INFORMATIEBEVEILIGINGSBELEID UNIVERSITEIT TWENTE

LISA

Versie 2.1

12-02-2021

COLOFON

ORGANISATIE
Library, ICT Services & Archive

TITEL
Informatiebeveiligingsbeleid Universiteit Twente

KENMERK
LISA-0322

VERSIE (STATUS)
2.1

DATUM
12-02-2021

AUTEUR(S)
Wim Koolhoven, Jan Evers, Henk Swaters

DOCUMENTHISTORIE

VERSIE	DATUM	AUTEUR(S)	OPMERKINGEN
1.0	27-11-2015	W. Koolhoven	Definitieve eerste versie Vastgesteld in CvB van 07-12-2015
1.1	27-03-2019	J.L. Evers	Actualisatie: update verwijzing AVG, ICTS veranderd in LISA, beschrijving organisatie security mgt geüpdatet
1.2	17-04-2019	J.L. Evers	Opmerkingen verwerkt; URL's vervangen door documentnamen; securityregels aangescherpt: verwijzing e-waste regeling, encryptie waar mogelijk 06-05-2019 MT LISA akkoord
1.3	20-10-2020	H.W. Swaters	URL's naar de cybersafety website in de voettekst. Werkwijze LISA securitymanagement volgens best practice ITIL securitymanagement verwijderd. Rol ISO bij aangifte toegevoegd. Beveiligingsstrategie gebaseerd op het "Zero Trust" model toegevoegd aan richtlijn. Richtlijn authenticatiemiddelen aangescherpt. Minimum beveiligingseisen voor Informatiesystemen en werkplekken toegevoegd. Bijlagen: Security-regels hardware, verantwoordelijkheden verduidelijkt
2.0	01-12-2020	H.W. Swaters	Definitief gemaakt
2.1	12-02-2021	H.W. Swaters	Beleidsprincipe "Eigendom van informatie" verwijderd.

DISTRIBUTIELIJST

VERSIE	DATUM	AUTEUR(S)	GEDISTRIBUEERD AAN
1.1	27-03-2019	J.L. Evers	Security mgrs, IT-auditor, hoofd DSM
1.2	17-04-2019	J.L. Evers	MT LISA dd 06-05-2019 UCB 04-06-2019
1.3	25-10-2020	H.W. Swaters	MT-LISA geaccordeerd en definitief gemaakt
2.0	01-12-2020	H.W. Swaters	CvB ter vaststelling
2.1	12-02-21	H.W. Swaters	CvB ter vaststelling van de wijzigingen t.o.v. 2.0

INHOUDSOPGAVE

Het informatiebeveiligingsbeleid Universiteit Twente is gebaseerd op het Model Informatiebeveiligingsbeleid van het Hoger Onderwijs opgesteld door SURFibo[1] en gepubliceerd onder de Creative Commons[2] licentie.

SAMENVATTING

Beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening zijn van groot belang. Hoe we deze aspecten op de UT borgen wordt vastgesteld in dit beleid. Het belang van informatiebeveiliging blijkt ook uit het jaarlijkse Cyberdreigingsbeeld van SURF.

De UT houdt zich aan de wet en informatie over studenten en medewerkers wordt zo zorgvuldig als mogelijk behandeld. Aandacht hiervoor hoort bij de proactieve houding van iedere medewerker, tegelijkertijd worden er niet meer maatregelen genomen dan noodzakelijk om het ondernemende en creatieve karakter van de UT niet te frustreren.

Informatiebeveiliging is ieders verantwoordelijkheid en een lijnverantwoordelijkheid. Leidinggevenden dragen de primaire verantwoordelijkheid voor een goede informatiebeveiliging op hun afdeling/eenheid. Alle informatiesystemen worden geclassificeerd op de aspecten beschikbaarheid, integriteit en vertrouwelijkheid; deze classificatie bepaalt het niveau van de beveiligingsmaatregelen.

De verantwoordelijkheid van alle betrokken functionarissen wordt beschreven. In het bijzonder van de Informatie Security Officer, Informatie Security Manager, systeemhouders en leidinggevenden. Het belang van het regelmatig onder de aandacht brengen van beveiligingsrisico's en –maatregelen wordt uitgewerkt. De rol van CERT-UT (Computer Emergency Response Team UT) wordt vastgelegd.

Om bewustwording en gedragsbeïnvloeding van medewerkers en studenten met betrekking tot informatiebeveiliging en privacy te bewerkstelligen is er een permanente werkgroep "bewustzijn cybersafety".

In de bijlagen wordt ingegaan op de relevante wetgeving, wordt een overzicht gegeven van de overige beleidsdocumenten en gedragscodes op het gebied van informatiebeveiliging en worden de securityregels (operationele richtlijnen) geformuleerd.

[1] Informatiebeveiligers en privacy officers werkzaam in het hoger onderwijs overleggen in SCIPR (SURF Community voor Informatiebeveiliging en PRivacy, voorheen SURFibo). Het doel is de informatiebeveiliging en privacy bij hogescholen en universiteiten te verbeteren. Dit doet SCIPR o.a. door het ontwikkelen van beleid en leidraden.
[2] zie creativecommons.org/licenses/by/3.0/nl/

1 INLEIDING

Onder informatiebeveiliging wordt verstaan het treffen en onderhouden van een samenhangend pakket aan maatregelen om de beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening te garanderen. Hierbij gaat het ook om de controleerbaarheid van de maatregelen die genomen zijn om deze kwaliteitsaspecten te borgen.

Informatiebeveiliging is een beleidsverantwoordelijkheid van het bestuur van de Universiteit Twente. In de bedrijfsvoering, maar ook in het onderwijs en onderzoek is sprake van toenemende afhankelijkheid van informatie en computersystemen, waar kwetsbaarheden en risico's kunnen optreden. Het is daarom van belang hiertegen adequate maatregelen te nemen. Immers, onvoldoende informatiebeveiliging kan leiden tot onacceptabele risico's bij de uitvoering van onderwijs en onderzoek en bij de bedrijfsvoering van de instelling. Incidenten en inbreuken in deze processen kunnen leiden tot financiële schade en imagoverlies.

De Universiteit Twente heeft de ambitie om met het onderhavige beleidsdocument informatie-beveiliging structureel naar een hoger niveau te brengen en daar te houden door de aspecten governance, wet- en regelgeving, de organisatie van de beveiligingsfunctie en het informatiebeveiligingsbeleid – ook in hun onderlinge relatie – duidelijk te beschrijven en vast te stellen. Privacy krijgt op de UT ook veel aandacht, zeker met de sinds mei 2018 stringentere wetgeving (AVG – Algemene Verordening Gegevensbescherming). Er is daarom een apart UT privacybeleid[3] opgesteld.

1.1 REIKWIJDTE VAN HET BELEID

Bij de Universiteit Twente wordt informatiebeveiliging breed geïnterpreteerd. Er is een nauwe relatie en een gedeeltelijke overlap met aanpalende beleidsterreinen, zoals safety (ARBO- en milieuwetgeving), fysieke beveiliging en bedrijfscontinuïteit. In het kader van "integrale veiligheid" is een goede afstemming tussen deze aanpalende beleidsterreinen nodig.

Het informatiebeveiligingsbeleid binnen de Universiteit Twente heeft betrekking op alle medewerkers, studenten, gasten, bezoekers en externe relaties (inhuur / outsourcing), alsmede op alle organisatie-onderdelen. Tevens vallen onder het informatiebeveiligingsbeleid alle devices waarmee geautoriseerde toegang tot het instellingsnetwerk verkregen kan worden.

Bij het informatiebeveiligingsbeleid ligt de nadruk op de informatie en toepassingen die vallen onder de verantwoordelijkheid van de Universiteit Twente.

1.2 LEESWIJZER

De aparte hoofdstukken in dit beleidsdocument zijn zelfstandig leesbaar. Er worden normen geformuleerd die implementatie behoeven door de betreffende verantwoordelijken. Alle lezers wordt aangeraden in ieder geval uit hoofdstuk 3 Uitgangspunten de paragraaf 3.1 Basisregels en 3.2 Beleidsuitgangspunten door te lezen. In hoofdstuk 4 over Governance wordt expliciet geformuleerd hoe de verantwoordelijkheden op de UT met betrekking tot informatiebeveiliging belegd zijn. De rollen van Informatie Security Officer, Informatie Security Manager en CERT-UT (Computer Emergency Respons Team) worden hier vastgelegd.

In de bijlagen wordt ingegaan op de relevante wetgeving en UT beleidsdocumenten en worden de securityregels (operationele richtlijnen) geformuleerd. Voor de evaluatie en bijstelling van de securityregels zijn betreffende ICT-medewerkers intensief betrokken. Door deze securityregels op te nemen als bijlage is de relatie tussen de securityregels en het beleid helder. De securityregels zijn zo geformuleerd dat ze ook begrijpelijk zijn voor niet-technici. ICT-medewerkers die alleen geïnteresseerd zijn in de consequenties voor hun eigen werk kunnen volstaan met het lezen van de betreffende securityregels.

[3] https://www.utwente.nl/nl/cyber-safety/cybersafety/wetgeving/

2 DOELSTELLING INFORMATIEBEVEILIGINGSBELEID

Het informatiebeveiligingsbeleid bij de UT heeft als doel het waarborgen van de continuïteit van bedrijfsvoering, onderwijs en onderzoek en het minimaliseren van de schade door het voorkomen van beveiligingsincidenten en het minimaliseren van eventuele gevolgen.

De doelen van het informatiebeveiligingsbeleid voor de UT zijn meer specifiek de volgende:

- *Kader*: het beleid biedt een kader om (toekomstige) maatregelen in de informatiebeveiliging te toetsen aan een vastgestelde best practice of norm en om de taken, bevoegdheden en verantwoordelijkheden in de organisatie te beleggen.
- *Normen*: de basis voor de inrichting van het security management is ISO 27001.[4] Maatregelen worden genomen op basis van best practices in het hoger onderwijs en op basis van ISO 27002[5]. Daarnaast wordt ISO 27017[6] gehanteerd als basis voor de informatiebeveiligingsaspecten van clouddiensten.
- *Expliciet*: uitgangspunten en organisatie van informatiebeveiligingsfuncties zijn vastgelegd en worden gedragen door het College van Bestuur, en afgeleid daarvan, door de hele organisatie.
- *Daadkrachtig*: basis voor duidelijke keuzes in maatregelen, actieve controle op beleidsregels en de uitvoering daarvan.
- *Compliance*: het beleid biedt de basis om te voldoen aan wettelijke voorschriften.

[4] Voluit: NEN-ISO/IEC 27001: Eisen aan Managementsystemen voor informatiebeveiliging
[5] Voluit: NEN-ISO/IEC 27002: Praktijkrichtlijn met beheersmaatregelen voor informatiebeveiliging
[6] Voluit: NEN-ISO/IEC 27017: Informatiebeveiliging voor clouddiensten

3 UITGANGSPUNTEN INFORMATIEBEVEILIGING

3.1 BASISREGELS

Algemene strategiedocumenten van de UT geven op zichzelf onvoldoende aanknopingspunten om een Informatiebeveiligingsbeleid op te baseren, oftewel om een bij de UT passende risicoacceptatie te formuleren. Om te voorkomen dat het beleid onvoldoende gekend en gedragen wordt door de organisatie is het belangrijk expliciet te formuleren wat we echt belangrijk vinden.

1. *De UT houdt zich, als publiekrechtelijke organisatie, aan de wet.* Ook als ondernemende universiteit gaat de UT niet mee in de redenering dat de keuze om je als organisatie aan de wet te houden een kosten-baten analyse hoort te zijn. Anderzijds is de universiteit natuurlijk ook geen politieagent.
2. *Informatie over studenten en medewerkers wordt zo zorgvuldig als mogelijk behandeld.* Medewerkers en studenten moeten er op kunnen vertrouwen dat er zo zorgvuldig als mogelijk met hun informatie wordt omgegaan. Zorgvuldig met privacy omgaan is een van de uitdagingen waar we als universiteit voor staan.
3. *Aandacht besteden aan informatiebeveiliging binnen alle processen en activiteiten hoort bij de proactieve houding van de UT-medewerker.* Informatiebeveiliging heeft veel aspecten en raakt aan bijna alle processen en activiteiten. Risico nemen hoort bij de ondernemende houding van de UT. Onderdeel hiervan is vooraf de mogelijke gevolgen te onderzoeken en maatregelen te nemen die onaanvaardbare risico's beperken.
4. *Het ondernemende en creatieve karakter van de UT wordt niet gefrustreerd door het informatiebeveiligingsbeleid.* Noodzakelijke beveiligingsmaatregelen moeten natuurlijk genomen worden, ook als individuen dit minder waarderen, maar dan wel na een afweging. Proportionaliteit is hierbij gewenst. Ingrijpende of beperkende maatregelen die niet in verhouding staan tot het feitelijk verminderen van risico's worden niet genomen.

3.2 BELEIDSUITGANGSPUNTEN

Security management wordt als proces ingericht. Dat houdt in dat de jaarlijkse planning en controlecyclus, gebaseerd is op ISO 27001 (Plan, Do, Check, Act). Hierin worden jaarplannen opgesteld en uitgevoerd. De resultaten ervan worden geëvalueerd en vertaald naar nieuwe jaarplannen.

De beveiliging dient de volgende aspecten van de informatievoorziening te waarborgen:

- **B**eschikbaarheid: de mate waarin gegevens of functionaliteit op de juiste momenten en locaties beschikbaar zijn voor gebruikers;
- **I**ntegriteit: de mate waarin gegevens of functionaliteit juist ingevuld zijn;
- **V**ertrouwelijkheid: de mate waarin de toegang tot gegevens of functionaliteit beperkt is tot degenen die daartoe bevoegd zijn.

De Universiteit Twente hanteert de volgende beleidsprincipes:

- Informatiebeveiliging is **ieders verantwoordelijkheid**. Communiceer met medewerkers, studenten, docenten en derden dat er van hen verwacht wordt dat ze actief bijdragen aan de veiligheid van geautomatiseerde systemen en de daarin opgeslagen informatie. Dat kan bijvoorbeeld in de aanstellingsbrief, tijdens functioneringsgesprekken, met een instellingsbrede gedragscode, met periodieke bewustwordingscampagnes, et cetera.
- Informatiebeveiliging is een **lijnverantwoordelijkheid**. Dit betekent dat de leidinggevenden de primaire verantwoordelijkheid dragen voor een goede informatiebeveiliging op hun afdeling / eenheid. Dit omvat ook de keuze van maatregelen en de uitvoering en handhaving ervan.
- Informatiebeveiliging is een **continu proces**. Regelmatige herijking van beleid en audits, technologische en organisatorische ontwikkelingen binnen en buiten de instelling maken het noodzakelijk om periodiek te bezien of de UT nog wel op de juiste wijze bezig is de beveiliging te waarborgen. De audits maken het mogelijk het beleid en de genomen maatregelen te controleren op efficiency en effectiviteit (**controleerbaarheid**).

- **Waardering van informatie**. Iedereen behoort de waarde van informatie te kennen en daarnaar te handelen. Deze waarde wordt bepaald door de mogelijke schade als gevolg van verlies van beschikbaarheid, integriteit of vertrouwelijkheid. Classificatie kan hierbij behulpzaam zijn, zie de volgende paragraaf.

3.3 CLASSIFICATIE

Voor het goed functioneren van de Universiteit Twente is het omgaan met informatie van groot belang. Studenten en medewerkers moeten er op kunnen vertrouwen dat informatie toegankelijk is wanneer en waar die nodig is, correct en volledig is en alleen beschikbaar is voor daartoe geautoriseerde personen.

Niet alle informatie is vertrouwelijk. Het is niet gebruiksvriendelijk om niet vertrouwelijke informatie net zo streng te beschermen als hoog vertrouwelijke informatie. Proportionaliteit, ook omwille van efficiënt gebruik van de beschikbare financiële middelen, is hierbij gewenst. Het ligt voor de hand om onderscheid in bescherming aan te brengen. Classificatie van informatie is hiervoor het hulpmiddel.

Bij de Universiteit Twente zijn alle gegevens, waarop dit informatiebeveiligingsbeleid van toepassing is, geclassificeerd op de kwaliteitsaspecten *Beschikbaarheid*, *Integriteit* en *Vertrouwelijkheid*.

Welk niveau van beveiligingsmaatregelen geschikt is voor een bepaald informatiesysteem hangt af van de classificatie van de informatie die het systeem verwerkt. Voor de classificatie wordt per kwaliteitsaspect de driepuntschaal *Standaard*, *Gevoelig*, *Kritiek* gebruikt.

De classificatie dient door of namens de eigenaar van de betreffende informatie of van het betreffende informatiesysteem te worden bepaald. Voor de instellingssystemen van de UT zijn door het College van Bestuur houders (directeuren van diensten) aangewezen die de rol van eigenaar vervullen. Voor de beschrijving en uitwerking van de beveiligingsniveaus wordt verwezen naar de *Classificatierichtlijn Informatie en Informatiesystemen Universiteit Twente*[7], waarin tevens de classificatiemethodiek is geformuleerd.

[7] https://www.utwente.nl/nl/cyber-safety/cybersafety/wetgeving/

4 GOVERNANCE INFORMATIEBEVEILIGINGSBELEID

Het goed, efficiënt en verantwoord leiden van een organisatie wordt vaak aangeduid met de term *governance*. Het omvat vooral ook de relatie met de belangrijkste belanghebbenden van de instelling, zoals de studenten, medewerkers en de samenleving als geheel. Een goede *governance* zorgt er voor dat alle belanghebbenden hun rechten en plichten kennen en er naar handelen.

4.1 AFSTEMMING MET AANPALENDE BELEIDSTERREINEN

Onderdeel van governance is dat aan alle soorten risico's en hun onderlinge verwevenheid passende aandacht geschonken wordt, dit wordt Integrale Veiligheid genoemd. Fysieke beveiliging, Arbo- en milieuveiligheid blijven hier verder buiten beschouwing.

De problematiek rond privacy, het zorgvuldig verwerken van persoonsgegevens, is onderdeel van informatiebeveiliging. Tegelijkertijd heeft het zoveel specifieke elementen dat hier apart privacybeleid voor is opgesteld.

Bedrijfscontinuïteit valt deels binnen het domein van informatiebeveiliging, maar is primair een lijnverantwoordelijkheid. Eenheden dienen bedrijfscontinuïteitsplannen op te stellen voor de bedrijfsprocessen waar ze verantwoordelijk voor zijn.

4.2 DOCUMENTEN

Een niet compleet overzicht van beschikbare beleidsdocumenten op het gebied van informatiebeveiliging is opgenomen in Bijlage B. Alle beleidsdocumenten worden na vaststelling gepubliceerd op de Cybersafety website.[8]

Om de noodzakelijke beveiligingseisen en –procedures vast te kunnen leggen zijn op deelgebieden specifieke securityregels noodzakelijk als uitwerking van het informatiebeveiligingsbeleid. Een opsomming van de Securityregels is opgenomen in Bijlage C.

Algemene voorlichting over informatiebeveiliging wordt door LISA verzorgd. Specifieke werkinstructies worden in de lijn aan medewerkers verstrekt.

In alle overeenkomsten met dienstverleners is een paragraaf over informatiebeveiliging opgenomen.

4.3 ORGANISATIE VAN DE INFORMATIEBEVEILIGINGSFUNCTIE

Om informatiebeveiliging gestructureerd en gecoördineerd op te pakken worden bij de Universiteit Twente een aantal rollen onderkend die aan functionarissen binnen de UT zijn toegewezen.

4.3.1 COLLEGE VAN BESTUUR

Het College van Bestuur is eindverantwoordelijk voor de informatiebeveiliging binnen de Universiteit Twente en stelt het beleid en de basismaatregelen op het gebied van informatiebeveiliging vast. De inhoudelijke verantwoordelijkheid voor informatiebeveiliging is gemandateerd aan de Information Security Officer. Deze heeft de opdracht om voor de informatiebeveiliging voor de gehele instelling zorg te dragen.

4.3.2 PORTEFEUILLEHOUDER INFORMATIEBEVEILIGING

De portefeuillehouder informatiebeveiliging is het Collegelid dat bedrijfsvoering in portefeuille heeft en daarmee eindverantwoordelijk is voor informatiebeveiliging binnen de Universiteit Twente.

[8] www.utwente.nl/cybersafety

4.3.3 INFORMATION SECURITY OFFICER

De Information Security Officer (ISO) is een rol op strategisch en tactisch niveau. De ISO heeft een zelfstandige en onafhankelijke advies en informatie bevoegdheid naar het CvB en de directeur LISA. De Information Security Officer formuleert het informatiebeveiligingsbeleid, helpt bij een juiste vertaling daarvan naar instellingsonderdelen, ziet toe op de (uniforme) naleving ervan en rapporteert over lacunes, inconsistenties en onvolkomenheden.

4.3.4 INFORMATION SECURITY MANAGER

De Information Security Manager (ook wel IT Security Manager) vervult een rol bij de vertaling van de strategie naar tactische (en operationele) plannen. Dit doet hij in overleg met de Information Security Officer. Hij coördineert het CERT (Computer Emergency Response Team) van de UT. Tevens adviseert hij over specifieke informatiebeveiligingsmaatregelen in projecten – variërend van allerhande staande projecten tot acquisities van bijvoorbeeld software of hardware. Op operationeel niveau wordt overlegd met LISA-medewerkers en met functioneel beheerders, onder andere over de implementatie van de informatiebeveiligingsmaatregelen. Ieder kwartaal stelt de Information Security Manager een managementrapportage op.

4.3.5 SYSTEEMHOUDER

De systeemhouder[9] is er verantwoordelijk voor dat de applicatie een goede ondersteuning biedt aan de bedrijfsprocessen waarvoor de systeemhouder verantwoordelijk is. Dit betekent dat de systeemhouder er voor zorgt dat zowel nu als in de toekomst de applicatie blijft beantwoorden aan de eisen en wensen van de gebruikers, aan wet- en regelgeving en aan het informatiebeveiligingsbeleid. De beveiliging van informatiesystemen zijn een integraal onderdeel van verantwoord beheer van het betreffende informatiesysteem.

De systeemhouder kan hierin ondersteund worden door de security organisatie binnen LISA.

4.3.6 LEIDINGGEVENDE

Naleving van het informatiebeveiligingsbeleid is onderdeel van de integrale bedrijfsvoering. Iedere leidinggevende heeft de taak om:

- er voor te zorgen dat zijn medewerkers op de hoogte zijn van (de voor hen relevante aspecten van) het beveiligingsbeleid;
- toe te zien op de naleving van het beveiligingsbeleid door zijn medewerkers;
- regelmatig het onderwerp informatiebeveiliging onder de aandacht te brengen in werkoverleggen;
- als aanspreekpunt beschikbaar te zijn voor alle personeel gerelateerde informatiebeveiligingszaken.

De leidinggevende kan hierin ondersteund worden door de security organisatie binnen LISA.

4.3.7 INTERNE IT-AUDITOR

De interne IT-auditor controleert jaarlijks conform een vooraf opgesteld IT-Auditjaarplan de IT-beheersmaatregelen van de IT organisatie.

4.3.8 FUNCTIONARIS GEGEVENSBESCHERMING

De functionaris voor de gegevensbescherming (FG) houdt binnen de Universiteit Twente toezicht op de toepassing en naleving van de privacywetgeving (AVG – Algemene Verordening Gegevensbescherming). De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie in de organisatie.

[9] zie verder de notitie “Houderschap van een instellingssysteem”, kenmerk SB/UIM/15/2801/EVS

4.4 OVERLEG

Om de samenhang in de organisatie van de informatiebeveiligingsfunctie goed tot uitdrukking te laten komen en de initiatieven en activiteiten op het gebied van informatiebeveiliging binnen de verschillende onderdelen op elkaar af te stemmen wordt op diverse niveaus gestructureerd overleg gevoerd over informatiebeveiliging.

Op **strategisch** niveau wordt richtinggevend gesproken over *governance* en *compliance*, alsmede over doelen, scope en ambitie op het gebied van informatiebeveiliging. Dit gebeurt in het bestuur, geadviseerd door de Information Security Officer.

Op **tactisch** niveau wordt de strategie vertaald naar plannen, te hanteren normen, evaluatiemethoden, e.d. Deze plannen en instrumenten zijn sturend voor de uitvoering. Dit tactisch overleg wordt uitgevoerd door de Information Security Officer, Information Security Managers en overige betrokkenen.

4.5 NALEVING EN BEWUSTWORDING

De naleving is geborgd met algemeen toezicht op de dagelijkse praktijk van het security management proces. Van belang hierbij is dat leidinggevenden hun verantwoordelijkheid nemen en hun medewerkers aanspreken in geval van tekortkomingen.

De Information Security Officer monitort in hoeverre de organisatie het informatiebeveiligingsbeleid heeft geïmplementeerd. Het Normenkader SURFaudit[10] wordt gebruikt als uitgangspunt voor interne en externe controles. Voor bepaalde onderdelen van het informatielandschap kan besloten worden om tot certificering over te gaan.

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van informatiebeveiliging uit te sluiten. In de praktijk blijkt de mens meestal de belangrijkste risicofactor. Daarom worden beveiligingsrisico's en –maatregelen regelmatig onder de aandacht gebracht, zodat kennis van risico's wordt verhoogd en het (veilig en verantwoord) gedrag wordt aangemoedigd. Onderdeel van de uitvoering van het informatiebeveiligingsbeleid zijn regelmatig terugkerende bewustwordingscampagnes voor medewerkers, studenten en derden. Zulke campagnes kunnen aansluiten bij landelijke campagnes in het hoger onderwijs, zo mogelijk in afstemming met beveiligingscampagnes voor Arbo, milieu en fysiek.

Verhoging van het beveiligingsbewustzijn is zowel een verantwoordelijkheid van de leidinggevenden alsook van de security organisatie binnen LISA.

Om bewustwording en veilig gedrag van medewerkers en studenten met betrekking tot informatiebeveiliging en privacy te bewerkstelligen is er een permanente werkgroep "bewustzijn cybersafety" ingesteld. De werkgroep heeft in ieder geval de volgende leden:

- Information Security Officer (LISA)
- Information Security Manager (LISA)
- Beleidsmedewerker HR (HR)
- Communicatiemedewerker (M&C)

[10] Het normenkader van SURFaudit is gebaseerd op ISO 27002.

5 MELDING EN AFHANDELING VAN INCIDENTEN

Incidentbeheer en –registratie hebben betrekking op de wijze waarop geconstateerde dan wel vermoede inbreuken op de informatiebeveiliging door de medewerkers en studenten gemeld worden en de wijze waarop deze worden afgehandeld.

Het is van belang om te leren van incidenten. Incidentregistratie en periodieke rapportage over opgetreden incidenten horen thuis in een volwassen informatiebeveiligingsomgeving. Bij de Universiteit Twente is er daarom een meldpunt ingericht en is bekend gemaakt hoe dat is te benaderen: CERT-UT, het Computer Emergency Response Team UT.

Elke eenheid is zelf verantwoordelijk voor het signaleren en melden van incidenten en inbreuken op informatiebeveiliging. De lijnmanager, medewerker of student dient de incidenten en inbreuken direct te melden aan cert@utwente.nl of via de centrale LISA servicedesk.

Er is een, door het CvB vastgesteld, responsible disclosure beleid. Daarmee geeft de UT mogelijke melders van veiligheidsgaten in onze informatiesystemen een garantie dat de UT, onder voorwaarden, geen juridische stappen tegen hen zal ondernemen.

De incidenten worden afgehandeld en worden in het relevante operationeel overleg besproken – en als bedrijfsproces, financiën of goede naam in gevaar zijn, ook in het CvB. Bij constatering van verontrustende trends kan hierop meteen worden ingespeeld, bijvoorbeeld door het nemen van extra maatregelen of een bewustwordingscampagne.

Het doel van CERT-UT is het zo mogelijk voorkomen van informatiebeveiligingsincidenten en deze te bestrijden zodra ze zich voordoen en daarmee de continuïteit van de Universiteit Twente te ondersteunen en haar reputatie te beschermen. CERT-UT houdt zich ook bezig met beveiligingsincidenten buiten de Universiteit Twente als daar eigen medewerkers of studenten in enige rol bij betrokken zijn. In zulke gevallen wordt gebruik gemaakt van de diensten van SURFcert, die wereldwijd in verbinding staat met andere Computer Security Incident Response Teams (CSIRTs).

De leden van CERT-UT zijn benoemd door de directeur LISA en opereren in diens opdracht. CERT-UT kan in geval van ernstige incidenten via de directeur LISA escaleren naar de portefeuillehouder informatiebeveiliging. CERT-UT wordt geleid door de Information Security Manager.

CERT-UT is gerechtigd het tijdelijk isoleren van systeem/netwerkgebruikers, computersystemen of netwerksegmenten te gelasten ten einde haar taak uit te kunnen voeren.

In de specifieke securityregels voor Security Incident- en Eventmanagement wordt een en ander verder uitgewerkt.

6 VASTSTELLING EN WIJZIGING

Dit beleid is vastgesteld door het CvB van de Universiteit Twente op 1 maart 2021. Dit beleid wordt na twee jaar op initiatief van de Information Security Manager geëvalueerd, waarbij ook een controle op de effectiviteit van de maatregelen wordt uitgevoerd.

Voor vragen of opmerkingen met betrekking tot dit beleid kunt u terecht bij de Information Security Officer.

Bijlage A Wetgeving

Bij de Universiteit Twente wordt op de volgende wijze omgegaan met relevante wet- en regelgeving. Deze lijst is niet uitputtend.

i. Wet op het Hoger onderwijs en Wetenschappelijk onderzoek

De Universiteit Twente heeft een kwaliteitszorgsysteem, waarin (onder meer) het zorgvuldig omgaan met gegevens in de studentenadministratie en met de studieresultaten is gewaarborgd. Daarnaast worden integriteitscodes voor wetenschappelijk onderzoek nageleefd en toegepast.

ii. Algemene Verordening Gegevensbescherming (AVG)

De Universiteit Twente heeft de wettelijke privacy vereisten (juistheid en nauwkeurigheid van gegevens en passende technische en organisatorische maatregelen tegen verlies en onrechtmatige verwerking) beleidsmatig vastgelegd in een apart Privacybeleid.

iii. Archiefwet

De Universiteit Twente houdt zich aan de voorschriften ten aanzien van bewaartermijnen, zoals die bijvoorbeeld in de Archiefwet zijn vastgelegd, en het Archiefbesluit over de wijze waarop omgegaan moet worden met informatie vastgelegd in (gedigitaliseerde) documenten, informatiesystemen, websites, e.d. Dit is periodiek onderdeel van de externe accountantsrapportages.

iv. Auteurswet

De Universiteit Twente verspreidt geen originele werken zonder dat daarvoor toestemming is verkregen van de eigenaar van de auteursrechten. Dit impliceert ook dat de Universiteit Twente het gebruik van software zonder het bezitten van de juiste licenties tegen gaat.

De bibliotheek geeft op haar website praktische informatie over hoe met auteursrecht om te gaan. LISA beheert de software licenties.[11]

v. Telecommunicatiewet

De Universiteit Twente kent geen openbaar deel van het netwerk. Het UT-net is beschikbaar voor een gesloten groep van betrokkenen bij onderwijs en onderzoek en geeft toegang tot daarvoor relevante services. Daarom is de meeste regelgeving uit de Telecommunicatiewet niet van toepassing. De regelgeving omtrent netneutraliteit is van toepassing voor zover het de studentenhuisvesting betreft.

vi. Wet op de inlichtingen- en veiligheidsdiensten

Het parlement heeft in 2018 een wijzigingsvoorstel op de Wiv aangenomen. Diensten als AIVD en MIVD krijgen hiermee het recht om dataverkeer van het Internet af te tappen. De consequenties voor de UT zullen, bij voorkeur in SURF verband, uitgezocht moeten worden.

vii. Wet Computercriminaliteit III

In 2019 is de derde versie van de Wet Computercriminaliteit in werking getreden. De wet richt zich op de strafrechtelijke probleemgebieden in relatie tot het computergebruik. Het stelt een aantal zaken explicieter strafbaar. De derde versie betreft voornamelijk wijzigingen in de rechten, en bijbehorende plichten, van opsporingsdiensten, zoals de politie. Zo biedt de nieuwe versie hen de mogelijkheid om, in bepaalde gevallen, de criminelen terug te hacken.

[11] Zie *Software licenties en de UT*, kenmerk SB/UIM/12/0601/khv

Daarnaast is de heling van computergegevens nu als zelfstandig delict strafbaar. Daarmee kan iemand worden aangepakt die over gegevens van anderen beschikt, ook als niet bewezen kan worden dat hij zelf die gegevens heeft overgenomen.

Het naleven van dit informatiebeveiligingsbeleid en het implementeren van de securityregels zorgen ervoor dat de UT een basisniveau van beveiliging heeft. Indien er aanvallen op de UT plaatsvinden die die beveiliging significant doorbreken en die vallen onder de Wet Computercriminaliteit, zal de UT in beginsel aangifte doen. Aangifte wordt door de Information Security Manager gedaan. Zo mogelijk in overleg met Information Security Officer en directeur LISA. De portefeuillehouder informatiebeveiliging wordt van een aangifte in kennis gesteld. Zowel de directeur als de portefeuillehouder worden van de voortgang op de hoogte gehouden.

Bijlage B Beleidsdocumenten

Naast het Informatiebeveiligingsbeleid zijn een aantal beleidsdocumenten en gedragscodes op het gebied van informatiebeveiliging geformuleerd. Alle beleidsdocumenten worden na vaststelling gepubliceerd op de website van Cybersafety.[12]

Een selectie uit deze documenten:

1. *Classificatierichtlijn Informatie en Informatiesystemen Universiteit Twente*. Classificatie van informatie geeft een inschatting van de gevoeligheid en het belang van de informatie en de daarbij horende graad van beveiliging. Het gaat daarbij om de juiste mate van beveiliging, één die past bij de risico's die de informatie loopt.
2. *Digitale gedragscode voor medewerkers Universiteit Twente* en *Digitale gedragscode voor studenten Universiteit Twente*. De gedragscodes geven de wijze aan waarop bij de Universiteit Twente wordt omgegaan met ICT- en internetgebruik. De codes regelen het verantwoord gebruik van ICT-voorzieningen en internet en de wijze waarop controle op het gebruik plaatsvindt.
3. *Gedragscode ICT-functionarissen Universiteit Twente*. Vanuit hun functie hebben ICT-functionarissen vaak verregaande bevoegdheden binnen informatieverwerkende systemen. Door de tools die hen ter beschikking staan kunnen zij vaak op eenvoudige wijze privacygevoelige informatie verzamelen.
4. *Wachtwoordbeleid Universiteit Twente*. Bij de opstelling van de Beleidsregels Identitymanagement Universiteit Twente is ervoor gekozen om een apart wachtwoordbeleid op te stellen waarin alle aspecten opnieuw worden afgewogen en uitgewerkt. De verschillende inzichten worden in dit document belicht.

[12] www.utwente.nl/cybersafety

Bijlage C Securityregels

Om de noodzakelijke beveiligingseisen en –procedures vast te kunnen leggen zijn op deelgebieden specifieke securityregels noodzakelijk. Door het formeel vaststellen van deze securityregels wordt de implementatie toetsbaar. LISA-medewerkers kunnen zich over het algemeen beperken tot de voor hun relevante securityregels.

De beveiligingsstrategie is gebaseerd op het “Zero Trust” model. Het uitgangspunt hiervan is dat alle resources zich op het openbare internet bevinden en apparaten, gebruikers en netwerken nooit zomaar vertrouwd mogen worden. Het basisprincipe van Zero Trust luidt dan ook ‘vertrouw nooit, controleer altijd

Voor de volgende deelgebieden zijn specifieke securityregels vastgesteld:

1. Authenticatiemiddelen, beheer en gebruik van wachtwoorden, software- en/of hardwaresleutels.
2. Basis ICT-voorzieningen, zoals email, dataopslag, telefonie en chat.
3. Datacentra met de daarin opgestelde servers.
4. Hardware, de gehele levenscyclus van aanschaf tot uitfasering.
5. Informatiesystemen, de gehele levenscyclus van verwerving tot uitfasering.
6. Netwerk, inclusief de actieve netwerkcomponenten zoals routers, switches, hubs, access-points etc.
7. Security Incident- en Eventmanagement, werkwijze CERT-UT en afhandeling van beveiligingsincidenten.
8. Werkplekken van gebruikers.

Securityregels – Authenticatiemiddelen

Inleiding

In het Informatiebeveiligingsbeleid wordt aangegeven dat er op deelgebieden specifieke securityregels noodzakelijk zijn. Een van deze deelgebieden betreft het beheer en gebruik van authenticatiemiddelen. Om toegang te krijgen tot het gebruik van bepaalde ICT-voorzieningen wordt voor de authenticatie naast de gebruikersnaam gebruik gemaakt van een wachtwoord, software- en/of hardwaresleutel.

In de *Digitale gedragscode voor medewerkers*[13], Beleidsregels Identitymanagement, Wachtwoordbeleid en het Autorisatiebeleid worden aanverwante relevante uitspraken gedaan, deze worden hier niet herhaald.

Verantwoordelijkheid

1. LISA is verantwoordelijk voor de authenticatiemiddelen.
2. Voor alle soorten authenticatiemiddelen bestaat er een auditbare procedure voor uitgifte, gebruik, vervanging, inname en verlies.

Doelbinding

3. Authenticatiemiddelen zijn persoonsgebonden, apparaatgebonden of applicatiegebonden.
4. Persoonsgebonden authenticatiemiddelen zijn persoonlijk en niet overdraagbaar.
5. Voor alle apparaatgebonden en applicatiegebonden authenticatiemiddelen is steeds minimaal één persoon verantwoordelijk. Hij beheert het betreffende middel en ziet toe op het gebruik. LISA registreert wie voor welk authenticatiemiddel verantwoordelijk is.

Wachtwoorden

6. Voor persoonsgebonden wachtwoorden is een zekere mate van complexiteit noodzakelijk. De Information Security Officer evalueert de richtlijn periodiek en stelt de richtlijn vast. LISA publiceert een richtlijn die deze eis verder uitwerkt en draagt zorg voor de toepassing hiervan.
7. Apparaatgebonden en applicatiegebonden wachtwoorden zijn zeer complex en hebben een hoge entropie. LISA publiceert een richtlijn die deze eis verder uitwerkt en draagt zorg voor de toepassing hiervan.
8. Default wachtwoorden zoals ingesteld door de leverancier dienen te worden aangepast voordat het apparaat op het netwerk wordt aangesloten.

Aanvullende authenticatie middelen

9. Information Security Officer evalueert de beleidsregels voor aanvullende authenticatiemiddlen, zoals MFA, periodiek en stelt deze vast. LISA draagt zorg voor de toepassing hiervan.

[13] zie voor de genoemde documenten de Cybersafety website www.utwente.nl/cybersafety

Securityregels – Basis ICT-voorzieningen

Inleiding

In het Informatiebeveiligingsbeleid wordt aangegeven dat er op deelgebieden specifieke securityregels noodzakelijk zijn. Een van deze deelgebieden betreft de basis ICT-voorzieningen zoals email, dataopslag, telefonie en chat. Deze regels worden in dit document vastgelegd.

Verantwoordelijkheid

1. Voor de centraal aangeboden basis ICT-voorzieningen is LISA houder en verantwoordelijk voor naleving van de securityregels.
2. Voor het veilig gebruik van ICT-voorzieningen geeft LISA voorlichting op de website.

Uitgifte

3. Bij uitgifte van een account wordt de gebruiker meteen geïnformeerd over security, o.a. door te wijzen op de *Digitale gedragscode voor medewerkers*

Data

4. Toegang tot data, inclusief berichten, configuratie en metadata, van een gebruiker mag alleen met toestemming van de betreffende gebruiker of in schriftelijke opdracht van het CvB, zoals vastgelegd in de Gedragscode. In alle gevallen wordt deze toegang geregistreerd.
5. Alle transport van data voldoet qua versleuteling aan de maatregelen uit de *Classificatierichtlijn Informatie en Informatiesystemen*.

Mail

6. Van alle mail die door de UT wordt verstuurd, dient de persoon of applicatie die de mail heeft verstuurd achterhaalbaar te zijn.
7. In- en uitgaande mail wordt gecontroleerd op malware en spam, zo nodig wordt de mail geheel of gedeeltelijk verwijderd of apart gezet.
8. Het aantal geadresseerden en de grootte van mails zijn aan een redelijke bovengrens gebonden. De details worden door LISA op de website gepubliceerd.

Securityregels – Datacentra

Inleiding

In het Informatiebeveiligingsbeleid wordt aangegeven dat er op deelgebieden specifieke securityregels noodzakelijk zijn. Een van deze deelgebieden betreft de datacentra met de daarin opgestelde servers. Deze regels worden in dit document vastgelegd.

Verantwoordelijkheid

1. LISA is verantwoordelijk voor de datacentra, inclusief noodstroom, koeling, etc.
2. LISA maakt sluitende afspraken met leveranciers, zoals CFM en SURFnet.
3. LISA is verantwoordelijk voor de eigen servers in de datacentra en maakt sluitende afspraken met de eigenaren van de overige servers.

Toegang

4. Toegang tot de datacentra is alleen toegestaan voor het plaatsen, onderhouden, vervangen of verwijderen van hardware en voor onderhoud van de datacentra faciliteit zelf.
5. LISA stelt nadere richtlijnen op voor de toegang tot de datacentra overeenkomstig het *Autorisatiebeleid*.
6. Alle toegang tot de datacentra wordt geregistreerd.

Servers

7. LISA houdt een registratie bij van alle geplaatste servers, van iedere server is het doel, een beheerder en een plaatsvervanger geregistreerd. Een registratienummer is goed leesbaar aangebracht op de server.
8. Processen en poorten die niet noodzakelijk zijn voor het gebruik van de server zijn uitgeschakeld.
9. Een server die het UT-net of andere ICT-diensten verstoort of anderszins een securityissue veroorzaakt, wordt op last van CERT-UT uitgeschakeld of geïsoleerd.

Beheer

10. Technisch beheer van applicaties en servers vindt plaats via een netwerk dat logisch gescheiden is van het netwerk voor gebruikers.
11. Voor het beheer wordt gebruik gemaakt van aparte persoonsgebonden beheeraccounts.
12. Gebruik van beheeraccounts wordt gelogd.
13. Beheer van beheeraccounts volgt het Autorisatiebeleid.

Securityregels – Hardware

Inleiding

In het Informatiebeveiligingsbeleid wordt aangegeven dat er op deelgebieden specifieke securityregels noodzakelijk zijn. Een van deze deelgebieden betreft de levenscyclus van hardware, van aanschaf tot uitfasering. Deze regels worden in dit document vastgelegd.

Verantwoordelijkheid

1. LISA is eindverantwoordelijk voor naleving van de securityregels.
2. Wanneer een informatiesysteem op infrastructuur van LISA draait of als LISA het technisch beheer voert, dan is LISA verantwoordelijk voor naleving van de securityregels.
3. Wanneer de houder of eigenaar van een systeem het technisch beheer voert, dan is de houder of eigenaar verantwoordelijk voor naleving van de securityregels.

Aanschaf

4. Voor alle hardware die met het UT-netwerk verbonden kan worden is een zekere mate van beveiliging noodzakelijk. De Informatie Security Manager beheert deze minimumvereisten en publiceert deze op de LISA-website.
5. Wanneer veel of belangrijke hardware wordt aangeschaft dan wordt de Informatie Security Manager tijdig betrokken bij het inkooptraject.

Beheer

6. Default wachtwoorden zoals ingesteld door de leverancier dienen te worden aangepast voordat apparatuur op het netwerk wordt aangesloten.
7. Bij incidenten dient de verantwoordelijke aanspreekbaar te zijn. Daartoe registreert LISA alle hardware die met het UT-netwerk wordt verbonden, c.q. logt het account waarmee toegang verkregen wordt tot het UT-netwerk.
8. Als een firmware-update een securityissue oplost dan moet deze binnen redelijke termijn uitgevoerd worden.

Uitfasering

9. Bij buitengebruikstelling en afvoer van datadragers, zoals harde schijven, tapes, mobiele devices, USB-sticks etc., dienen de gegevens door of namens de eigenaar adequaat vernietigd te worden. LISA geeft via de website per soort datadrager voorlichting over de wijze waarop dit mogelijk is.
10. Uitfasering van overcomplete elektronische persoonlijke apparatuur gaat volgens de e-waste regeling van de UT (*Regeling overcomplete electronische persoonlijke apparatuur*).

Securityregels – Informatiesystemen

Inleiding

In het Informatiebeveiligingsbeleid wordt aangegeven dat er op deelgebieden specifieke securityregels noodzakelijk zijn. Een van deze deelgebieden betreft de levenscyclus van informatiesystemen, van verwerving tot uitfasering. Deze regels worden in dit document vastgelegd. Software aangeschaft voor individuele gebruikers waarbij Beschikbaarheid, Integriteit en Vertrouwelijkheid niet van belang zijn, is niet gebonden aan deze regels.

Verantwoordelijkheid

1. De houder of eigenaar van een informatiesysteem is verantwoordelijk voor naleving van de securityregels.
2. Wanneer LISA het technisch- en/of applicatie beheer voert, dan worden er in de SLA met de houder ook afspraken vastgelegd ten aanzien van de security en de naleving van deze regels.
3. Toegang tot een informatiesysteem wordt geregeld conform het *Autorisatiebeleid*.

Verwerving

4. Voor of aan het begin van het project wordt er conform de *Classificatierichtlijn Informatie en Informatiesystemen* een classificatie uitgevoerd, zodat de resultaten nog de vereisten voor het informatiesysteem kunnen meebepalen.
5. Bij het gebruik van cloudservices wordt het *Juridisch normenkader cloudservices hoger onderwijs* van SURF toegepast.
6. Bij ieder projectplan voor softwareaanschaf of –ontwikkeling wordt een beveiligingsparagraaf opgenomen. De Informatie Security Manager beheert een generiek overzicht van aandachtspunten voor deze paragrafen en publiceert deze op de LISA-website.

Beheer

7. Bij door de UT ontwikkelde software worden security issues opgelost.
8. Patches en updates van leveranciers worden planmatig uitgevoerd.
9. Functiescheiding wordt daar waar nodig toegepast, voorbeeld: ontwikkelaars hebben geen rechten op de productieomgeving.
10. Toepassen van adequate wachtwoordbeveiliging, encryptie van datadragers, tijdige beveiligingspatches, antivirussoftware en een goed geconfigureerde softwarematige firewall zijn minimum vereisten voor het beheer van een informatiesysteem.

Logging

11. Er wordt niet meer gelogd dan noodzakelijk.
12. De houder houdt een registratie bij van de doelen en bewaartermijnen van de logfiles van alle informatiesystemen onder zijn verantwoordelijkheid.

Uitfasering

13. Niet meer ondersteunde software wordt uitgefaseerd, tenzij dit niet mogelijk is en passende maatregelen securityrisico’s voldoende beperken.
14. Bij uitfasering wordt aandacht besteed aan conversie, archivering en vernietiging van data.

Securityregels – Netwerk

Inleiding

In het Informatiebeveiligingsbeleid wordt aangegeven dat er op deelgebieden specifieke securityregels noodzakelijk zijn. Een van deze deelgebieden betreft het netwerk inclusief de actieve netwerkcomponenten zoals routers, switches, hubs, access-points etc. Deze regels worden in dit document vastgelegd.

Verantwoordelijkheid

1. LISA is verantwoordelijk voor het netwerk, inclusief alle actieve netwerkcomponenten zoals routers, switches, hubs, access-points etc.
2. Actieve netwerkcomponenten worden voor zover mogelijk in een afgesloten ruimte geplaatst.
3. LISA houdt een registratie bij van alle actieve netwerkcomponenten.
4. De UT hanteert als uitgangspunt een open netwerk waar in beginsel geen beperkingen aan internetverkeer worden opgelegd.
5. De UT houdt zich aan de afspraken zoals die gemaakt zijn met SURFnet.

Eigen apparatuur

6. In principe verzorgt alleen LISA de plaatsing van netwerkapparatuur. LISA houdt een registratie bij van de uitzonderingsgevallen inclusief de gemaakte schriftelijke afspraken.
7. LISA houdt een registratie van derdenaansluitingen bij, met vastlegging van de gemaakte afspraken.
8. Apparatuur die het UT-net of andere ICT-diensten verstoort of anderszins een securityissue veroorzaakt, wordt op last van CERT-UT uitgeschakeld of geïsoleerd. Dit geldt ook voor apparatuur die het gebruik van het draadloze netwerk verstoort.

Campus

9. Campusbewoners mogen eigen routers etc. installeren.
10. Wanneer de router van een campusbewoner of een van de systemen achter de router het UT-net of andere ICT-diensten verstoort of anderszins een securityissue veroorzaakt, wordt op last van CERT-UT de router uitgeschakeld of geïsoleerd.

Beheer

11. Beheer van netwerkcomponenten vindt plaats via een gescheiden beheernetwerk of tenminste via een beveiligde verbinding.
12. Beheertoegang tot netwerkcomponenten wordt geregeld conform het *Autorisatiebeleid*.

Securityregels – Afhandeling security incidenten

Inleiding

In het Informatiebeveiligingsbeleid wordt aangegeven dat er op deelgebieden specifieke securityregels noodzakelijk zijn. Een van deze deelgebieden betreft de werkwijze van CERT-UT en de afhandeling van beveiligingsincidenten. Deze regels worden in dit document vastgelegd.

Verantwoordelijkheid

1. LISA is verantwoordelijk voor het inrichten en functioneren van CERT-UT zoals vastgelegd in het Informatiebeveiligingsbeleid.
2. De Informatie Security Manager is verantwoordelijk voor het Security Incident- en Eventmanagement.

Incidenten

3. Incidenten worden onmiddellijk via de LISA-Helpdesk of rechtstreeks aan CERT-UT gemeld.
4. CERT-UT hanteert standaard procedures voor het registreren en verhelpen van incidenten.
5. Er is een specifieke procedure voor securitycalamiteiten.
6. Alle meldingen worden vertrouwelijk behandeld.

Events

7. Acties, handelingen of gebeurtenissen die invloed kunnen hebben op de beveiliging van informatie worden geconstateerd en geregistreerd. Wanneer een event invloed heeft op de bedrijfsvoering dan wordt dit als incident gemeld.

Preventie

8. De Informatie Security Manager geeft voorlichting aan gebruikers, ontwikkelaars en beheerders om securityincidenten te voorkomen.
9. De Informatie Security Manager kan gevraagd en ongevraagd advies uitbrengen over mogelijke beveiligingsproblemen.

Rapportage

10. De Informatie Security Manager levert ieder kwartaal een managementrapportage over de geconstateerde incidenten, events en uitgebrachte adviezen.
11. Deze rapportage behandelt in ieder geval alle securitycalamiteiten en gesignaleerde trends.

Securityregels – Werkplekken

Inleiding

In het Informatiebeveiligingsbeleid wordt aangegeven dat er op deelgebieden specifieke securityregels noodzakelijk zijn. Een van deze deelgebieden betreft de werkplekken van gebruikers. Deze regels worden in dit document vastgelegd.

Verantwoordelijkheid

1. LISA is verantwoordelijk voor de beveiliging van werkplekken voor zover die door LISA worden beheerd.
2. Gebruikers zijn verantwoordelijk voor de beveiliging van hun eigen werkplek voor zover die niet door LISA wordt beheerd. Via de LISA website kunnen ze beveiligingsinformatie en –hulpmiddelen vinden.

Beheer

3. Voor het beheer door LISA wordt gebruik gemaakt van aparte persoonsgebonden beheeraccounts.
4. Gebruik van beheeraccounts wordt gelogd.
5. Beheer van beheeraccounts volgt het *Autorisatiebeleid*.
6. Toepassen van wachtwoordbeveiliging, encryptie van datadragers, tijdige beveiligingspatches, antivirussoftware en een goed geconfigureerde softwarematige firewall zijn minimum vereisten voor het beheer van een werkplek.

Gebruikers

7. Medewerkers vragen nooit aan gebruikers om het wachtwoord af te geven. Zo nodig wordt aan de gebruiker gevraagd om zelf in te loggen.
8. Gebruikers worden door LISA periodiek actief geïnformeerd over beveiliging, hierbij wordt o.a. gewezen op de *Digitale gedragscode voor medewerkers*.
9. Als gebruikte apparatuur voorzieningen voor encryptie biedt, moeten deze ingeschakeld zijn.

Storingen

10. Een werkplek die het UT-net of andere ICT-diensten verstoort of anderszins een securityissue veroorzaakt, wordt op last van CERT-UT uitgeschakeld of geïsoleerd.