiebeveiliging (NEN norm 27001/2). De persoonsgegevens worden verwerkt conform de Wet bescherming persoonsgegevens.

Concreet worden bovenstaande normen uitgewerkt in een aantal documenten. Belangrijk zijn het Informatiebeveiligingsbeleid en de Baseline van maatregelen die moeten worden genomen. Er worden risicoanalyses op systemen verricht om de classificatie van gegevens te bepalen en daarna de maatregelen die voor die systemen moeten worden genomen. Verder wordt er gewerkt aan campagnes om het bewustzijn van de medewerkers en studenten te vergroten.

Informatiebeveiliging

Het doel van beveiliging is enerzijds het waarborgen van de continuïteit van de bedrijfsprocessen en anderzijds het minimaliseren van eventuele schade, direct of indirect, die ontstaat uit beveiligings-incidenten. Dit doel wordt bereikt door het treffen van een evenwichtig pakket preventieve maatregelen (het voorkomen van incidenten), alsmede repressieve en correctieve maatregelen (gericht op het beperken van de negatieve gevolgen van incidenten). De Code voor Informatie-beveiliging richt zich niet alleen op de beveiliging van informatie in computers en netwerken, maar op alle vormen van informatie, dus bijvoorbeeld ook de informatie die is opgeslagen in papieren documenten.

De informatiebeveiliging kent drie aspecten: beschikbaarheid, integriteit en vertrouwelijkheid. De beschikbaarheid moet aansluiten bij het gebruik in het proces en daarom neemt de universiteit maatregelen tegen o.a. overbelasting van computers of het niet goed functioneren hiervan. Bij integriteit van gegevens gaat het om maatregelen die het ongeautoriseerd toevoegen, wijzigen en wissen van gegevens tegengaat. Vertrouwelijkheid is belangrijk zodat het netwerk niet wordt afgeluisterd of anderszins door hackers wordt gecompromitteerd.

Beveiligingsprincipes

Een aantal beveiligingsprincipes die de universiteit hanteert zijn:
- we voorzien alle ICT voorzieningen van logische toegangscontrole (toegang alleen na expliciete toestemming; alle gebruikers zijn uniek herleidbaar tot een natuurlijk persoon; de authenticiteit van de gebruiker wordt vastgesteld op basis van identificatie)
- we delen ICT voorzieningen in zones in waarbinnen gegevens vrijelijk kunnen worden uitgewisseld. Uitwisseling met andere zones verloopt via koppelvlakken. Doel hiervan is isolatie van risico's
- we gebruiken diverse fysieke en logische beveiligingsmaatregelen. Dit betekent dat het doorbreken van één maatregel niet leidt tot de val van het hele systeem.

Controle

Omdat de ontwikkelingen binnen de informatiebeveiliging snel gaan wordt elk jaar en bij aanpassing van het systeem gecontroleerd of de maatregelen nog adequaat zijn via risicoanalyse en audits. Deze audits worden getoetst door een externe partij. De uitkomsten hiervan zijn input voor nieuwe maatregelen.

Ondanks alle inspanningen kan het gebeuren dat er een incident plaatsvindt. Voor het omgaan met incidenten zijn processen ingericht. Een absolute veiligheid kan namelijk niet worden gegarandeerd. Als de Universiteit Leiden kennisneemt van een inbreuk op de beveiliging zullen wij de getroffen gebruikers op de hoogte stellen, zodat zij passende beschermende maatregelen kunnen nemen. Tevens zal de inbreuk zo spoedig mogelijk worden verholpen. Meldingsprocedures omvatten kennisgeving per e-mail of publicatie van een melding op onze website.