Begrippenlijst voor beleidsdocumenten

Informatiebeveiliging

document

identificatie	OU Begrippenlijst voor beleidsdocumenten
status	Definitief
auteur(s)	Martin Romijn
eigenaar	Chief Information Security Officer (Martin Romijn)
opgeslagen	Teams-omgeving

wijzigingshistorie

datum	Wijziging
30-08-2022	Initiële versie naar aanleiding van definities in beleidsdocumenten (verplaatst naar nieuw document begrippenlijst)
03-11-2022	Bijgewerkt naar aanleiding van reviews beleidsdocumenten, kolom voorbeelden toegevoegd
03-01-2023	Laatste details en in de huisstijl gezet, informeel aangeboden aan IT commissie van de ondernemingsraad
20-10-2023	Omgezet in definitieve versie en Pdf i.v.m. vaststelling door het College; paginanummering toegevoegd

accordering

acroniem	handtekening	datum
Cvb	Vastgesteld per Cvb besluit na advies (en waar nodig instemming) van de medezeggenschapsraden.	26 september 2023

Lijst van begrippen die voorkomen in beleidsdocumenten van de OU

Voor de betekenis van gebruikte termen wordt primair gebruik gemaakt van de definities uit het Cybersecurity woordenboek 2021. Daar waar de termen niet in het woordenboek voorkomen, wordt maximaal aangesloten bij de terminologie zoals deze door ITIL wordt gebruikt.

Term	Betekenis	Voorbeeld binnen de OU
Account	Element van een digitaal systeem dat een gebruiker representeert. Bij een account hoort informatie over de gebruiker, zoals persoonlijke gegevens, inloggegevens en informatie waar de gebruiker bij mag. Er bestaan verschillende soorten accounts, zoals een gebruikersaccount of een administratoraccount voor beheerders.	Het Microsoft-account dat je gebruikt voor het inloggen op webmail of Teams.
Autorisatie	De bevoegdheden die een Gebruiker van een computersysteem heeft om toegang te krijgen tot gegevens of handelingen te mogen uitvoeren. Bijvoorbeeld het opstarten van programma's of het inzien, wijzigen of wissen van informatie.	
AVG	Algemene Verordening Gegevensbescherming. Deze is per 25 mei 2018 van kracht.	
Back-up	Een reservekopie van gegevens of digitale systemen. Hiermee kan men gegevens of systemen herstellen als het origineel beschadigd of weg is.	
Bedrijfsmiddel	IT-infrastructuur in bezit van de organisatie die helpt om de IT-diensten te leveren: de hardware en software.	Applicaties zoals ANS en O4U, bekabeling, besturingssystemen zoals Linux en Windows, T-schijf, laptop, firewall en switch.
Bedrijfsproces	[ITIL] Een proces dat eigendom is van en uitgevoerd wordt door een bedrijf. Een bedrijfsproces draagt bij aan de levering van een product of service aan een bedrijfsklant. Bijvoorbeeld, een winkelier kan een inkoopproces hebben dat helpt om diensten te leveren aan klanten. Veel bedrijfsprocessen steunen op IT- diensten.	
Betrokkene	Een individueel en natuurlijk persoon op wie een Persoonsgegeven betrekking heeft.	
Beveiligingsupdate	[Patch] Een nieuwe versie van software waarin bekende kwetsbaarheden in het systeem zijn verholpen.	
Bezoeker	De natuurlijke persoon die, anders dan als Medewerker, op legale gronden een ruimte wenst te betreden.	Onderhoudsmonteur, schilder, schoonmaker.
BIV-classificatieniveau	Model om drie verschillende kenmerken van informatiebeveiliging aan te duiden: beschikbaarheid, integriteit en vertrouwelijkheid van informatie en informatiesystemen. Met andere woorden: is de informatie en het systeem op het gewenste moment te zien en te gebruiken? Klopt de informatie? En wie mag de informatie zien en het systeem gebruiken?	

Cryptografische sleutel	Een sleutel om via een algoritme informatie om te zetten in een code zodat een ander het niet kan lezen.	
Data	Vastlegging van Feiten of begrippen in gegevens die zich lenen voor communicatie en bewerking door computers of andere machines.	In een computer (of soortgelijke machine) vastgelegde gegeven. Zoals: 01-10-2022; 13:00; 18
Datalek	Een inbreuk op de beveiliging van Persoonsgegevens, die leidt tot enige ongeoorloofde Verwerking daarvan. Hier vallen zowel opzettelijke als onopzettelijke datalekken onder.	
Data at rest	[Wikipedia] Data die fysiek is ondergebracht op computergegevensopslag in elke digitale vorm (bijvoorbeeld cloudopslag, bestandshostingdiensten, databases, datawarehouses, spreadsheets, archieven, tapes, off-site of cloudback-ups, mobiele apparaten enz.).	
Data in transit	[Wikipedia] Data tijdens transport, ook wel data in beweging [in motion] en data tijdens de vlucht [in flight] genoemd, is data onderweg tussen bron en bestemming, meestal op een computernetwerk.	
Derde	Ieder ander, niet zijnde de Betrokkene, de Verwerkingsverantwoordelijke of de Verwerker, of enig persoon die onder rechtstreeks gezag valt van de Verwerkingsverantwoordelijke of de Verwerker en gemachtigd is om Persoonsgegevens te verwerken.	
Feit	[Wikipedia] Een feit is een gebeurtenis of omstandigheid waarvan de werkelijkheid vaststaat, doordat het ofwel zintuiglijk waargenomen ofwel instrumenteel gemeten kan worden.	18 graden Celsius
Gastheer of -vrouw	Gastheer/-vrouw: de Medewerker/-ster die een Bezoeker/-ster ontvangt [en ervoor verantwoordelijk is dat de Bezoeker op de hoogte is van de huisregels en deze naleeft].	
Gebruiker	Elke Medewerker of student die toegang heeft tot computersystemen of informatie; deze omvatten werknemers, tijdelijke werknemers, aannemers, consultants, tijdelijk personeel, andere werknemers en personen die een studie volgen bij de OU.	
Gegeven	[Wikidepia] Een gegeven is de vastgelegde uitdrukking van een feit. Gegevens zijn de objectief waarneembare neerslag of registratie van feiten op een bepaald medium, zodanig dat deze gegevens uitgewisseld en voor langere tijd bewaard kunnen worden.	Datum: 1 oktober 2022. Tijd: 13:00 Temperatuur: 18 graden
Gegevensbeschermings effectbeoordeling	Zie *Privacy Impact Assessment*.	

Informatie	Gegevens (Data) die in een context (verband) zijn geplaatst en daardoor betekenis en waarde hebben gekregen.	Op 1 oktober 2022 om 13:00 was het 18 graden Celsius.
Informatiesysteem	Een samenhangend geheel van instrumenten, Gegevens en Informatie dat wordt gebruikt om een proces of functie te ondersteunen.	
IT-faciliteiten	Alle apparaten en (web)applicaties waarmee geautoriseerde toegang tot (diensten van) het OU-netwerk kan worden verkregen en/of waarmee data van de instelling wordt verwerkt.	Zie Bedrijfsmiddel.
Kwetsbaarheid	Fout in een digitaal systeem waardoor een aanvaller in het systeem kan komen. De aanvaller kan vervolgens bij informatie of toepassingen in het systeem komen, terwijl hij dat niet mag. Of de aanvaller zorgt ervoor dat de gebruiker niet meer bij deze informatie kan komen. Of de toepassing niet meer kan gebruiken.	
Leverancier	Een derde partij die verantwoordelijk is voor het leveren van vereiste goederen of IT-diensten, zoals hardware- en softwareleveranciers, netwerk- en telecomaanbieders en uitbestedingsorganisaties.	
Licentie	Toestemming om een bepaalde software te mogen gebruiken zonder er de eigendomsrechten over te verkrijgen.	
Logbestand	Een digitaal logboek. Bestand waarin een digitaal systeem automatisch veranderingen en gebeurtenissen bijhoudt.	
Malware	Kwaadaardige software die aanvallers op een digitaal systeem zetten om er op afstand bij te kunnen, het te vernielen of informatie te stelen. Malware is een samentrekking van het Engelse *malicious software*.	Adware, backdoor, virus, worm, keylogger, ransomware, spyware.
Medewerker	[Te hergebruiken uit het privacy beleidsdocument] Degene die een tijdelijk of vast dienstverband heeft bij de OU dan wel degene die anders dan uit dienstbetrekking arbeid verricht voor de OU.	Personen die werk verrichten vanuit dienstverband, als inhuur- of als uitzendkracht.
Microperimeter	Een microperimeter is wat beleidsmatig wordt benoemd rond een *Protect Surface*. Het creëert een controlepunt dat ervoor zorgt dat alleen bekend toegestaan verkeer en legitieme toepassingen toegang hebben tot het te beveiligingen oppervlak.	
Minderjarige	In het kader van de AVG: iedere persoon die de leeftijd van 16 jaar nog niet heeft bereikt.	
Need-to-know	Het principe dat een gebruiker alleen toegang heeft tot de informatie die zijn/haar functie vereist, en niet meer dan dat.	
Netwerk	Systeem waardoor twee of meer computers via kabels of draadloos netwerk met elkaar kunnen communiceren.	
Omgeving [voor het verstrekken van	[ITIL] Een deelverzameling van de IT- infrastructuur die gebruikt wordt voor een specifiek doel.	Intranet, GoodHabitz.

informatie over informatiebeveiliging]		
Patch	Nieuwe versie van software. In deze nieuwe versie heeft de Leverancier kwetsbaarheden in het systeem hersteld. Hij heeft geen nieuwe functies toegevoegd.	
Personeel	Degenen die een dienstverband hebben bij de OU dan wel degenen die - anders dan vanuit dienstbetrekking - arbeid verricht voor de OU.	
Persoonsgegeven	Elk gegeven betreffende een geïdentificeerd of identificeerbaar natuurlijk persoon.	
Persoonsverificatie	Het controleren van de identiteit van een Gebruiker.	
Privacy by Default	Een gegevensverwerking waarbij de standaardinstellingen van producten en diensten zo zijn ingesteld dat de privacy van Betrokkenen maximaal wordt gewaarborgd. Dit betekent onder meer dat er zo min mogelijk gegevens worden gevraagd en verwerkt.	
Privacy by Design	Het beheer van de gehele levenscyclus van Persoonsgegevens, vanaf het verzamelen tot het verwerken en verwijderen, waarbij mechanismen zo zijn ontworpen dat zij zo veel mogelijk rekening houden met de privacy van Betrokkenen. Hierbij wordt stelselmatig aandacht besteed aan allesomvattende waarborgen m.b.t. nauwkeurigheid, vertrouwelijkheid, integriteit, fysieke veiligheid en verwijdering van de Persoonsgegevens.	
Privacy Impact Assessment	Een beoordeling die helpt bij het identificeren van privacy risico's en de handvatten levert om deze risico's te verkleinen tot een acceptabel niveau.	
Product owner	De persoon die verantwoordelijk is voor het creëren van de maximale waarde voor de producten die door het werk van het scrum team tot stand komen.	
Profilering	Elke vorm van geautomatiseerde Verwerking van Persoonsgegevens waarbij aan de hand van Persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd, onder andere met de bedoeling zijn beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen.	
Protect Surface	Een herkenbaar te beschermen element/oppervlak.	ATI, HIP, laptops, O4U, T-schijf.
Risicoprofiel	Overzicht van alle risico's van een organisatie, project, proces of programma. Een risicoprofiel laat zien welke risico's er zijn, inclusief kans van optreden en de gevolgen.	
Ruimte	• Vrij toegankelijk: ruimtes die toegankelijk zijn voor medewerkers en bezoekers. Deze ruimtes bevatten geen permanent aanwezige niet-publieke informatie.	

	• Beperkt toegankelijke ruimtes bevatten:
	  • geen permanent aanwezige niet-publieke informatie of informatiesystemen;
	  • niet-publieke informatie of informatiesystemen waar enkel specifieke gebruikers toegang toe hebben.	

Screening	De integriteit van een persoons onderzoeken en vaststellen op basis van diverse bronnen.	CV-onderzoek, paspoortcontrole, gesprek.
Sleutel	Zie Cryptografische sleutel.	
Tweefactor authenticatie	Methode om vast te stellen of een gebruiker of digitaal systeem wel is wie of wat hij zegt te zijn. Je gebruikt hiervoor verschillende manieren (factoren).	Wachtwoord en SMS en/of Tiqr code.
Update	Aanpassing van een bestaande versie van hard- of software. Deze repareert bekende zwakke plekken, zorgt eventueel voor nieuwe beveiliging en extra functies.	
Verwerker	Een door de OU ingeschakelde (derde) partij die ten behoeve van de OU en op basis van diens schriftelijke instructies, Persoonsgegevens verwerkt.	AFAS, Microsoft, SURF.
Verwerking	Elke handeling of geheel van handelingen met betrekking tot Persoonsgegevens, waaronder het verzamelen, vastleggen, ordenen, opslaan, raadplegen, bijwerken, afschermen, wissen of vernietigen van gegevens.	Bijhouden van cijfers, het opslaan van onderzoeksgegevens, het inzien van een personeelsdossier.
Verwerkingsverantwoordelijke	College van bestuur van de OU die het doel en de middelen van de Verwerking van Persoonsgegevens vaststelt.	
Volwassenheidsniveau	De mate waarin een organisatie controle heeft over haar informatiebeveiliging. In gangbare modellen bestaan 5 niveaus, waarbij niveau 1 staat voor ad hoc werkend en niveau 5 voor een bedrijfsbrede risicogebaseerde aanpak.	De volwassenheidsniveaus zoals toegepast in de sector hoger onderwijs worden onder andere toegelicht op https://www.surf.nl/normenkader-surfaudit-audit-je-informatiebeveiliging
Wachtwoord	Reeks van letters, cijfers en of andere karakters waarmee een gebruiker in een computersysteem kan komen. Het is de bedoeling dat een gebruiker dit wachtwoord niet aan anderen geeft en een sterk wachtwoord kiest zodat dit moeilijk te kraken is door aanvallers.	
Webapplicatie	[NCSC] Een applicatie die bereikbaar is met een webbrowser of een andere client, die ondersteuning biedt voor het Hypertext Transfer Protocol (http).	Het begrip moet breed geïnterpreteerd worden. Internetsites, extranetten, intranetten, software-as-a-service (SaaS)-applicaties, webservices en web-api's zijn voorbeelden van webapplicaties.
Wijziging	De toevoeging, verandering of verwijdering van alles dat een effect kan hebben op IT-diensten. De scope is gericht op alle wijzigingen van alle architecturen,	

	processen, instrumenten, meetwaarden en documentatie, en op wijzigingen van IT-diensten en andere configuratie-items.	
Zero Trust	Model met strenge regels hoe een intern netwerk qua onderling vertrouwen is ingericht. Het uitgangspunt is: vertrouw niets of niemand impliciet en controleer altijd expliciet of een gebruiker of computer wel is wie hij zegt te zijn. Een gebruiker mag alleen in een digitaal systeem alet systeem heeft gecontroleerd wie hij is en waar hij is. Daarnaast is toegang tot data gelimiteerd op een need-to-know basis.	