UNIVERSITEIT VAN AMSTERDAM | Hogeschool van Amsterdam

Baseline Informatiebeveiliging UvA-HvA

Ronald Boontje (ISM)
Bart Visser (ISO)
Rein de Vries (extern)

Datum:	13 mei 2015
Versie:	1.0
Status:	Definitief
Documenteigenaar:	Directeur ICTS
Documentbeheerder:	Information Security Officer UvA-HvA

Inhoud

1 Inleiding

1.1 Algemeen

Veel informatie en ICT-voorzieningen zijn van groot belang voor de continuïteit van de werkprocessen binnen de UvA en HvA, en voor studenten, medewerkers en derden (bezoekers, gasten e.d.). Het is dan ook vereist dat deze middelen voldoende tegen uiteenlopende dreigingen zijn beschermd. Een standaard, minimaal niveau van beveiliging is voor een ongestoorde gang van zaken een must.

Deze Baseline Informatiebeveiliging (Baseline IB) beschrijft een set van beheersmaatregelen die tenminste nodig zijn om alle informatie die van belang is voor beide instellingen te beschermen tegen onbevoegde toegang, corruptie, fouten, verlies en uitval. Daarnaast beschrijft deze Baseline de maatregelen die minimaal nodig zijn om de ICT-voorzieningen van de UvA en de HvA te beschermen tegen onbevoegd gebruik, uitval of beschadiging. Tenslotte geeft de Baseline IB aan welk gedrag de instelling verwacht c.q. verlangt van studenten, medewerkers en gasten om informatie en voorzieningen voldoende beveiligd te laten zijn.

De Baseline IB beschrijft hoe de instelling het wat betreft informatiebeveiliging op orde wenst te hebben. Op het moment dat deze Baseline IB formeel als basisbeveiligingsnorm is bekrachtigd zullen lang niet alle beschreven beheersmaatregelen geïmplementeerd zijn. Een stapsgewijze, gefaseerde invoering is nodig, hetzij middels een aantal gerichte activiteiten, hetzij als onderdeel van een of meer ICT-projecten.

De Baseline IB sluit aan op wet- en regelgeving die relevant is voor informatiebeveiliging, en is gebaseerd op de algemeen geaccepteerde open standaarden NEN/ISO27001 en 27002.

Wetten en regelingen die van toepassing zijn, zijn onder meer:

- Wet op het Hoger onderwijs en Wetenschappelijk onderzoek
- Wet Bescherming Persoonsgegevens (WBP), inclusief het bijbehorende Vrijstellingsbesluit
- Wet Computercriminaliteit II
- Telecommunicatiewet
- Archiefwet
- Auteurswet

Daarnaast wordt de inhoud zoveel mogelijk afgestemd op gemeenschappelijke landelijke beveiligingsnormen voor het onderwijs en de overheid. Voorbeelden hiervan zijn:

- Juridisch normenkader cloud services Hoger Onderwijs (SURF)
- ICT-beveiligingsrichtlijnen voor webapplicaties (NCSC)
- Baseline Informatiebeveiliging Rijksdienst/Gemeenten (BIR/BIG)

In de Baseline IB is rekening gehouden met de architectuurprincipes die betrekking hebben op informatiebeveiliging, zoals die door de Architectuurcommunity HvA-UvA zijn opgesteld.

De instelling evalueert de Baseline IB tenminste elke drie jaar en stelt deze indien nodig bij. Bijstelling vindt plaats in samenspraak met de Regiegroep ICTS en de Expertisegroepen Basisdiensten.

1.2 Aard en reikwijdte

Deze baseline is bedoeld als een algemeen geldend minimumniveau van maatregelen voor beveiliging van de informatievoorziening binnen de UvA en HvA. Alle informatiesystemen van enig belang dienen de baseline na te leven, en om te beginnen de concerninformatiesystemen. De beschreven maatregelen zijn een combinatie van best-practices en bestaande praktijken. Bij het samenstellen van de inhoud is primair uitgegaan van de 2007-versie van de Code voor Informatiebeveiliging (ISO 27002:2007).

Voor de beschreven maatregelen geldt het ‘pas toe of leg uit’ beginsel. Afwijken kan, maar alleen vanwege zakelijk onderbouwde en gegronde redenen.

De reikwijdte van deze Baseline IB omvat alle medewerkers, studenten, gasten, bezoekers en externe relaties (inhuur / outsourcing), alsmede alle organisatieonderdelen. Tevens vallen onder de baseline alle bedrijfsprocessen, onderliggende informatiesystemen, inclusief devices van waaraf geautoriseerde toegang tot het instellingsnetwerk verkregen kan worden.

De Baseline IB heeft betrekking op de informatie van de instelling in de meest brede zin van het woord, die daarbinnen verwerkt wordt. Ook als gebruikers instellingsinformatie niet binnen de instelling verwerken, maar bijvoorbeeld in de cloud, is deze Baseline IB van toepassing.

1.3 De structuur van de baseline

Hoofdstuk 1 en 2 geven een inleiding op de baseline en de dreigingen waaraan het Hoger Onderwijs met name bloot staat. Hoofdstuk 3 bevat een verklarende woordenlijst voor termen die veel worden gebruikt. De opbouw en het gebruik van de baseline wordt behandeld in Hoofdstuk 4. Dit hoofdstuk laat zien hoe aan de hand van de classificatie bepaald kan worden of de beheersmaatregelen uit de Baseline IB toereikend zijn, danwel of mogelijk aanvullende maatregelen nodig zijn.

Elk van de hoofdstukken 5 t/m 15 bevat een aantal hoofdbeveiligingscategorieën. Elke hoofdbeveiligingscategorie (bijvoorbeeld 6.1) bevat een beheersdoelstelling die omschrijft welk specifiek beveiligingsdoel wordt nagestreefd, alsmede één of meer beheersmaatregelen (6.1.1 t/m 6.1.8) die moeten worden ingevuld om de beheersdoelstelling te behalen. Deze tekstgedeelten zijn cursief weergegeven en zijn een-op-een overgenomen uit de ISO 27002:2007-standaard. De overige tekstdelen bevatten de uitwerkingen, in de vorm van richtlijnen, zoals die specifiek voor UvA en HvA gelden. In een aantal gevallen zijn de gestelde richtlijnen direct toepasbaar. In andere gevallen is een vertaling nodig naar een procedure of een implementatierichtlijn op uitvoeringsniveau.

Bijlage 1 bevat een uitwerking van bevoegdheden en verantwoordelijkheden van de aangestelde Eigenaar van een informatiesysteem waar het informatiebeveiliging betreft. Bijlage 2 beschrijft de toegepaste systematiek voor identificatie en authenticatie (‘Level of Assurance’). Bijlage 3 geeft de beveiligingseisen voor het omgaan met informatie door gebruikers.

2 Cyberdreigingen

In het cyberdreigingsbeeld voor de sector Hoger Onderwijs en Wetenschappelijk Onderzoek, dat in november 2014 door SURF is gepubliceerd, wordt ingegaan op de diverse aspecten die een rol spelen bij de cyberdreigingen[1] waarmee een Hoger Onderwijs instelling zoals de HvA en UvA wordt geconfronteerd.

Het dreigingslandschap wordt omvangrijker en complexer. Dit komt door:

- Toenemende connectiviteit: meer internet, (mobiele) apparatuur, interfaces en opslag en verwerking in de cloud;
- Groei van digitale data: meer en zoveel mogelijk (big) data en meer gedeeld;
- Toename geavanceerde cyberdreigingen: meer winst mee te behalen, beter georganiseerd en onbeperkte middelen beschikbaar;
- Digitalisering in O&O: meer gebruik van digitale mogelijkheden.

Cyberdreigingen waar een instelling mee te maken kan krijgen zijn:

- Verkrijging en openbaarmaking van (vertrouwelijke) informatie, denk aan persoons-, onderzoeksgegevens, intellectueel eigendom;
- Identiteitsfraude: je voordoen als een ander voor persoonlijk winstbejag, oneigenlijk toegang, et cetera;
- Manipulatie van data: zoals het ‘corrigeren’ van studieresultaten;
- Spionage: ontvreemding van onderzoeksgegevens voor buitenlandse mogendheden;
- Verstoring van ICT: DDoS- en malware-aanvallen;
- Overname en misbruik ICT, bijvoorbeeld om spam te versturen, DDoS-aanvallen uit te voeren of andere systemen te overmeesteren;
- Bewust beschadigen imago: activisten, digitaal bekladden.

Als actoren die vanuit bepaalde belangen een dergelijke cyberdreiging ten uitvoer kunnen brengen, worden genoemd:

- Studenten
- Medewerkers
- Cybercriminelen
- Cyberonderzoekers
- Staten
- Commerciële bedrijven en partnerinstellingen
- Activisten en cybervandalen

Een instelling kan ernstige schade oplopen als bovengenoemde dreigingen zich manifesteren. Denk daarbij aan:

- Financiële schade (claims)
- Reputatieschade
- Uitval van onderwijs en/of onderzoek
- Kamervragen
- Terugtreden bestuurders

De beheersmaatregelen die in deze Baseline IB zijn opgenomen hebben als doel om enerzijds schade door beveiligingsincidenten zo goed mogelijk voor te zijn en anderzijds de schadelijke gevolgen van incidenten zo veel mogelijk te beperken, onder meer door incidenten in een zo vroeg mogelijk stadium te detecteren.

[1] Cyberdreigingen zijn ongewenste gebeurtenissen die schade kunnen toebrengen aan de instelling door verstoring, uitval of (bewust) misbruik van ICT-middelen en –diensten die digitaal (bijvoorbeeld via internet) aan de buitenwereld (kunnen) zijn verbonden.

3 Begrippenlijst

Voor de informatiebeveiliging van de instelling gelden de volgende definities:

2FA / 2-factor authenticatie: Een wijze van authenticatie die een hoge mate van zekerheid biedt dat het daadwerkelijk de legitieme gebruiker is die zich aanmeldt, door het toepassen van twee authenticatiefactoren, zoals via iets wat alleen jij weet (een wachtwoord) èn iets wat alleen in jouw bezit is (zoals een uniek token).

Authenticatie: Het verifiëren van de identiteit van een persoon of zaak, aan de hand van met de identiteit verbonden kenmerken, zoals een wachtwoord en/of fysieke kenmerken.

Bedrijfskritisch systeem: systeem dat ingevolge de classificatiemethodiek als '*gevoelig'* of *'kritiek'* is geclassificeerd.

Beschikbaarheid: Het waarborgen dat vanuit hun functie geautoriseerde gebruikers op de juiste momenten tijdig toegang hebben tot informatie en aanverwante bedrijfsmiddelen (informatiesystemen).

Betrouwbaarheid: De mate waarin de organisatie zich kan verlaten op een informatiesysteem voor zijn informatievoorziening, ter ondersteuning van een of meer afhankelijke bedrijfsprocessen.

BYOD – Bring Your Own Device: Het gebruik van 'vreemde' ICT-middelen toestaan, zoals smartphone, tablet, laptop en USB-stick, die niet eigendom van de organisatie zelf zijn (privé of van een derde partij, zoals een dienstverlener).

Calamiteitenplan: Opsomming van alle maatregelen welke tot uitvoering moeten komen als zich een situatie voordoet waarbij de beschikbaarheid, integriteit en/of vertrouwelijkheid van een informatiesysteem in beduidende mate niet aan de eisen voldoen.

Eigenaar: Identificeerbaar, aangewezen persoon binnen de organisatie die een specifieke rol vervult voor een specifiek bedrijfsmiddel zoals een informatiesysteem, gegevensverzameling, bedrijfsruimte of overeenkomst. Denk bij een informatiesysteem of gegevensverzameling aan het (eind)verantwoordelijk zijn voor het specificeren, implementeren en handhaven van beveiliging van het systeem cq. de gegevensverzameling. Eigenaarschap is hierbij niet in juridische zin en ligt veelal bij de manager van het proces dat het systeem benut.

Functiescheiding: Het uit controle-overwegingen aanbrengen van een splitsing in taken en bevoegdheden die samenhangen met handelingen, die in potentie verstrekkende gevolgen (kunnen) hebben, over verschillende daartoe aangewezen functionarissen.

Gebruiker: Elk persoon die op enige wijze is verbonden aan de instelling, voor zijn/haar werk middelen van de organisatie benut (zoals informatie, informatiesystemen en ruimten) en tot dit gebruik geautoriseerd is, zoals vaste en tijdelijke medewerkers, studenten, externen, stagiaires/afstudeerders, et cetera.

Informatiebeveiliging: Het proces van vaststellen van de vereiste betrouwbaarheid van informatiesystemen in termen van vertrouwelijkheid, beschikbaarheid en integriteit alsmede het treffen, onderhouden en controleren van een samenhangend pakket van bijbehorende maatregelen.

Informatiebeveiligingsgebeurtenis ('beveiligingsincident'): Geconstateerde dan wel vermoede aantasting van de vertrouwelijkheid, integriteit en/of de beschikbaarheid van informatie of informatievoorzieningen alsmede situaties die het ontstaan van een aantasting in de hand werken.

Informatiesysteem: Een samenhangend geheel van gegevensverzamelingen, en de daarbij behorende personen, procedures, processen en software alsmede de voor het informatiesysteem getroffen voorzieningen voor opslag, verwerking en communicatie.

Instelling: Hetzij HvA danwel UvA.

Integriteit: Het waarborgen van de juistheid en volledigheid van informatie en de verwerking ervan.

Level of Assurance: De gewenste/vereiste mate van zekerheid 1) wat betreft de identiteit van de gebruiker bij registratie (is hij werkelijk de persoon voor wie hij zich uitgeeft) en 2) dat het daadwerkelijk de legitieme gebruiker is die inlogt in het systeem (authenticatie).

Restrisico: Het risico dat overblijft (resteert) nadat maatregelen zijn getroffen.

Risico: De kans (waarschijnlijkheid) dat een onzekere gebeurtenis met negatieve effecten zich in een gegeven periode en situatie zal voordoen.

Risicobeheer: Het systematisch inventariseren, beoordelen en door het treffen van maatregelen beheersbaar maken van risico's en kansen die het bereiken van de doelstellingen van een organisatie bedreigen dan wel bevorderen.

Step up: Een extra ingebouwde, verplichte authenticatieslag om een of meer handelingen te kunnen verrichten waarvoor bijzondere rechten nodig zijn, bijvoorbeeld voor het invoeren van tentamenresultaten of het plegen van technisch of functioneel beheer.

Sterke authenticatie: Een wijze van authenticatie die een hoge mate van zekerheid biedt dat het daadwerkelijk de legitieme gebruiker is die zich aanmeldt, door het toepassen van meer dan één authenticatiefactor (zoals via iets wat alleen jij weet èn iets wat alleen in jouw bezit is).

Sterk wachtwoord: Een wachtwoord dat voldoet aan gestelde kwaliteitscriteria waardoor het zeer lastig te raden is. Denk hierbij aan lengte (aantal karakters), het gebruik van vreemde tekens en verbod op woordenboekwoorden.

Vertrouwelijkheid: Het waarborgen dat informatie alleen toegankelijk is voor degenen, die hiertoe zijn geautoriseerd. Het gaat hier onder meer om het beveiligen van de toegang tot de gebouwen, informatiesystemen en de ICT-infrastructuur tegen onbevoegden (hackers en andere indringers) en malafide software (virussen, Trojan horses e.d.). Maar ook om maatregelen om te voorkomen dat gebruikers toegang krijgen tot informatie die niet voor hen is bedoeld.

4 Over het gebruik van deze Baseline

4.1 Beveiligingsniveaus

Informatiebeveiliging maakt onderscheid tussen de kwaliteitsaspecten beschikbaarheid, integriteit en vertrouwelijkheid.

- **Beschikbaarheid:** de mate waarin gegevens of functionaliteit op de juiste momenten beschikbaar zijn voor gebruikers;
- **Integriteit:** de mate waarin gegevens of functionaliteit correct zijn;
- **Vertrouwelijkheid:** de mate waarin de toegang tot gegevens of functionaliteit beperkt is tot degenen die daartoe bevoegd zijn.

Wat betreft beveiligingsmaatregelen worden drie niveaus onderscheiden:

- **Standaard:** Verstoring van de beschikbaarheid , integriteit en/of vertrouwelijkheid van de informatie veroorzaakt een belemmering in een van de secundaire processen, maar niet van ernstige of onomkeerbare aard. De verstoring brengt geen merkbare schade toe, mogelijk enig ongemak / lichte schade aan het imago van de instelling;
- **Gevoelig:** Een inbreuk op de beschikbaarheid, integriteit en/of vertrouwelijkheid van informatie veroorzaakt een verstoring in een van de primaire processen, maar niet van zeer ernstige of onomkeerbare aard. Ook mogelijke negatieve effecten voor het imago van de instelling kunnen aanleiding zijn om de classificatie ‘gevoelig’ toe te kennen.
- **Kritiek:** Aantasting van beschikbaarheid, integriteit en/of vertrouwelijkheid veroorzaakt een zeer ernstige of onomkeerbare verstoring van een van de primaire processen, brengt ernstige schade toe aan het imago van de instelling of houdt een ernstige wetsovertreding in.

Implementatie van het ‘standaard’ beveiligingsniveau biedt bescherming tegen verlies van vertrouwelijkheid, verlies van integriteit en permanent verlies van gegevens door alledaagse niet-gerichte dreigingen, zoals virussen, stroomuitval, hardware fouten, “script-kiddie” aanvallen en basale fouten van beheerders. Beschikbaarheid wordt bepaald op basis van “best effort”.

Soms is meer bescherming nodig dan het standaardniveau kan bieden. Bijvoorbeeld tegen gerichte aanvallen – een aanvaller wil om een bepaalde reden niet “een systeem” hacken, maar per se “dát systeem”. Of beschikbaarheid is van zo'n groot belang dat “best effort” niet meer voldoende is. Het hogere niveau, aangeduid met ‘gevoelig’ dient bescherming te bieden tegen toegang tot gegevens door gerichte aanvallen van niet-professionele aanvallers met een in zekere mate beperkt kennis en middelen niveau en fysieke toegang tot het instellingsnetwerk, verhoogde bescherming tegen ongeautoriseerde wijziging of vernietiging van gegevens door technisch falen en gericht handelen van personen. Ongeautoriseerde wijziging of vernietiging kan wel optreden, maar is op dit niveau doorgaans tegen redelijke meerkosten te herstellen. Het dient tevens een verhoogde bescherming te bieden tegen verlies en uitval als gevolg van technisch falen door middel van toepassing van noodstroom (geschikt om langdurige stroomonderbreking op te vangen) en redundante voedingen/voedingslijnen. Op dit niveau is nog geen sprake van algehele systeem-redundantie of bescherming tegen bewust veroorzaakte uitval. Uitval is dus wel mogelijk, maar de kans is substantieel kleiner ten opzichte van het basisniveau door toepassing van noodstroom en enige redundantie op hardware niveau. Dit niveau is tegen redelijke meerkosten te realiseren.

Het ‘standaard’ niveau en het naast hogere ‘gevoelig’ niveau zijn beschreven in de baseline. Voor het niveau ‘gevoelig’ zijn extra maatregelen beschreven met name op het gebied van toegangsbeheer, encryptie en redundantie.

De maatregelen die nodig zijn voor het hoogste beveiligingsniveau, aangeduid met ‘kritiek’, zijn niet beschreven in deze baseline. Voor dit niveau is altijd sprake van maatwerk. Een risicoanalyse is vereist om te kunnen bepalen welke onderdelen extra aandacht behoeven. In het algemeen geldt dat dit niveau bescherming moet bieden tegen ongewenste toegang tot gegevens door gerichte aanvallen van professionele aanvallers met veel kennis en middelen en fysieke toegang tot het instellingsnetwerk. Ook is bescherming vereist tegen wijziging of vernietiging van gegevens door ernstig technisch falende apparatuur of gerichte aanvallen van professionele frauderende handelingen. tenslotte is een zeer hoge bescherming vereist tegen verlies en uitval (ongeacht de oorzaak, al dan niet moedwillig) door o.a. algehele systeemredundantie en noodstroomvoorzieningen (geschikt om langdurige stroomonderbreking op te vangen). De kans op uitval is bij het beschermingsniveau ‘kritiek’ zeer

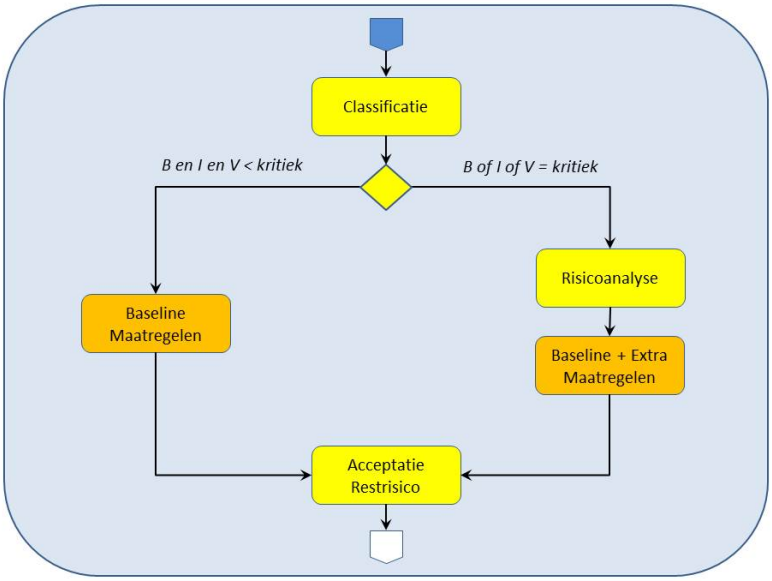
laag. Het realiseren van dit niveau brengt doorgaans (zeer) hoge kosten met zich mee en levert veelal meer ongemak op voor gebruikers.

4.2 Risicobeheersing

Via classificatie kunnen de risico's die gemoeid zijn met informatie en informatiesystemen effectief en efficiënt worden beheerst. Daarbij worden deze middelen ingedeeld in verschillende risicoklassen die elk een verschillend niveau van beveiligingsmaatregelen kennen. De beheersing zit 'm in het stomweg implementeren van alle maatregelen zoals bepaald door de toegekende risicoklasse. Aanvullend worden gebruikers gevraagd informatie te behandelen overeenkomstig de risicoklasse van de informatie, zie Bijlage 3 (Beveiligingseisen Verwerken Informatie) met de richtlijnen zoals deze van kracht zijn binnen de UvA en HvA.

Bij informatiebeveiliging onderscheiden we grofweg drie type bedrijfsmiddelen: informatiesystemen, gegevensverzamelingen en (losse, ongestructureerde) informatie. In lijn met de architectuurprincipes van de UvA-HvA[2] hebben deze middelen een Eigenaar met specifieke verantwoordelijkheden, zie Bijlage 1. De Eigenaar van het betreffende bedrijfsmiddel bepaalt de risicoklasse[3].

Het beveiligingsniveau van de maatregelen uit deze Baseline IB is zo gekozen dat dit voor de meeste processen en ondersteunende ICT-voorzieningen bij beide instellingen voldoende is. Hiermee voorkomen we dat voor ieder systeem een uitgebreide risicoanalyse nodig is.



Dit is schematisch weergegeven in bovenstaande figuur.

Een informatiesysteem moet als 'kritiek' worden bestempeld als het niet beschikbaar zijn van het systeem (B), het uitlekken van informatie (V) en/of het incorrect zijn van de informatieverwerking (I) leidt tot (een kans op) onacceptabele schade[4] voor de instelling of als daarmee de instelling met (de kans op) dergelijke incidenten een ernstige overtreding van wet- en regelgeving begaat. Dit is onder meer het geval als het systeem door optredende schade slechts zeer kort niet beschikbaar mag zijn, als er sprake is van zeer vertrouwelijke persoonsgegevens zoals bedoeld in Artikel 16 van de WBP, of als een verwerkingsfout (schending van integriteit) kan leiden tot zeer hoge kosten.

Als een informatiesysteem informatie verwerkt die als 'geheim' is bestempeld, geldt het beveiligingsniveau 'kritiek' en is een volledige risicoanalyse nodig die kan resulteren in extra maatregelen.

---

2 Architectuurprincipes UvA/HvA Versie 1.0, 10 november 2014.

3 Eigenaren treden over de toe te kennen risicoklasse in overleg als de eigenaar van de gegevensverzameling een andere is dan de eigenaar van het informatiesysteem dat de gegevensverzameling huisvest.

4 Ordegrootte 100 k€ of hoger. Denk bij schade ook aan kosten voor herstel van de correctheid informatie, kosten voor het opnieuw beschikbaar maken van informatie, kosten van alternatieven om informatie (tijdig) beschikbaar te maken, et cetera.

Bij het inventariseren, analyseren en minderen van risico's dient uiteindelijk de Eigenaar als eindverantwoordelijke te besluiten tot het treffen van extra maatregelen, door af te wegen of de kosten en inspanning die gemoeid zijn met de implementatie van aanvullende beveiligingsmaatregelen opwegen tegen de mogelijke schade als gevolg van het manifest worden van onderkende risico's. Als een Eigenaar besluit tot extra maatregelen dienen de set van extra maatregelen en het accepteren van restrisico in de vorm van een beveiligingsplan te worden gedocumenteerd.

De Eigenaar kan op verschillende manieren met (rest-)risico's omgaan. Mogelijke strategieën zijn:

1. **Risicomijdend**
   Besluiten om in verhouding veel – zo veel als redelijkerwijs mogelijk is - in beveiliging(smaatregelen) te investeren om zo min mogelijk risico te lopen. Op de langere termijn kan dit resulteren in hogere kosten voor de organisatie voor maatregelen dan kosten die door incidenten zouden zijn veroorzaakt, die de organisatie via maatregelen heeft ingeperkt;

2. **Risiconeutraal**
   Besluiten om te maken kosten voor beveiliging(smaatregelen) vergelijkbaar te laten zijn met de kosten (schade) die incidenten over een langere periode gezien (bijvoorbeeld jaarlijks) veroorzaken;

3. **Risicodragend**
   Besluiten om risico te lopen c.q. accepteren, waardoor de organisatie in verhouding minder in beveiliging(smaatregelen) hoeft te investeren. Op de langere termijn kan dit resulteren in hogere kosten voor de organisatie door incidenten dan zou zijn uitgegeven om deze incidenten in te perken.

De keuze voor een bepaalde strategie dient door de Eigenaar bewust te worden gemaakt. Het accepteren van restrisico's dient te worden gedocumenteerd.

5 Beveiligingsbeleid

5.1 Informatiebeveiligingsbeleid

Doelstelling:
De directie richting en ondersteuning bieden voor informatiebeveiliging overeenkomstig de bedrijfsmatige eisen en relevante wetten en voorschriften.

5.1.1 Beleidsdocument voor informatiebeveiliging

Een document met informatiebeveiligingsbeleid behoort door de directie te worden goedgekeurd, gepubliceerd en kenbaar te worden gemaakt aan alle werknemers en relevante externe partijen.

Het College van Bestuur (CvB) stelt het beleid voor informatiebeveiliging vast in een beleidsdocument (Informatiebeveiligingsbeleid UvA-HvA), ziet toe op beleidsimplementatie en draagt het beleid uit. De Information Security Officer (ISO) verzorgt de praktische invulling van deze verantwoordelijkheid in afstemming met de directeur ICTS.

Een lid van het CvB vervult de rol van Portefeuillehouder Informatiebeveiliging (IB). De Portefeuillehouder IB is eigenaar van het Informatiebeveiligingsbeleid UvA-HvA en is eindverantwoordelijk voor informatiebeveiliging binnen de UvA en de HvA.

Het Informatiebeveiligingsbeleid UvA-HvA is evenals deze baseline voor iedereen die tot de organisatie behoort beschikbaar via het intranet. Ze mag worden gecommuniceerd naar partijen met wie de instelling een formele relatie onderhoudt.

5.1.2 Beoordeling van het informatiebeveiligingsbeleid

Het informatiebeveiligingsbeleid behoort met geplande tussenpozen, of zodra zich belangrijke wijzigingen voordoen, te worden beoordeeld om te bewerkstelligen dat het geschikt, toereikend en doeltreffend blijft.

Tenminste elke drie jaar, of zodra zich belangrijke wijzigingen voordoen, evalueert en beoordeelt een commissie ingesteld door de Chief Security Officer (CSO) het informatiebeveiligingsbeleid in opdracht van het CvB.

De CSO is tezamen met de ISO verantwoordelijk voor het signaleren van een eventuele noodzaak tot en het initiëren van tussentijdse evaluatie c.q. beoordeling.

Bij de evaluatie kijkt de commissie naar mogelijkheden voor verbetering van het informatiebeveiligingsbeleid en de benadering van het beheren van informatiebeveiliging als reactie op onder meer het bestaan en de werking van informatiebeveiliging, beveiligingsincidenten, terugkoppeling van belanghebbende partijen, resultaten van onafhankelijke beoordeling, veranderingen in de organisatie, wijziging van de (bedrijfs-)omstandigheden, wettelijke voorwaarden en/of de technische omgeving.

Onder verantwoordelijkheid van de CSO wordt een verslag gemaakt van de evaluatie. De geïdentificeerde verbeteringen worden in een geactualiseerde versie van het Informatiebeveiligingsbeleid opgenomen en ter goedkeuring aan het CvB voorgelegd voordat ze worden gepubliceerd. De CSO is verantwoordelijk voor het archiveren van evaluatieverslagen.

6 Organisatie van informatiebeveiliging

6.1 Interne organisatie

Doelstelling:
Beheren van de informatiebeveiliging binnen de organisatie.

6.1.1 Betrokkenheid van de directie bij informatiebeveiliging

De directie behoort actief beveiliging binnen de organisatie te ondersteunen door duidelijk richting te geven, betrokkenheid te tonen en expliciet verantwoordelijkheden voor informatiebeveiliging toe te kennen en te erkennen.

De rol van het CvB is vastgelegd in het Informatiebeveiligingsbeleid UvA-HvA. Het CvB is met name eindverantwoordelijk voor informatiebeveiliging binnen de instelling en stelt het beleid en de basismaatregelen op het gebied van informatiebeveiliging vast.

6.1.2 Coördinatie van informatiebeveiliging

Activiteiten voor informatiebeveiliging behoren te worden gecoördineerd door vertegenwoordigers uit verschillende delen van de organisatie met relevante rollen en functies.

De organisatie van de informatiebeveiligingsfunctie, waaronder coördinatie, is vastgelegd in het Informatiebeveiligingsbeleid UvA-HvA.

6.1.3 Toewijzing van verantwoordelijkheden voor informatiebeveiliging

Alle verantwoordelijkheden voor informatiebeveiliging behoren duidelijk te zijn gedefinieerd.

De verantwoordelijkheden voor informatiebeveiliging en de toewijzing, zijn vastgelegd in het Informatiebeveiligingsbeleid.

6.1.4 Goedkeuringsproces voor IT-voorzieningen

Er behoort een goedkeuringsproces voor nieuwe IT-voorzieningen te worden vastgesteld en geïmplementeerd.

Het goedkeuringsproces voor grotere ICT-vernieuwingstrajecten (al dan niet instellingsbreed) is verwoord in het collegebesluit van 9 oktober 2012 betreffende de ICT governance UvA–HvA.

Voor UvA en HvA is een regiegroep ICT in het leven geroepen, die het CvB adviseren in alle relevante strategische ICT-zaken en de budgetten voor ICT-projecten.

De regiegroep ICT bestaat uit een decaan resp. domeinvoorzitter, de voorzitters van de expertisegroepen en het hoofd van het informatieregiesecretariaat ICT UvA-HvA.

Naast de regiegroep ICT is er het informatieregiesecretariaat, dat o.a. als taak heeft om de Regiegroep te ondersteunen en de faculteiten/domeinen te ondersteunen op het gebied van ICT-beleid en SLA-afspraken met de ICTS. Tevens verzorgt het informatieregiesecretariaat het portfoliomanagement van de ICT – vernieuwingsprojecten.

De Expertisegroepen bestaan uit informatiemanagers en vertegenwoordigers van eenheden binnen faculteiten/domeinen en diensten. Zij verzamelen informatie inzake bestaande en gewenste, toekomstige ICT-voorzieningen en rapporteren hierover aan de regiegroep ICT.

6.1.5 Geheimhoudingsovereenkomst

Eisen voor vertrouwelijkheid of geheimhoudingsovereenkomst die een weerslag vormen van de behoefte van de organisatie aan bescherming van informatie behoren te worden vastgesteld en regelmatig te worden beoordeeld.

Aanstelling
Behoudens het gestelde in de aanstelling (UvA) danwel de arbeidsovereenkomst (HvA) kent de instelling geen aparte geheimhoudings- c.q. integriteitsovereenkomst voor medewerkers (zowel vast als tijdelijk).

Overeenkomsten
Om vertrouwelijkheid van informatie te waarborgen dienen leverings- en samenwerkingsovereenkomsten met derden, zoals leveranciers en ketenpartners, altijd een toereikende, juridisch afdwingbare geheimhoudingsparagraaf met boeteclausules te bevatten.

De Algemene Inkoopvoorwaarden van de instelling voorzien hierin en zijn in de meeste gevallen afdoende. Deze voorwaarden worden periodiek afgestemd op de eisen voor vertrouwelijkheid van de instelling en de geldende wet- en regelgeving op dit gebied. Ze voldoen tenminste aan de volgende eisen en richtlijnen:

1. In de overeenkomst behoudt de instelling zich het recht op audit voor, van activiteiten waarbij vertrouwelijke informatie betrokken is. Dit behelst het recht om activiteiten inzake waarborging van vertrouwelijkheid te (laten) controleren;
2. Geheimhouding dient na afloop van de overeenkomst en/of de werkzaamheden voor onbepaalde duur van kracht blijven;
3. Correcte borging van eigendom van informatie, bedrijfs- en (vak)geheimen en intellectueel eigendom;
4. Informatie van de instelling met een vertrouwelijk karakter wordt na afloop van de overeenkomst en/of de werkzaamheden naar keuze van de instelling geretourneerd danwel op door de instelling voorgeschreven wijze vernietigd;
5. Personen die zonder aanstelling of arbeidsovereenkomst werkzaamheden verrichten voor de instelling, zoals ingehuurde krachten, medewerkers van leveranciers, stagiaires en afstudeerders, dienen via een individuele verklaring met boeteclausules te worden gehouden aan geheimhouding en integriteit. Werkzaamheden mogen niet eerder dan na ondertekening aanvangen.

Aanvullend op de Algemene Inkoopvoorwaarden van de instelling kunnen afhankelijk van de risicosetting aanvullende afspraken worden gemaakt met betrekking tot:

1. Definitie en omschrijving van het toegestane gebruik van informatie met een vertrouwelijk karakter;
2. Vereiste maatregelen en activiteiten ter waarborging van de vertrouwelijkheid;
3. Notificatie en rapportage bij schending;
4. Aansprakelijkheid en sancties bij schending.

Personen die zonder aanstelling of arbeidsovereenkomst werkzaamheden verrichten voor de instelling dienen uitsluitend toegang te krijgen tot informatie die voor de openbaarheid bestemd is, danwel de informatie die voor het uitvoeren van hun taak noodzakelijk is.

Als de instelling een overeenkomst van een derde partij accepteert, moet de manager onder wiens verantwoordelijkheid verplichtingen worden aangegaan (de “Contracteigenaar”), toe te zien op opname van een toereikende geheimhoudingsparagraaf inclusief boeteclausule.

6.1.6 Contact met (overheids-)instanties

Er behoren geschikte contacten met relevante overheidsinstanties te worden onderhouden.

Vanuit risicoperspectief is er voor de instelling geen noodzaak om in het kader van informatiebeveiliging anders dan het normale contact te onderhouden met instanties zoals brandweer, politie, nutsbedrijven en gezondheids- en/of veiligheidsinstanties.

6.1.7 Contact met speciale belangengroepen

Er behoren geschikte contacten met speciale belangengroepen of andere specialistische platforms voor beveiliging en professionele organisaties te worden onderhouden.

De informatiebeveiligingsfunctionarissen van de instelling nemen deel in het landelijke overleg van informatiebeveiligers in het hoger onderwijs (SURFibo).

Via SCIRT (Surfnet Community for Incident Response Teams) onderhoudt de instelling nauwe samenwerkingscontacten met SURFcert en CERTs (Computer Emergency Response Teams) van andere onderwijsinstellingen.

Daarnaast nemen de informatiebeveiligingsfunctionarissen van de instelling deel aan professionaliseringsactiviteiten bij organisaties zoals Platform voor Informatiebeveiliging (PvIB), e.d.

6.1.8 Onafhankelijke beoordeling van informatiebeveiliging

De benadering van de organisatie voor het beheer van informatiebeveiliging en de implementatie daarvan (d.w.z. beheersdoelstellingen, beheersmaatregelen, beleid, processen en procedures voor informatiebeveiliging) behoren onafhankelijk en met geplande tussenpozen te worden beoordeeld, of zodra zich significante wijzigingen voordoen in de implementatie van de beveiliging.

De ISO is verantwoordelijk voor periodieke onafhankelijke beoordeling, zowel door interne als externe partijen, en voor het signaleren van een eventuele noodzaak tot en het initiëren van tussentijdse beoordeling. Hij is ook verantwoordelijk voor het archiveren van beoordelingsrapporten.

Onafhankelijke interne beoordeling
De onafhankelijke interne beoordeling van de implementatie van het informatiebeveiligingsbeleid wordt uitgevoerd door de afdeling Financiën, Planning & Control. De ISO en de hoofden van deze afdelingen stemmen af welke beoordelingsactiviteiten in welke periode moeten worden uitgevoerd. Jaarlijks nemen deze afdelingen de in dit kader uit te voeren activiteiten in hun audit jaarplan op. Rapportage is gericht aan de ISO.

Externe beoordeling
Het Informatiebeveiligingsbeleid UvA-HvA en de Baseline Informatiebeveiliging UvA-HvA worden tezamen met de verdere structurele invulling van informatiebeveiliging in opdracht van de ISO tenminste een keer per drie jaar beoordeeld op geschiktheid, toereikendheid, doeltreffendheid en effectiviteit door een onafhankelijke deskundige partij. Hierbij wordt gerapporteerd aan de ISO.

Verder verricht aanvullend de accountant van de instelling jaarlijks in het kader van de werkzaamheden op het gebied van de jaarrekening externe controle van de algemene kwaliteit van de informatiebeveiliging en belangrijke onderdelen van het beveiligingsstelsel en maatregelen. De accountant rapporteert aan het CvB.

6.2 Externe partijen

Doelstelling:
Beveiliging van de informatie en IT-voorzieningen van de organisatie handhaven waartoe externe partijen toegang hebben of die door externe partijen worden verwerkt of beheerd, of die naar externe partijen wordt gecommuniceerd.

6.2.1 Identificatie van risico's die betrekking hebben op externe partijen

De risico's voor de informatie en IT-voorzieningen van de organisatie vanuit bedrijfsprocessen waarbij externe partijen betrokken zijn, behoren te worden geïdentificeerd en er behoren geschikte beheersmaatregelen te worden geïmplementeerd voordat toegang wordt verleend.

Wat betreft identificatie van risico's die betrekking hebben op externe partijen beperkt de instelling zich tot een aantal basisvoorwaarden waaraan voldaan moet worden.

Waar het zakelijk gezien nodig is om (medewerkers van) een externe partij toegang te verlenen tot informatie of IT-voorzieningen van de instelling, moet:

1. Zoveel als redelijkerwijs mogelijk is de toegang worden beperkt tot hetgeen functioneel en zakelijk gezien noodzakelijk is;
2. De Eigenaar verlangt van de externe partij dat zij zich conformeert aan het beveiligingsbeleid van de instelling. De Eigenaar legt alle voorwaarden waaronder toegang wordt verleend vast in een door beide partijen rechtsgeldig te ondertekenen overeenkomst. De externe partij dient daarbij de aansprakelijkheid te aanvaarden die gepaard gaan met de toegang tot informatie en IT-voorzieningen van de instelling en het verwerken, communiceren of beheren ervan. De Eigenaar van het informatiesysteem is (eind) verantwoordelijk voor de overeenkomst;
3. Worden gewaarborgd dat de externe partij kennis draagt van de Acceptable Use Policy (AUP) en de ICT gedragsregels, inclusief verplichtingen en verantwoordelijkheden.

Alleen de Eigenaar van een informatiesysteem kan toegang door een externe partij autoriseren. De Eigenaar laat in zijn beslissing de risico's die de toegang met zich meebrengt meewegen en neemt daarbij onder meer in ogenschouw:

1. Zakelijke noodzaak, inclusief eisen/beperkingen vanuit wet- en regelgeving en contractuele verplichtingen;
2. Het informatiesysteem zelf en de aard van de informatie waarmee men in contact komt c.q. kan komen (waarde, vertrouwelijkheid, privacy-gevoeligheid, et cetera);
3. De soort toegang (fysiek, logisch, op locatie of op afstand, via internet of anders);
4. Benodigde middelen en inspanning, waaronder mogelijkheden tot afscherming en registratie, logging en monitoring;
5. Karakteristieken en kwaliteiten van de externe partij en type externe gebruiker, met inbegrip van door de externe partij ingestelde autorisatie en verdere getroffen maatregelen.

Toegang wordt pas verleend na formele goedkeuring van de Eigenaar, implementatie van alle geïdentificeerde, noodzakelijke maatregelen en het beschikbaar zijn van een rechtsgeldige overeenkomst. Daar waar nodig laat de Eigenaar zich adviseren door de ISO en/of ISM.

Bij beëindiging van de werkzaamheden dienen verantwoordelijke beheerders op last van de Eigenaar alle uitgegeven toegangsrechten direct in te trekken, zowel tot informatiesystemen als tot beveiligde ruimten. Alle verstrekte informatie (gegevens, documentatie, rapporten, et cetera) dient onmiddellijk te worden teruggevorderd of de externe partij dient schriftelijk te verklaren de verstrekte informatie direct na beëindiging van de werkzaamheden te vernietigen.

Voorbeelden van externe partijen zijn: toeleveranciers, overige samenwerkingspartners, dienstverlenende bedrijven, de huisaccountant, auditors, consultants, (tijdelijke krachten van) uitzendbureaus, et cetera. Voorbeelden van IT-voorzieningen zijn het intranet en de salarisadministratie.

6.2.2 Beveiliging behandelen in de omgang met klanten

Alle geïdentificeerde beveiligingseisen behoren te worden behandeld voordat klanten toegang wordt verleend tot de informatie of bedrijfsmiddelen van de organisatie.

Elke student, cursist, alumnus of gepensioneerde die gebruik zal maken van IT-voorzieningen van de instelling, ontvangt daarvoor een persoonsgebonden instellingsaccount en wordt uiterlijk bij aanvang van het gebruik door of namens de verantwoordelijke gemandateerde verzocht akkoord te gaan met de Acceptable Use Policy (AUP) en de ICT gedragsregels (10 gouden regels).

Op instellingsniveau worden onder verantwoordelijkheid van de ISO ten behoeve van eindgebruikers periodiek bewustwordingsactiviteiten op het gebied van informatiebeveiliging georganiseerd.

Bij overtredingen van de AUP kan de instelling sancties treffen.

6.2.3 Beveiliging behandelen in overeenkomsten met een derde partij

In overeenkomsten met derden waarbij toegang tot, het verwerken van, communicatie van of beheer van informatie of IT-voorzieningen van de organisatie, of toevoeging van producten of diensten aan IT-voorzieningen waarbij sprake is van toegang, behoren alle relevante beveiligingseisen te zijn opgenomen.

Overeenkomsten met derden worden in overleg met een juridisch deskundige en eventuele inbreng van de ISO onder supervisie van de (eind)verantwoordelijke manager c.q. Eigenaar opgesteld. Deze functionaris is hiermee de 'Contracteigenaar' en dient in de overeenkomst te worden vermeld als gemandateerde (namens de instelling). De Contracteigenaar is (eind)verantwoordelijk voor het opnemen van alle noodzakelijk geachte beveiligingsvoorwaarden en het beheer van de overeenkomst.

Zaken, waarover de Contracteigenaar afspraken in overeenkomsten met derden *moet* maken, zijn:

1. Geheimhouding en integriteit;
2. Aansprakelijkheid;
3. Recht op audit;
4. Sancties bij niet naleving van verplichtingen;
5. Beëindiging en heronderhandeling.

Zaken die de Contracteigenaar in overeenkomsten met derden *kan* behandelen, zijn:

1. Beschrijving van de diensten die beschikbaar moeten worden gesteld;
2. De noodzaak om risico's die met toegang gemoeid zijn te reduceren;
3. De motivatie om derden toegang te geven en restrisico's te accepteren;

4. Toegestane toegang en gebruik, inclusief tijdstippen voor toegang en bepalingen voor (of tegen) het kopiëren en/of openbaar maken van informatie;
5. Alle toegang die niet expliciet is toegestaan is verboden;
6. Duiding, autorisatie, beperking, privileges, opleiding en bewustwording van gebruikers en beheerders;
7. Toegangsmethode(n) inclusief beheer en gebruik van toegangscodes en wachtwoorden, het beheer van gebruikersaccounts en het intrekken van toegangsrechten;
8. Gebruikers- c.q. beheerderslijst en autorisatiematrix (overzicht van personen die bevoegd zijn de ter beschikking gestelde dienst te gebruiken, en wat hun rechten zijn ten aanzien van het gebruik).
   Als de gebruikersadministratie niet door de instelling plaatsvindt: de verplichting tot het bijhouden van een autorisatiematrix;
9. Documentatie;
10. Continuïteitsvoorzieningen;
11. Maatregelen voor de bescherming van informatie en bedrijfsmiddelen[5], inclusief verwijzingen naar procedures.
12. Beveiliging van de uitwisseling van informatie;
13. Beperkingen en verplichtingen die voortvloeien uit wet- en regelgeving;
14. Rapportage;
15. Toezicht op naleving, logging en monitoring;
16. Herroepen van toegang in geval van misbruik;
17. Wijziging(en), service window en verantwoordelijkheid voor onderhoud en beheer van hardware en software;
18. Beëindiging van het gebruik;
19. Melding, afhandeling en escalatie van (beveiligings-)incidenten;
20. Onderaanneming.

Afspraken dienen concreet en zoveel mogelijk toetsbaar te zijn. Als de derde partij persoonsgegevens zal verwerken, dient de Contracteigenaar in samenwerking met Inkoop, Judische Zaken en/of de Functionaris Gegevensbescherming zorg te dragen voor een bewerkersovereenkomst, zie paragraaf 15.1.4.

Als een derde partij zijn (leverings)voorwaarden wenst toe te passen, dient de Contracteigenaar alvorens met de voorwaarden in te stemmen de voorwaarden in samenwerking met de ISO te (laten) toetsen aan:

1. Informatiebeveiligingsdreigingen en -risico's voor de instelling en eventueel betrokken partijen (zoals: beïnvloeden de opgedrongen bepalingen de beveiliging van de instelling niet onnodig nadelig?);
2. Wet- en regelgeving (waaronder Wbp);
3. De Baseline IB;
4. Juridische Normenkaders voor de sector Onderwijs (zoals Juridisch Normenkader Cloud Services Hoger Onderwijs en Juridisch Normenkader Surf);
5. Toepasselijke best practices (zoals de ICT-beveiligingsrichtlijnen voor webapplicaties van het NCSC).

Als de derde partij geen of niet in voldoende mate gehoor geeft aan door de instelling als noodzakelijk bevonden aanpassingen[6], moeten voorafgaand aan bekrachtiging resterende risico's formeel worden gewogen, gerapporteerd en geaccepteerd door de (daartoe bevoegde) Eigenaar.

Medewerkers van gecontracteerde derden dienen via een individuele verklaring met boeteclausules te worden gehouden aan geheimhouding en integriteit. Werkzaamheden mogen niet eerder dan na ondertekening aanvangen.

De medewerker van een gecontracteerde derde partij, die gebruik zal maken van IT-voorzieningen van de instelling, ontvangt daarvoor een persoonsgebonden instellingsaccount en wordt uiterlijk bij aanvang van het gebruik door of namens de verantwoordelijke gemandateerde verzocht akkoord te gaan met de Acceptable Use Policy (AUP) en ICT gedragsregels (10 gouden regels).

Controle en beoordeling van dienstverlening door (medewerkers van) derden is een verantwoordelijkheid van de Contracteigenaar. Hij behoort te waarborgen dat de derde partij de voorwaarden van de overeenkomsten voor de informatiebeveiliging naleeft en informatiebeveiligingsincidenten en -problemen goed afhandelt. Hiertoe draagt hij zorg voor een goede relatie tussen de instelling en de dienstverlenende partij en verifieert hij steekproefsgewijs of afspraken worden nagekomen.

---

5 Zoals het verbreken van de verbinding tussen gekoppelde informatiesystemen.
6 Denk hierbij bijvoorbeeld aan (cloud-)diensten van Microsoft, Google en Amazon.

7 Beheer van bedrijfsmiddelen

7.1 Verantwoordelijkheid voor bedrijfsmiddelen

Doelstelling:
Bereiken en handhaven van een adequate bescherming van bedrijfsmiddelen van de organisatie.

7.1.1 Inventarisatie van bedrijfsmiddelen

Alle bedrijfsmiddelen behoren duidelijk te zijn geïdentificeerd en er behoort een inventaris van alle belangrijke bedrijfsmiddelen te worden opgesteld en bijgehouden.

Belangrijke bedrijfsmiddelen moeten worden geïdentificeerd, geregistreerd en gedocumenteerd.

Met betrekking tot de bedrijfsprocessen van de instelling en de informatievoorziening c.q. -verwerking houdt ICTS een overzicht bij van alle belangrijke informatiesystemen.

De ICT-infrastructuur wordt eveneens door ICTS centraal geregistreerd. Relevante middelen wordt centraal geregistreerd in een configuratiedatabase (CMDB).

7.1.2 Eigendom van bedrijfsmiddelen

Alle informatie en bedrijfsmiddelen die verband houden met IT-voorzieningen behoren een 'eigenaar' te hebben in de vorm van een aangewezen deel van de organisatie.

De voor de organisatie belangrijke IT-voorzieningen zoals (delen van) informatiesystemen en gegevensverzamelingen kennen een Eigenaar in de vorm van een formeel (eind)verantwoordelijk persoon.

Zie bijlage 1 voor een uitgebreide beschrijving van Eigenaarschap.

Directeur ICTS is Eigenaar van alle gemeenschappelijke ICT-infrastructuur (instellingsnetwerk, telefonie, et cetera) en een aantal generieke, instellingsbreed gebruikte informatiesystemen zoals de informatiesystemen voor Identity Management (het centrale IDM-systeem), kantoorautomatisering en e-mail.

ICTS onderhoudt een overzicht van formeel aangewezen eigenaren.

Een Eigenaar kan bijvoorbeeld op basis van een hoge integriteitseis besluiten tot vergaande invoervalidatie, stringente invoerprocedures en controles.

7.1.3 Aanvaardbaar gebruik van bedrijfsmiddelen

Er behoren regels te worden vastgesteld, gedocumenteerd en geïmplementeerd voor aanvaardbaar gebruik van informatie en bedrijfsmiddelen die verband houden met IT-voorzieningen.

Op de toegang door gebruikers tot de IT-voorzieningen van de instelling is de Acceptable Use Policy (AUP) van toepassing. De instelling vraagt van alle gebruikers dat men zich houdt aan het veilig gebruik zoals dat door ICTS is verwoord in AUP. Hiertoe behoort het veilig gebruik van onder meer:

1. Het instellingsnetwerk en toepassingen;
2. E-mail en internet;
3. Printers en multifunctionals;
4. Mobiele apparatuur (zoals laptops, tablets en smartphones;
5. Mobiele gegevensdragers (zoals USB-geheugensticks).

Onder gebruikers wordt in dit verband ten minste verstaan: aankomend studenten, studerenden, cursisten, alumni, en medewerkers.

Bij het verlenen van toegang aan gebruikers wordt door de verlener (i.c. de gemandateerde, zoals CSA, P&O) aan de betrokkene een exemplaar verstrekt van de AUP en de ICT gedragsregels, die deel uitmaakt van de AUP. Beiden zijn tevens beschikbaar via de website van de instelling. ICTS houdt de AUP en de ICT gedragsregels op het intranet up-to-date.

In het geval van andere personen dan medewerkers dienen deze gebruikers schriftelijk akkoord te gaan met de regels.

7.2 Classificatie van informatie

Doelstelling:
Bewerkstelligen dat informatie een geschikt niveau van bescherming krijgt.

7.2.1 Richtlijnen voor classificatie

Informatie behoort te worden geclassificeerd met betrekking tot de waarde, wettelijke eisen, gevoeligheid en onmisbaarheid voor de organisatie.

De instelling classificeert zowel informatie als informatiesystemen. De wijze van classificatie is gedocumenteerd[7].

7.2.2 Labeling en verwerking van informatie

Er behoren geschikte, samenhangende procedures te worden ontwikkeld en geïmplementeerd voor de labeling en verwerking van informatie overeenkomstig het classificatiesysteem dat de organisatie heeft geïmplementeerd.

De instelling kent geen voorschriften of procedures voor het labelen van informatie.

In beginsel dient alle informatie als ‘Intern’ te worden geclassificeerd en overeenkomstig te worden behandeld. De eigenaar van de informatie kan, als de situatie dat vereist, de rubricering aanpassen naar ‘Openbaar’ danwel ‘Vertrouwelijk’ of ‘Geheim’.

Hoe om te gaan per categorie informatie is weergegeven in de tabel Beveiligingseisen Verwerking Informatie in Bijlage 3. Voor de categorie ‘Openbaar’ zijn geen specifieke regels van kracht.

[7] Zie “UvA-HvA Classificatie Methodiek” dd. 18-08-2014.

8 Beveiliging van personeel

8.1 Voorafgaand aan het dienstverband

Doelstelling:
Bewerkstelligen dat werknemers, ingehuurd personeel en externe gebruikers hun verantwoordelijkheden begrijpen, en geschikt zijn voor de rollen waarvoor zij worden overwogen, en om het risico van diefstal, fraude of misbruik van faciliteiten te verminderen.

8.1.1 Rollen en verantwoordelijkheden

De rollen en verantwoordelijkheden van werknemers, ingehuurd personeel en externe gebruikers ten aanzien van beveiliging behoren te worden vastgesteld en gedocumenteerd.

De instelling verwacht in het algemeen van medewerkers en ingehuurd personeel, dat men:

1. Bijdraagt aan het verwezenlijken van hetgeen is vastgelegd in het Informatiebeveiligingsbeleid UvA-HvA en de Baseline IB UvA-HvA;
2. De bedrijfsmiddelen van de instelling behoedt tegen ongeoorloofde toegang, openbaarmaking, wijziging, vernietiging of verstoring;
3. Zorgvuldig om gaat met informatie (ontvangen) van derden (leveranciers, klanten, et cetera);
4. De diverse beveiligingsprocedures en -regels in acht neemt;
5. Toepasselijke wet- en regelgeving (zoals auteursrechtwetgeving en de WBP) in acht neemt;
6. (Potentiële) verstoringen, beveiligingsincidenten en risico's meldt conform de vastgestelde meldingsprocedure;
7. Verantwoordelijkheid neemt voor het eigen handelen en verantwoordelijkheden ook in acht neemt bij het werken buiten de normale kantooruren en/of buiten de bedrijfslocaties (zoals bij telewerken).

Onervaren medewerkers mogen alleen onder begeleiding en onder voorwaarden bedrijfskritische informatiesystemen bedienen. Alvorens systemen zelfstandig mogen worden bediend, dient de kennis en ervaring van medewerkers te worden beoordeeld en/of via opleiding/training op niveau te worden gebracht.

Bovenstaande taken en verantwoordelijkheden zijn algemeen van aard en van toepassing op alle medewerkers en ingehuurd personeel. Als een medewerker specifieke rollen of taken vervult of een specifieke verantwoordelijkheid ten aanzien van informatiebeveiliging draagt, ziet de leidinggevende er op toe dat dat wordt vastgelegd.

8.1.2 Screening

Verificatie van de achtergrond van alle kandidaten voor een dienstverband, ingehuurd personeel en externe gebruikers behoren te worden uitgevoerd overeenkomstig relevante wetten, voorschriften en ethische overwegingen, en behoren evenredig te zijn aan de bedrijfseisen, de classificatie van de informatie waartoe toegang wordt verleend, en de waargenomen risico's.

Voor aangestelde of gecontracteerde kandidaten die binnen de instelling als onderdeel van hun werk toegang zullen krijgen tot als vertrouwelijk of hoger geclassificeerde informatie, zorgt P&O voor tenminste de volgende controles:

1. Het opvragen van referenties bij tenminste twee voorgaande werkgevers (nabellen);
2. Het verifiëren van genoten opleidingen, via het opvragen van de originelen van diploma's, certificaten, et cetera en, zo nodig het bellen van betrokken opleiders;
3. Het controleren van een origineel identiteitsbewijs (geen kopie);
4. Een VOG (verklaring omtrent gedrag), profiel onderwijs.

Bovenstaande geldt tevens voor freelancers, ZZP'ers, et cetera. Voor overig ingehuurd personeel geldt dat de leverancier (detacheerder, uitzendbureau) in moet staan voor de juistheid van de gegevens verstrekt over kandidaten.

8.1.3 Arbeidsvoorwaarden

Als onderdeel van hun contractuele verplichting behoren werknemers, ingehuurd personeel en externe gebruikers de algemene voorwaarden te aanvaarden en te ondertekenen van hun arbeidscontract, waarin

hun verantwoordelijkheden en die van de organisatie ten aanzien van informatiebeveiliging behoren te zijn vastgelegd.

De Arbeidsvoorwaarden van de instelling bevatten een paragraaf inzake geheimhouding en integriteit, en een sanctieregeling. Voor medewerkers van ICTS is daarnaast een Integriteitsverklaring van kracht.

De afdeling Inkoop ziet er op toe dat ook in inhuur-contracten de hierboven genoemde bepalingen inzake geheimhouding, integriteit en sancties zijn opgenomen. Ingehuurd personeel dient een aparte geheimhoudings- en integriteitsverklaring te ondertekenen. Waar nodig, dienen verantwoordelijkheden na beëindiging van het dienstverband of de inhuur nog een vastgestelde periode van kracht te blijven.

Naast bepalingen in de arbeidsovereenkomst, contracten en de geheimhoudings- en integriteitsverklaring voor externen is met betrekking tot informatiebeveiliging het een en ander opgenomen in de Acceptable Use Policy (AUP) en de ICT-gedragsregels (10 gouden regels).

Elke medewerker, ingehuurd persoon en klant (student, cursist, alumni, scholier of gepensioneerde) die gebruik zal maken van IT-faciliteiten van de instelling, ontvangt daarvoor een persoonsgebonden instellingsaccount en wordt uiterlijk bij aanvang van het gebruik door of namens de verantwoordelijke gemandateerde verzocht akkoord te gaan met de Acceptable Use Policy (AUP) en de ICT-gedragsregels.

De instelling wil met deze beheersmaatregel waarborgen dat medewerkers en ingehuurd personeel instemmen met afspraken die passend zijn voor de toegang die men heeft tot de bedrijfsmiddelen van de instelling, waaronder informatie en informatiesystemen.

Van de instelling mag worden verwacht dat zij zorgzaam omgaat met en verantwoordelijkheid draagt voor het verwerken van persoonlijke informatie van medewerkers en ingehuurd personeel, waaronder persoonlijke informatie gecreëerd als resultaat van of gedurende het dienstverband met de instelling.

P&O draagt zorg voor de invulling van deze beheersmaatregel en is eigenaar van de Arbeidsvoorwaarden, de Geheimhoudings- en Integriteitsverklaring Externen en de sanctieregeling.

ICTS is primair aanspreekpunt voor de Acceptable Use Policy en de ICT-gedragsregels.

8.2 Tijdens het dienstverband

Doelstelling:
Bewerkstelligen dat alle werknemers, ingehuurd personeel en externe gebruikers zich bewust zijn van bedreigingen en gevaren voor informatiebeveiliging, van hun verantwoordelijkheid en aansprakelijkheid, en dat ze zijn toegerust om het beveiligingsbeleid van de organisatie in hun dagelijkse werkzaamheden te ondersteunen, en het risico van een menselijke fout te verminderen.

8.2.1 Directieverantwoordelijkheid

De directie en het management behoort van werknemers, ingehuurd personeel en externe gebruikers te eisen dat ze beveiliging toepassen overeenkomstig vastgesteld beleid en vastgestelde procedures van de organisatie.

De leidinggevende is verantwoordelijk voor het uitvoeren en controleren van de naleving van procedures en regels binnen het eigen team c.q. binnen de eigen afdeling. Tot de verantwoordelijkheden van het CvB en leidinggevenden behoort dat medewerkers en ingehuurd personeel:

1. Goed zijn ingelicht over hun rollen, taken en -verantwoordelijkheden aangaande de beveiliging van informatie en informatiesystemen en de voor hen toepasselijke stukken tekenen voordat men toegang krijgt tot vertrouwelijke of hoger geclassificeerde informatie en/of bedrijfskritische informatiesystemen;
2. (Blijvend) weten welk gedrag, houding en handelingen de organisatie van hen verwacht inzake informatiebeveiliging;
3. Gemotiveerd zijn om zich aan het beleid en de procedures en regels van de instelling te houden;
4. Vaardigheden en kwalificaties aangaande de beveiliging van informatie en informatiesystemen blijven houden.
5. Voor specifieke (beveiligings-)functies: De mogelijkheid hebben een zodanig niveau van vaardigheid en (veiligheids-)bewustzijn verwerven, als vereist is voor de uitoefening van hun functie.

Het verantwoordelijke management handelt schending van procedures en regels af conform de sanctieregeling van de instelling, indien nodig met betrokkenheid van Juridische Zaken (JZ).

8.2.2 Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging

Alle werknemers van de organisatie en, voor zover van toepassing, ingehuurd personeel en externe gebruikers, behoren geschikte training en regelmatige bijscholing te krijgen met betrekking tot beleid en procedures van de organisatie, voor zover relevant voor hun functie.

Op instellingsniveau worden onder verantwoordelijkheid van de ISO regelmatig terugkerende bewustwordingsactiviteiten op het gebied van informatiebeveiliging georganiseerd gericht op medewerkers, ingehuurd personeel, studenten, cursisten, alumni, scholieren, gepensioneerden en gasten.

De ISO organiseert tenminste eenmaal per jaar een gerichte bewustzijnsactie. Verder kan hij leidinggevenden ondersteunen bij specifieke bewustwordingsactiviteiten en middelen ter beschikking stellen.

De leidinggevende dient periodiek na te gaan of voor medewerkers die een bijzondere taak vervullen aangaande informatiebeveiliging extra scholing benodigd is.

Beveiligingsbewustzijn is een van de onderwerpen van de jaarlijkse planning & control cyclus.

8.2.3 Disciplinaire maatregelen

Er behoort een formeel disciplinair proces te zijn vastgesteld voor werknemers die inbreuk op de beveiliging hebben gepleegd.

Juridische Zaken (JZ) vervat het formele disciplinaire proces in een uitgeschreven sanctieregeling.

Het formele disciplinaire proces moet waarborgen dat medewerkers die worden verdacht van inbreuk op de beveiliging een correcte en eerlijke behandeling krijgen. Er wordt voorzien in een getrapte aanpak die rekening houdt met factoren als:

1. Aard en ernst van de inbreuk en de gevolgen ervan voor de instelling;
2. Of het de eerste overtreding is of een herhaalde inbreuk;
3. Of degene die inbreuk heeft gepleegd correct was geïnformeerd of getraind.

Hierbij wordt waar nodig rekening gehouden met relevante wetgeving, zakelijke contracten en eventuele andere factoren.

Bij ernstige gevallen van inbreuk behoort het proces te voorzien in onmiddellijke schorsing, ontnemen van toegangsrechten en speciale bevoegdheden, en indien nodig het onmiddellijk verwijderen uit de locatie. Het disciplinaire proces behoort evenwel niet te worden gestart zonder voorafgaande verificatie dat zich een inbreuk op de beveiliging heeft voorgedaan.

De leidinggevende is verantwoordelijk voor het uitvoeren en controleren van de naleving van procedures en regels binnen het eigen team c.q. de eigen afdeling.

8.3 Beëindiging of wijziging van dienstverband

Doelstelling:
Bewerkstelligen dat werknemers, ingehuurd personeel en externe gebruikers ordelijk de organisatie verlaten of hun dienstverband wijzigen.

8.3.1 Beëindiging van verantwoordelijkheden

De verantwoordelijkheden voor beëindiging of wijziging van het dienstverband behoren duidelijk te zijn vastgesteld en toegewezen.

De instelling kent verschillende 'exit' procedures, met voor elke procedure een overzicht van bij wie binnen de organisatie welke actie ligt als een medewerker ontslag neemt (of met pensioen gaat), de werkzaamheden van een ingehuurd persoon beëindigd worden of wanneer een student afstudeert of te kennen geeft zijn studie te willen beëindigen.

De instelling kent een aparte procedure voor wijziging van functie, met aandacht voor het inleveren van aangereikte middelen van de instelling en het intrekken van rechten op informatiesystemen.

Beëindiging van dienstverband met medewerker en werkzaamheden ingehuurde personen
P&O is eigenaar van en verantwoordelijk voor de beëindigings- en wijzigingsprocedure voor medewerkers en ingehuurde personen. Ze werkt daarbij nauw samen met de directe leidinggevende van de persoon die vertrekt, ter waarborging van de zorgvuldige uitvoering van de diverse benodigde acties.

Het vertrek van een medewerker of ingehuurd persoon dient tijdig door de leidinggevende naar alle medewerkers te worden gecommuniceerd die weet van dit feit moeten hebben.

Tijdens een exitgesprek dient de direct leidinggevende de vertrekkende medewerker of ingehuurd persoon te wijzen op het van kracht blijven van afspraken zoals geheimhouding.

Voor vroegtijdige beëindiging van het dienstverband van een medewerker of de inzet van een ingehuurd persoon op initiatief van de instelling is door P&O een aparte procedure opgesteld, met inbegrip van aspecten die vanuit het oogpunt van informatiebeveiliging aandacht dienen te krijgen.

Leidinggevenden zijn verantwoordelijk voor het op de hoogte brengen van relevante externe partijen van ingetrokken bevoegdheden.

Bij wijziging van functie
Leidinggevenden zijn verantwoordelijk voor het op de hoogte brengen van relevante externe partijen van ingetrokken bevoegdheden.

Na afloop van de studie door student
De Centrale Studenten Administratie (CSA) is eigenaar van en verantwoordelijk voor de beëindigings- en wijzigingsprocedure voor studenten. Zie verder paragrafen 8.3.2 en 8.3.3.

8.3.2 Retournering van bedrijfsmiddelen

Alle werknemers, ingehuurd personeel en externe gebruikers behoren alle bedrijfsmiddelen van de organisatie die ze in hun bezit hebben te retourneren bij beëindiging van hun dienstverband, contract of overeenkomst.

De instelling hanteert een checklist voor het retourneren van alle bedrijfsmiddelen die medewerkers en ingehuurd personeel in bruikleen kunnen hebben, zoals sleutels, passen/tokens, laptop, smartphone, tablet, bedrijfsdocumenten, software, et cetera. P&O is eigenaar van de retourneer-checklist.

De direct leidinggevende is verantwoordelijk voor het invorderen van de betreffende zaken en zorgt voor het terugbezorgen van de middelen bij de betreffende eigenaar binnen de instelling.

Wanneer een medewerker of ingehuurd personeel beschikt over kennis die belangrijk is voor de lopende bedrijfsvoering, dient de directe leidinggevende er op toe te zien dat die informatie wordt gedocumenteerd en overgedragen aan de organisatie.

Bij ingehuurde personen dienen daarnaast alle verstrekte gegevens, resultaten, constructies, rapporten, documentatie en daarin vervatte informatie onmiddellijk te worden teruggevorderd of dient de ingehuurde persoon (of zijn werkgever) schriftelijk te verklaren alle verstrekte informatie(dragers) direct na beëindiging van de werkzaamheden te vernietigen.

Als een vertrekkende medewerker of ingehuurd persoon privé apparatuur voor werkzaamheden heeft gebruikt of apparatuur van de organisatie tegen betaling wenst over te nemen, dient een procedure er voor te zorgen dat alle relevante informatie wordt overgedragen aan de instelling en nauwkeurig wordt gewist van de apparatuur.

8.3.3 Blokkering van toegangsrechten

De toegangsrechten van alle werknemers, ingehuurd personeel en externe gebruikers tot informatie en IT voorzieningen behoren te worden geblokkeerd bij beëindiging van het dienstverband, het contract of de overeenkomst, of behoort na wijziging te worden aangepast.

Beëindiging van dienstverband met medewerker en werkzaamheden ingehuurde personen
Bij beëindiging van het dienstverband met een medewerker of van de werkzaamheden van een ingehuurd persoon, dienen de verantwoordelijke beheerders alle toegangsrechten van de betreffende medewerker in principe direct (of anders zo snel als toepasselijk) in te trekken, zowel tot informatiesystemen als tot beveiligde ruimten. Bij informatiesystemen geldt dit onder meer voor de e-mailvoorziening, opslag en bedrijfstoepassingen. Bij ruimten geldt dit voor Zone 1 en hoger ruimten, zie paragraaf 9.1.1.

De instelling streeft er naar het intrekken van toegangsrechten zo veel mogelijk geautomatiseerd te laten verlopen (als waarborg voor het tijdig intrekken).

Als de vertrekkende persoon (mede) kennis van wachtwoorden heeft voor accounts die actief dienen te blijven, zoals niet-persoonsgebonden accounts, dienen deze wachtwoorden tijdig te worden gewijzigd.

Na afloop van de studie door student
Bij beëindiging van de studie dienen alle toegangsrechten, zowel tot informatiesystemen als beveiligde ruimten, van de betreffende student in principe direct (of anders zo snel als toepasselijk) worden ingetrokken.

Bij wijziging van functie
Na een wijziging van functie behoren de fysieke en logische toegangsrechten te worden aangepast, zowel voor vaste medewerkers als voor ingehuurde personen. Alle oude toegangsrechten worden ingetrokken en de nieuwe leidinggevende autoriseert nieuwe toegangsrechten en vraagt deze aan.

Als een persoon die van functie verandert kennis heeft van wachtwoorden voor accounts die hij/zij voor de uitoefening van de nieuwe functie niet langer nodig heeft, dienen de wachtwoorden van deze accounts te worden gewijzigd.

9 Fysieke beveiliging en beveiliging van de omgeving

9.1 Beveiligde ruimten

Doelstelling:
Het voorkomen van onbevoegde fysieke toegang tot, schade aan of verstoring van het terrein en de informatie van de organisatie.

9.1.1 Fysieke beveiliging van de omgeving

Er behoren toegangsbeveiligingen (barrières zoals muren, toegangspoorten met kaartsloten of een bemande receptie) te worden aangebracht om ruimten te beschermen waar zich informatie en IT-voorzieningen bevinden.

Zonering
De instelling hanteert de volgende indeling in zones:

Zone 0: Publieke Algemene Verkeersruimte
Deze bestaat uit de ruimtes binnen een gebouw of voorziening die toegankelijk zijn voor iedereen, zonder autorisatie, binnen de vastgestelde openingstijden;

Zone 1: Instellings Algemene Verkeersruimte
Betreft de ruimtes die toegankelijk zijn voor iedereen met een geldige college- medewerkers- of bezoekerskaart.

Zone 2: Algemene leer- en werkzone
Betreft onderwijsruimtes, projectruimtes en generieke flex/werkplekken en is toegankelijk voor alle medewerkers met een geldige medewerkerkaart en specifiek hiervoor geautoriseerde studenten met een geldige collegekaart.

Zone 3: Specifieke werkruimtes
Betreft ruimtes (zoals kantoren) die toegankelijk zijn voor individuele of groepen medewerkers, of studenten die gedurende een langere periode (bijvoorbeeld de duur van aanstelling of opdracht) specifiek voor de betreffende ruimte(s) zijn geautoriseerd.

Zone 4: Kritische ruimtes
Betreft ruimtes die toegankelijk zijn voor individuele of groepen medewerkers of studenten die specifiek voor de betreffende ruimtes zijn geautoriseerd en die vanwege hun aard, functie of doel een hoger beveiligingsniveau en/of specifieke autorisatie procedure vereisen.

Zone T:
Betreft de technische ruimtes, liftschachten, kasten met meetapparatuur e.d., die in beheer zijn van FS én die niet afgesloten zijn met een SALTO slot.

Algemeen
Met betrekking tot de gebouwen van de instelling en zonering zijn de volgende algemene richtlijnen van kracht:

1) De buitenschil[8] is voorzien van een gecertificeerd inbraak- en brandalarm met afdoende detectie en alarmering. Ramen aan de buitenzijde op de begane grond en eerste etage zitten in principe op slot en zijn voorzien van inbraakmelders.
2) Online sloten worden altijd toegepast op kritieke punten waarbij zekerheid is vereist dat de laatste revisie op de toegangsrechten ter plaatse beschikbaar is. Hieronder vallen in ieder geval alle buitendeuren (sloten harde buitenschil).
3) Buiten de openingstijden gaan alle deuren van het pand op slot. De buitenschil is buiten de openingstijden alleen toegankelijk voor beveiligers, en voor overige medewerkers en personen in principe onder begeleiding van een beveiliger; <Anders dan de praktijk?: je moet nu aangeven wanneer en waar je wilt overwerken, de deur wordt dan op afstand gepend en vervolgens sta je alleen binnen …?>
4) De Hoofdgebruiker[9] autoriseert voor de buitenschil. Het invoeren van buitenschilautorisaties is voorbehouden aan Functioneel Beheer van het Elektronische Toegangscontrolesysteem (ETCS), om redenen van de beheersbaarheid van de uitgifte van dit soort kritische autorisaties;

---

[8] Met buitenschil wordt bedoeld alle deuren, poorten en overige sluitingsmechanismen die in hun totaliteit de fysieke grens vormen tussen de binnenruimte van een gebouw en de buitenruimte.
[9] Het instellingsonderdeel met de meeste gebruikers in het gebouw is ‘Hoofdgebruiker’.

5) Gedurende openingstijden wordt de fysieke toegang tot het gebouw mede met behulp van een bemenste receptie beheerst;
6) Per gebouw is voor ruimten in Zone 2 en hoger een specifieke bezoekersregeling van kracht. De ontvangende medewerker (gastheer/gastvrouw) moet zijn bezoeker(s) van tevoren aan melden bij de receptie. De receptie voorziet bezoekers van een bezoekersbadge en schrijft hen in en na afloop weer uit. Bezoekers dienen de bezoekersbadge zichtbaar te dragen. De ontvangende medewerker dient de bezoeker(s) doorlopend te begeleiden.
7) De zonegrenzen dienen te zijn gemarkeerd en te worden gecontroleerd. De exacte wijze van controle van zonegrenzen wordt per gebouw op basis van risicoanalyse vastgesteld;
8) Per gebouw is een sluitplan vastgesteld met:
   a) een kruistabel met toegangsrechten voor medewerkers conform het format van Functioneel Beheer (FB) die de toegang specificeert voor zone 3 en 4;
   b) zone-indeling zone 1 en 2;
   c) de wijze van controle en monitoring van zonegrenzen;
   d) de openingsstanden van de sloten;
   e) paragraaf calamiteitenbeheer.
9) Voor elk gebouw is de Hoofdgebruiker verantwoordelijk voor het vaststellen van het sluitplan.
10) De directeur van Facility Services (FS) is eigenaar van de dienst 'Toegang' en het Elektronische Toegangscontrolesysteem (ETCS), verantwoordelijk voor het technisch en functioneel beheer van dit systeem, en ziet toe op naleving van gebruik van het systeem conform beleid.
1) De instelling huisvest kritische bedrijfsmiddelen, zoals belangrijke ICT-infrastructuur en archieven, in Zone 4 en/of Zone T ruimten (denk aan MER/SER[10] en archiefruimten).

Zone 4 ICT-ruimten
Zone 4 ICT-ruimten dienen te voldoen aan de volgende richtlijnen:

1. De organisatorische eenheid die de betreffende ruimte in gebruik heeft stelt een eigenaar/beheerder aan, bij wie de autorisatie voor toegang is belegd;
2. De ruimte grenst niet aan een Zone 0 of 1 ruimte;
3. De fysieke grenzen moeten duidelijk worden gedefinieerd (in de administratieve zin) maar behoeven niet als zodanig zichtbaar te zijn;
4. De fysieke toegang wordt beheerst met verstevigde toegangsdeuren met sloten en anti-inbraakstrips, secustrips. Deurscharnieren zijn voorzien van dievenklauwen. De inbraakwering voldoet tenminste aan SKG-klasse II. De toegang wordt gedetecteerd met magneetcontacten op de toegangsdeuren die via het GBS-systeem aangesloten zijn op de meldkamer van de instelling.
5. MER/SER en andere ICT-ruimten zijn voorzien van toegangscontrole met cameraregistratie, noodverlichting, adequate brandbestrijdingsmiddelen, klimaatbeheersing en UPS;
6. Toegepaste brandbestrijdingsmiddelen dienen in lijn te zijn met wet- en regelgeving en de plaatselijke brandvoorschriften. Blusmiddelen dienen zo minimaal mogelijk schade aan aanwezige systemen of archieven te veroorzaken;
7. Branddeuren behoren te zijn voorzien van een alarm, te worden gecontroleerd en getest in combinatie met de muren, om overeenkomstig nationale, regionale of internationale normen het vereiste brandwerendheid niveau vast te stellen; ze behoren volgens de plaatselijke brandvoorschriften faalveilig te functioneren;
8. In serverruimten of ruimten met papieren archieven heerst een constante temperatuur (18-20 graden Celsius en maximaal 30 graden Celsius) en luchtvochtigheid (50-55%, tenminste 30% en maximaal 70%);
9. Aanwezige apparatuur voor klimaatbeheersing is voorzien van een temperatuur- en vochtigheidsalarm. Bij afwijkingen onderneemt de beheerder correctieve actie;
10. Aanbevolen wordt aan te sluiten bij de eisen zoals die worden gegeven door de Nederlandse Praktijk Richtlijn voor Computerruimtes en Datacenters (NPR 5313 Computerruimtes en datacenters);
11. Er mogen geen water-, gas- of elektriciteitsleidingen door of vlak boven Zone 4 ICT-ruimten lopen, anders dan welke nodig zijn voor voorzieningen in de ruimte zelf. Als dit onvermijdelijk is (bijvoorbeeld in bestaande bouw) dient de beheerder de aanwezigheid en locatie van leidingen duidelijk te (laten) documenteren en markeren.
12. ICT-voorzieningen of archieven die ICTS zelf beheert, moeten fysiek zijn gescheiden van systemen die door derden worden beheerd.

9.1.2 Fysieke toegangsbeveiliging

Beveiligde zones behoren te worden beschermd door geschikte toegangsbeveiliging, om te bewerkstelligen dat alleen bevoegd personeel wordt toegelaten.

[10] Main Equipment Room / Satellite Equipment Room.

Inzake het Elektronische ToegangsControleSysteem (ETCS) SALTO is het toegangsbeheer verwoord in het document 'Toegangsbeheer UvA/HvA' (huidige versie: 1.6 dd. 20 november 2012).

De instelling beperkt en beheerst de toegang tot ruimten in Zone 2 en hoger tot geautoriseerde personen.

De instelling maakt gebruik van een elektronisch toegangscontrolesysteem (ETCS) voor het beheersen van de toegang tot ruimten in Zone 2 en hoger. Facility Services (FS) voert het technisch en functioneel beheer uit voor dit systeem en reikt legitieme eindgebruikers (studenten/medewerkers) de persoonsgebonden kaart[11] aan (creditcard formaat). Organisatorische eenheden (domeinen, faculteiten, ICTS, et cetera) zijn verantwoordelijk voor het autoriseren van toegang en het activeren en intrekken van rechten verbonden aan de kaart.

In Zone 1 of hoger zijn eindgebruikers verplicht een geldige kaart bij zich te hebben en zich te kunnen legitimeren op verzoek van een beveiligingsmedewerker of bij servicebalies. Er geldt geen draagplicht.

Het is de eindgebruiker niet toegestaan zijn kaart uit te lenen.

BHV
BHV-medewerkers hebben uitsluitend in de rol van BHV'er (het recht op) toegang tot alle panden en ruimten, behalve tot ruimten die hiervan expliciet worden uitgesloten. Dit is vastgelegd in het sluitplan.

Tot de verantwoordelijkheden van (Campus) Hoofd BHV behoren:

1. Het toekennen en administreren van toegangsrechten aan BHV-medewerkers;
2. Het intrekken van toegangsrechten zodra deze niet langer nodig zijn;
3. Waarborgen beveiligingsbewustzijn BHV-ers.

Zone 4 ruimten
1. Medewerkers krijgen via de leidinggevende toegangsrechten tot Zone 4 ruimten op basis van het "need to be" principe;
2. De toegang tot Zone 4 ruimten is uitsluitend voorbehouden aan geautoriseerde medewerkers;
3. De leidinggevende beoordeelt de toegangsrechten van zijn medewerkers tenminste ieder kwartaal en laat deze zonodig onmiddellijk door de betreffende eigenaar/beheerder intrekken;

9.1.3 Beveiliging van kantoren, ruimten en faciliteiten

Er behoort fysieke beveiliging van kantoren, ruimten en faciliteiten te worden ontworpen en toegepast.

De toegang tot werkruimten, waar met als vertrouwelijk of hoger geclassificeerde informatie wordt gewerkt, dient te zijn beveiligd. Deze ruimten moeten voorzien zijn van afsluitbare opbergmiddelen met een toereikende capaciteit. De afscherming van een werkruimte of opbergmiddel hoeft niet zodanig zwaar te worden uitgevoerd dat onbevoegde toegang onmogelijk is, maar is bedoeld om te zorgen dat ongeautoriseerde toegang niet kan geschieden zonder duidelijke sporen van braak.

Medewerkers moeten over afdoende bergmiddelen beschikken om gegevensdragers met vertrouwelijke gegevens (zowel op papier als in digitale vorm) veilig op te kunnen bergen.

Gevaarlijke of brandbare materialen en voorraden moeten op een veilige afstand van Zone 4 ruimten worden opgeslagen.

De speciale bedrijfsruimten van de instelling (zoals MER/SER en opslagruimten) mogen niet zijn voorzien van een aanduiding die wijst op het gebruiksdoel van de ruimte en de aanwezigheid van bijzondere informatie of bedrijfsmiddelen.

Om redenen van brandveiligheid mogen branddeuren niet onnodig open staan.

Voor zover beveiliging van ruimten en faciliteiten onderdeel is van dienstverlening door derden (zoals data-center faciliteiten) maakt de instelling formele afspraken met de dienstverlener inzake de invulling van deze dienstverlening.

---

[11] De kaart biedt toegang tot ruimten die beveiligd zijn met toegangscontrolesystemen TiSM of SALTO. Er zijn vier kaartprofielen, te weten: college-, medewerker-, tijdelijke en bezoekerskaart. Voor studenten is het de collegekaart die ook dienst doet als educatief legitimatiebewijs. Voor medewerkers is de kaart het instellingslegitimatiebewijs.

9.1.4 Bescherming tegen bedreigingen van buitenaf

Er behoort fysieke bescherming tegen schade door brand, overstroming, aardschokken, explosies, oproer en andere vormen van natuurlijke of menselijke calamiteiten te worden ontworpen en toegepast.

De bedrijfsruimten van de instelling zijn zover als nodig beveiligd tegen braak, brand en wateroverlast. De braakwerendheid en alarmering is zodanig dat de mogelijkheid van diefstal van bedrijfskritische middelen zeer beperkt is. Afdoende brandmelders en blusmiddelen dienen voorhanden te zijn.

Reserveapparatuur wordt op tenminste 5 km afstand bewaard om te voorkomen dat deze beschadigd raakt of niet toegankelijk is door een calamiteit op de locatie.

De locatie van Zone 4 ruimten dient zo gekozen te worden dat de kans op schade door bedreigingen van buitenaf, zoals brand, overstroming, molest, et cetera minimaal is. Dit houdt in:

1. Boven straatniveau en, indien realiseerbaar, boven NAP;
2. Niet grenzend aan straatzijde of een Zone 0 of 1 ruimte ;
3. Niet in de nabijheid van een ruimte waar erg brandbare of anderszins gevaarlijke materialen worden opgeslagen. Hier dient bij de inrichting naar gekeken te worden. De wenselijke afstand is afhankelijk van het soort materiaal dat opgeslagen ligt, maar is zeker niet aangrenzend;
4. Niet in de directe nabijheid en zeker niet onder “natte” ruimten, zoals bijvoorbeeld toiletgroepen. Als dit onvermijdelijk is, dienen aanvullende maatregelen genomen te worden om schade door vocht of overstroming te voorkomen. Denk dan aan veel vrije ruimte onder de verhoogde vloer (dus geen stopcontacten op de ondervloer) en/of een extra overkapping over kasten of racks zodat eventueel van boven instromend water gekanaliseerd wordt.

De instelling treft geen bijzondere maatregelen om schade door explosies, extreme wateroverlast, aardschokken, oproer of andere vormen van natuurlijke of door mensen veroorzaakte calamiteiten te voorkomen (ze vormen hiermee een geaccepteerd risico).

9.1.5 Werken in beveiligde ruimten

Er behoren een fysieke bescherming en richtlijnen voor werken in beveiligde ruimten te worden ontworpen en toegepast.

Datacenter-, server-, patchruimten, MER/SER, et cetera, worden aangemerkt als Zone 4 ICT-ruimten. Bevoegde medewerkers mogen zonder toezicht in deze ruimten werken.

Het betreden van Zone 4 ruimten dient tot een minimum te worden beperkt. Deze ruimten mogen alleen worden betreden als ter plekke werkzaamheden noodzakelijk zijn. Registratie van genoten/verleende toegang is verplicht.

Voor werkzaamheden in Zone 4 ruimten gelden tenminste de volgende regels:

1. Toegangsrechten worden alleen verkregen van de beheerder van de ruimte na autorisatie door de leidinggevende;
2. Bij het als laatste verlaten van de ruimte dient de ruimte afgesloten te worden (ook als het voor korte duur is);
3. Ruimten dienen schoon te worden gehouden en mogen niet worden gebruikt voor opslag van goederen;
4. Eventuele onrechtmatigheden (sporen van braak, vocht, niet functionerende airconditioning, enzovoorts) dienen direct te worden gemeld aan de beheerder;
5. Eventueel in de ruimte ter kennisgeving opgehangen aanvullende regels dienen stipt te worden opgevolgd.

Naast een eet-, drink- en rookverbod zijn verder geen bijzondere voorschriften of regels van kracht.

Derden
Toegang tot de serverruimte door derden vindt alleen onder begeleiding van bevoegde medewerkers plaats. Het is hierbij aan de beheerder om te beoordelen of continue begeleiding noodzakelijk is.

9.1.6 Openbare toegang en gebieden voor laden en lossen

Toegangspunten zoals gebieden voor laden en lossen en andere punten waar onbevoegden het terrein kunnen betreden, behoren te worden beheerst en indien mogelijk worden afgeschermd van IT voorzieningen, om onbevoegde toegang te voorkomen.

Goederen dienen door leveranciers altijd bij de receptie te worden afgegeven en door de interne afnemer naar de juiste plek in het gebouw te worden gebracht, nimmer door de leverancier. Als wegens bijzondere omstandigheden laden en/of lossen niet op deze wijze kan plaatsvinden, dient de derde partij bij het laden en/of lossen doorlopend te worden begeleid.

9.2 Beveiliging van apparatuur

Doelstelling:
Het voorkomen van verlies, schade, diefstal of compromittering van bedrijfsmiddelen en onderbreking van de bedrijfsactiviteiten.

9.2.1 Plaatsing en bescherming van apparatuur

Apparatuur behoort zo te worden geplaatst en beschermd dat risico's van schade en storing van buitenaf en de gelegenheid voor onbevoegde toegang wordt verminderd.

ICTS is verantwoordelijk voor de plaatsing van IT-systemen (servers, desktops, et cetera). Als een leverancier de plaatsing verzorgt, maakt ICTS afspraken met de leverancier over de montage en overige werkzaamheden.

Apparatuur en systemen, welke niet bedoeld zijn voor persoonsgebonden gebruik, zoals servers en netwerkcomponenten dienen te worden geplaatst in speciaal daartoe ingerichte, beveiligde ruimten, zoals serverruimtes. Voor plaatsing van de apparatuur in deze ruimten gelden vastgestelde richtlijnen van ICTS. Standaard dienen systemen in afsluitbare 19” racks te worden gemonteerd.

9.2.2 Nutsvoorzieningen

Apparatuur behoort te worden beschermd tegen stroomuitval en andere storingen door onderbreking van nutsvoorzieningen.

Voor server- en datacomruimten geldt dat voorzien moet zijn in een deugdelijke energievoorziening. Iedere kast moet voorzien zijn van een stroomvoorziening met een capaciteit die toereikend is voor de in de kast geïnstalleerde apparatuur. Voor bedrijfskritische systemen dient de stroomvoorziening dubbel uitgevoerd te worden middels twee voedingslijnen uit verschillende schakelkasten.

Alle apparatuur in de serverruimte is aangesloten op een UPS. De UPS is met name bedoeld om te beschermen tegen kortstondige stroomuitval ('spanningsdip') en 'vuile' stroom. Om systemen gecontroleerd af te kunnen sluiten (‘graceful shutdown’) dienen UPS-en voldoende capaciteit te hebben om stroomonderbrekingen van tenminste een half uur op te vangen.

Met uitzondering van kleinere datacomruimten dienen serverruimten te zijn voorzien van een noodstroomvoorziening welke, zonder menselijke tussenkomst, tenminste een onderbreking van 24 uur kan overbruggen. De benodigde capaciteit is sterk afhankelijk van het beoogde gebruiksdoel van de ruimte en zal tijdens het inrichtingstraject moeten worden geraamd. Stroomonderbrekingen die langer dan 24 uur duren vormen een geaccepteerd risico.

ICTS bewaakt het functioneren en de belasting van UPS-en en noodstroom (in het kader van capaciteitsmanagement).

UPS-en en noodstroomvoorzieningen worden onderhouden en tenminste éénmaal per jaar nagelopen op correct functioneren.

Verder, ter waarborging van 1) het correct functioneren en 2) het aanwezig zijn van voldoende vaardigheden in de organisatie:

1. Laten betrokken beheerders de noodstroomvoorziening maandelijks proefdraaien;
2. Wordt jaarlijks een algehele stroomuitval nagebootst welke langer dan 1 uur duurt.

Betrokkenen doen hiervan verslag.

Voor zover bescherming van uitval van of storingen in nutsvoorzieningen onderdeel is van dienstverlening door derden maakt de instelling formele afspraken met de dienstverlener inzake de invulling van deze beheersmaatregel.

9.2.3 Beveiliging van kabels

Voedings- en telecommunicatiekabels die voor dataverkeer of ondersteunende informatiediensten worden gebruikt, behoren tegen interceptie of beschadiging te worden beschermd.

Bekabeling wordt conform de norm NEN 1010:2007+C1:2008 aangelegd en onderhouden. Elektriciteits- en telecommunicatiekabels worden beschermd door stevige kabelgoten. LAN- en telefoniebekabeling wordt veilig weggewerkt, onder meer in kabelgoten.

Bekabeling die niet of niet langer in gebruik is, moet losgekoppeld zijn van netwerkapparatuur.

Van zowel de bekabeling in de technische ruimten (zoals patch- en serverruimten) als naar de werkplekken houdt ICTS een administratie bij.

Voor zover bekabeling onderdeel is van dienstverlening door derden maakt de instelling formele afspraken met de dienstverlener inzake de invulling van deze beheersmaatregel.

9.2.4 Onderhoud van apparatuur

Apparatuur behoort op correcte wijze te worden onderhouden, om te waarborgen dat deze voortdurend beschikbaar is en in goede staat verkeert.

Vanwege het redundant uitvoeren van de IT-infrastructuur gelden voor onderhoud en reparatie niet de hoogste eisen. Een normaal niveau is toereikend; 'goud' of 'platina' is niet vereist.

Voor onderhoud van bedrijfskritische apparatuur sluit de instelling 7x24 overeenkomsten af met leveranciers. Het onderhoud van alle hardware wordt hiermee afgedekt. Een van de prestatie-eisen die leveranciers contractueel moet worden opgelegd is een time-to-repair van 4 uur (tijdens de normale kantooruren).

ICTS is zelf verantwoordelijk voor het softwareonderhoud (software-patches en updates) en wijst hiervoor per te onderhouden systeem tenminste een verantwoordelijk functioneel en technisch beheerder aan.

Alle onderhoudswerkzaamheden dienen op de eigen locatie te worden uitgevoerd. Als onderhoud c.q. reparatie op de eigen locatie onmogelijk is en/of leidt tot onacceptabel hoge kosten, dient door ICTS en de leverancier rekening te worden gehouden met de eventuele aanwezigheid van opgeslagen vertrouwelijke of geheime informatie, vitale gegevens en/of software. Indien nodig dient deze informatie voorafgaand aan de extern uit te voeren werkzaamheden afdoende te worden verwijderd of veiliggesteld.

ICT houdt een registratie bij van alle vermeende of daadwerkelijke storingen en van alle preventieve en corrigerende onderhoudswerkzaamheden. Voor werkstations vindt dit plaats middels het incident management proces en bijhorende informatiesystemen.

9.2.5 Beveiliging van apparatuur buiten het terrein

Apparatuur buiten de terreinen behoort te worden beveiligd waarbij rekening wordt gehouden met de diverse risico's van werken buiten het terrein van de organisatie.

Er is een instellingsbrede gebruikersovereenkomst voor mobiele apparatuur. De overeenkomst bevat onder meer een paragraaf met gebruiksvoorwaarden, beveiligingsrichtlijnen en gedragsregels voor een goede omgang met apparatuur en gegevensdragers (zoals extern gebruik, de eigen verantwoordelijkheid inzake op dit soort apparatuur opgeslagen informatie en maatregelen die verlies en diefstal tegen gaan).

Bij de uitlevering van de apparatuur dient de gebruiker kennis te nemen van de gebruiksvoorwaarden en deze voor akkoord te tekenen.

Voor mobiele apparatuur en gegevensdragers geldt: de gebruiker is zelf verantwoordelijk voor het veiligstellen van vitale informatie (back-up) en het regelmatig schonen om het uitlekken van vertrouwelijke of geheime informatie te voorkomen. Gebruikers dienen terughoudend te zijn met de opslag en transport van vertrouwelijke en geheime informatie en trachten niet meer van dergelijke informatie op de apparatuur te bewaren dan voor het werk noodzakelijk is. Dergelijke informatie dient zoveel mogelijk direct na gebruik van apparatuur te worden verwijderd.

De gebruiker beschermt apparatuur buiten het terrein door de volgende maatregelen te nemen:

1. Mobiele apparatuur (tablets, (smart)phones, USB-sticks, laptops) van de instelling, of andere apparatuur met vertrouwelijke of geheime informatie van de instelling mag niet onbeheerd achtergelaten worden op externe locaties;
2. Bij het reizen met mobiele apparatuur van de instelling moeten apparatuur en datadragers als handbagage vervoerd worden;
3. Mobiele apparatuur wordt beveiligd volgens de ICTS gepubliceerde beveiligingsrichtlijnen voor mobiele apparatuur en de in de gebruikersovereenkomst genoemde beveiligingsrichtlijnen.

Bij het beveiligen van apparatuur gaat het met name om het beletten dat als vertrouwelijk of hoger geclassificeerde informatie in vreemde handen komt.

9.2.6 Veilig verwijderen of hergebruiken van apparatuur

Alle apparatuur die opslagmedia bevat, behoort te worden gecontroleerd om te bewerkstelligen dat alle gevoelige gegevens en in licentie gebruikte programmatuur zijn verwijderd of veilig zijn overschreven voordat de apparatuur wordt verwijderd.

Als media worden afgedankt (bijvoorbeeld harde schrijven of back-up tapes), welke mogelijk informatie met een classificatie “Intern” of hoger bevat, dienen deze onleesbaar gemaakt te worden alvorens ze af te voeren.

ICTS is verantwoordelijk voor het afdoende wissen van gegevens van gegevensdragers alvorens apparatuur met deze gegevensdragers wordt afgevoerd of hergebruikt. ICTS maakt hiertoe uitsluitend gebruik van gecertificeerde (zoals CA+) dienstverleners. Hierbij dient een vernietigingsverklaring te worden afgegeven.

Onleesbaar maken van de media kan gedaan worden door de media te overschrijven met willekeurige data. Het verwijderen van bestanden of het “formatteren” van de media is niet toereikend. Specifiek geldt:

1. Harde schijven en Solid state schijven (SSD) dienen geheel te worden overschreven;
2. Smartphones en tablets dienen te worden teruggezet in de “factory defaults” en tevens dient het interne geheugen geheel te worden overschreven. Voorafgaand aan inlevering dient de gebruiker deze media veilig te bewaren;
3. CD’s, DVD’s en dergelijke dienen fysiek te worden vernietigd;
4. Papieren informatiedragers dienen te worden vernietigd middels een shredder[12];

Voordat desktops en laptops voor hergebruik worden opgeslagen, dienen deze eenmalig (geheel) te worden gewist.

Voor media die mogelijk informatie met de classificatie “Vertrouwelijk” of hoger bevatten geldt dat er tenminste 3 ronden nodig zijn: geheel overschrijven met willekeurige data, geheel overschrijven met nullen en nogmaals geheel overschrijven met (andere) willekeurige data.

Als de media zodanig zijn beschadigd, of van zodanige aard zijn (bijvoorbeeld read-only), dat overschrijving niet (meer) mogelijk is, dienen zij bij voorkeur fysiek vernietigd te worden of gedurende tenminste vijf jaar op een veilige plaats te worden opgeslagen alvorens te worden afgevoerd.

In voorkomende gevallen waarbij de media moeten worden ingenomen door de leverancier, bijvoorbeeld in verband met garantie, dienen sluitende afspraken te worden gemaakt met de leverancier in kwestie omtrent een veilig levenseinde van de media.

Voor zover het veilig verwijderen of hergebruiken van apparatuur onderdeel is van dienstverlening door derden maakt de instelling formele afspraken met de dienstverlener inzake de invulling van deze beheersmaatregel.

9.2.7 Verwijdering van bedrijfseigendommen

Apparatuur, informatie en programmatuur van de organisatie mogen niet zonder toestemming vooraf van de locatie worden meegenomen.

Het in bruikleen krijgen van mobiele apparatuur, zoals een laptop, tablet en/of smartphone wordt te allen tijde bekrachtigd via een gebruikersovereenkomst.

12 In aanmerking komen alleen shredders met een snippergrootte van niet meer dan 30mm lang en 5mm breed.

In bruikleen gegeven mobiele apparatuur is persoonsgebonden. Gebruikers hebben toestemming om de apparatuur van de locatie mee te nemen.

Toestemming van de Eigenaar is vereist voor het van de locatie meenemen van vertrouwelijke of geheime informatie en/of apparatuur anders dan een laptop, tablet of smartphone. Eigenaarschap is door ICTS duidelijk vastgesteld. De Eigenaar is verantwoordelijk voor registratie en het (doen) houden van toezicht op gebruik en naleving van afspraken zoals tijdige retournering.

10 Beheer van communicatie- en bedieningsprocessen

10.1 Bedieningsprocedures en verantwoordelijkheden

Doelstelling:
Waarborgen van een correcte en veilige bediening van IT-voorzieningen.

10.1.1 Gedocumenteerde bedieningsprocedures

Bedieningsprocedures behoren te worden gedocumenteerd, te worden bijgehouden en beschikbaar te worden gesteld aan alle gebruikers die deze nodig hebben.

Bedieningsprocedures geven de instructies voor de gedetailleerde uitvoering van taken die betrekking hebben op informatiesystemen.

ICTS onderhoudt specifieke bedieningsprocedures voor de diverse informatiesystemen. ICTS documenteert onder meer:

1. Het aanmaken van nieuwe gebruikers en het verwijderen van gebruikers;
2. Het configureren van (toegangs-)rechten en andere aspecten op systeemniveau;
3. Het maken en testen van back-ups (back-up-plan);
4. Het afhandelen van incidenten, calamiteiten en overige uitzonderlijke gebeurtenissen, inclusief:
    a. Periodieke verificatie van de correcte werking van bedrijfskritische toepassingen;
    b. Het afsluiten, herstellen en herstarten van (informatie)systemen;
    c. Het inschakelen van 2e en 3e lijns-ondersteuning.
5. Wijzigingsbeheer, inclusief het plegen van softwareonderhoud en het (proactief) patchen van systemen;
6. Capaciteitsbeheer;
7. Systeemacceptatie en het gebruik van de Ontwikkel-, Test- en Acceptatie- (OTA)-omgeving;
8. Het gebruik van beheer- en testtools.

Technisch Beheer onderhoudt documentatie met betrekking tot systeem- en applicatie-technische aspecten. Functioneel Beheer onderhoudt, voor zover vereist, de documentatie met betrekking tot het gebruik van bedrijfstoepassingen.

10.1.2 Wijzigingsbeheer

Wijzigingen in IT-voorzieningen en informatiesystemen behoren te worden beheerst.

In de procedures voor wijzigingsbeheer is minimaal aandacht besteed aan:

1. Een impactanalyse van mogelijke gevolgen van de wijzigingen;
2. Voor de installatie van nieuwe ICT-voorzieningen of wijziging van bestaande voorzieningen wordt door de procescoördinator wijzigingsbeheer een goedkeuringsprocedure vastgesteld;
3. In de procedures voor wijzigingsbeheer is vastgelegd dat ongeautoriseerde ICT voorzieningen niet mogen worden geïnstalleerd of gebruikt en dat elke installatie en bijbehorend doel en gebruik formeel moeten worden goedgekeurd op zakelijk en technisch niveau;
4. Zakelijke goedkeuring wordt verleend door de betreffende Eigenaar, technische goedkeuring door de managers die verantwoordelijk zijn voor onderhoud en beheer van de voorziening.

Voor een dienst die wordt verleend door een derde partij, is het beheer van wijzigingen de verantwoordelijkheid van de manager onder wiens verantwoordelijkheid de overeenkomst met de derde partij is aangegaan.

Steeds geldt dat tijdens en na een wijziging een situatie moet bestaan welke voldoet aan de gestelde (beveiligings-)eisen.

10.1.3 Functiescheiding

Taken en verantwoordelijkheidsgebieden behoren te worden gescheiden om gelegenheid voor onbevoegde of onbedoelde wijziging of misbruik van de bedrijfsmiddelen van de organisatie te verminderen.

De instelling past functiescheiding toe voor zover het management de risico's die gemoeid zijn met het ontbreken van functiescheiding niet acceptabel vindt en functiescheiding praktisch uitvoerbaar en realiseerbaar is.

Waar functiescheiding lastig kan worden gerealiseerd of in verhouding te hoge kosten met zich meebrengt, worden door de instelling andere maatregelen overwogen, zoals het (steekproefsgewijs) controleren van activiteiten, het voorzien in audit trails (logging) en supervisie.

10.1.4 Scheiding van faciliteiten voor ontwikkeling, testen en productie

Faciliteiten voor ontwikkeling, testen en productie behoren te zijn gescheiden om het risico van onbevoegde toegang tot of wijzigingen in het productiesysteem te verminderen.

Voor ontwikkel-, test- en acceptatiedoeleinden onderhoudt ICTS aparte omgevingen, los van de productieomgeving. Onder meer de volgende uitgangspunten en richtlijnen zijn van kracht:

1. ICTS gebruikt voor productie, testen en acceptatie gescheiden omgevingen;
2. De test- en acceptatieomgeving benadert de productieomgeving in ontwerp zo goed mogelijk;
3. De productieomgeving mag niet worden gebruikt voor testdoeleinden;
4. Tijdens overdracht van gegevens tussen de omgevingen dienen de vereiste beveiligingsmaatregelen gehandhaafd te blijven;
5. Voor de acceptatieomgeving gelden dezelfde beveiligingseisen als voor de productieomgeving;
6. Voor de verschillende omgevingen wordt verschillende accounts gebruikt om vergissingen te voorkomen.

ICTS onderhoudt de documentatie met betrekking tot het gebruik van de verschillende omgevingen en de bijbehorende procedures.

10.2 Beheer van de dienstverlening door een derde partij

Doelstelling:
Geschikt niveau van informatiebeveiliging en dienstverlening implementeren en bijhouden in overeenstemming met de overeenkomsten voor dienstverlening door een derde partij.

10.2.1 Dienstverlening

Er behoort te worden bewerkstelligd dat de beveiligingsmaatregelen, definities van dienstverlening en niveaus van dienstverlening zoals vastgelegd in de overeenkomst voor dienstverlening door een derde partij worden geïmplementeerd en uitgevoerd en worden bijgehouden door die derde partij.

Alle dienstverlening door derden dient contractueel te worden afgedekt, inclusief de invulling van alle relevante beveiligingsaspecten. De namens de instelling in de overeenkomst genoemde gemandateerde functionaris is als contracteigenaar verantwoordelijk voor het (doen) opnemen van noodzakelijke informatiebeveiligingseisen en –voorwaarden. Hij ziet er op toe dat tenminste opgenomen wordt:

1. De redenen, eisen en voordelen die de toegang door derden noodzakelijk maken;
2. Beschrijving van de dienst(en) die de instelling afneemt van de derde partij;
3. Respectievelijke aansprakelijkheden van de partijen in de overeenkomst;
4. Toegestane toegangsmethoden en beheer, en het gebruik van toegangscodes en wachtwoorden;
5. Autorisatieproces voor gebruikerstoegang en privileges van gebruikers;
6. Als de gebruikersadministratie niet door de instelling plaatsvindt: de verplichting tot het bijhouden van een overzicht van personen die bevoegd zijn de ter beschikking gestelde dienst te gebruiken, en wat hun rechten en privileges zijn;
7. Het beginsel dat alle toegang die niet expliciet is toegestaan, verboden is;
8. Een procedure om toegangsrechten te herroepen of de verbinding tussen systemen af te breken;
9. Beveiligingseisen voor de uitwisseling van informatie.

Medewerkers van gecontracteerde derden dienen verwezen te worden naar de Acceptable Use Policy (AUP) en de ICT-gedragsregels. Van deze medewerkers kan een verklaring verlangd worden ten aanzien van geheimhouding en integriteit, en naleving van de AUP en de ICT-gedragsregels.

10.2.2 Controle en beoordeling van dienstverlening door een derde partij

De diensten, rapporten en registraties die door de derde partij worden geleverd, behoren regelmatig te worden gecontroleerd en beoordeeld en er behoren regelmatig audits te worden uitgevoerd.

Controle en beoordeling van dienstverlening door (medewerkers van) derden is eveneens een taak van de in de overeenkomst genoemde gemandateerde ('contracteigenaar'). Hij ziet er op toe dat de dienstverlenende partij:

1. Zich houdt aan gestelde prestatie-eisen, informatiebeveiligingseisen en –voorwaarden, (gedrags-)regels, voorschriften en verdere richtlijnen;
2. Informatiebeveiligingsincidenten en -problemen conform afspraken meldt en afhandelt.

De contracteigenaar waakt op een goede verstandhouding tussen de instelling en de dienstverlenende partij en verifieert steekproefsgewijs of de dienstverlenende partij afspraken nakomt. Hij onderneemt passende actie wanneer hij manco's in de dienstverlening waarneemt.

Waar mogelijk is oplevering en acceptatie geformaliseerd.

Als hiertoe aanleiding is initieert de contracteigenaar een onafhankelijke audit.

10.2.3 Beheer van wijzigingen in dienstverlening door een derde partij

Wijzigingen in de dienstverlening door derden, waaronder het bijhouden en verbeteren van bestaande beleidslijnen, procedures en maatregelen voor informatiebeveiliging, behoren te worden beheerd, waarbij rekening wordt gehouden met de onmisbaarheid van de betrokken bedrijfssystemen en -processen en met heroverweging van risico's.

De in de overeenkomst genoemde gemandateerde ('contracteigenaar') is verantwoordelijk voor het beheer van wijzigingen in de door de derde partij verleende dienst. Hij houdt hierbij rekening met:

1. De implementatie van wijzigingen die door de instelling worden aangedragen, zoals gewenste verbeteringen in geleverde diensten, wijzigingen ten gevolge van ontwikkelingen aan de kant van de instelling (zoals nieuwe toepassingen en systemen) en wijzigingen in de procedures van de instelling.
2. De implementatie van wijzigingen of aanpassingen die de derde partij aanbiedt (of oplegt), zoals wijzigingen in en verbetering van netwerken, het gebruik van nieuwe technologieën, introductie van nieuwe producten of nieuwere versies/uitgaven, et cetera.

De contracteigenaar ziet er op toe dat hieromtrent afspraken onderdeel worden van de overeenkomst.

10.3 Systeemplanning en -acceptatie

Doelstelling:
Het risico van systeemstoringen tot een minimum beperken.

10.3.1 Capaciteitsbeheer

Het gebruik van middelen behoort te worden gecontroleerd en afgestemd en er behoren verwachtingen te worden opgesteld voor toekomstige capaciteitseisen, om de vereiste systeemprestaties te bewerkstelligen.

ICTS bewaakt het beschikbaar zijn van voldoende restcapaciteit om variaties in het gebruik van IT-voorzieningen op te vangen. ICTS realiseert tijdig benodigde capaciteitsuitbreiding. Daarnaast is capaciteitsbeheer een punt van aandacht bij de introductie van nieuwe informatiesystemen.

Zaken die ICTS in het kader van capaciteitsbeheer aandacht geeft zijn met name:

1. Processing/verwerkingscapaciteit;
2. Opslagcapaciteit (inclusief back-up en logging);
3. Geheugencapaciteit;
4. Voeding en UPS;
5. Netwerkbandbreedte;
6. Koelcapaciteit.

Dagelijks controleert ICTS het gebruik van opslagcapaciteit, het CPU- en geheugengebruik van serversystemen en de hoeveelheid netwerkverkeer op de verschillende verbindingen. Hierbij geven de volgende twee constateringen aanleiding tot actie:

1. Ongebruikelijke, plotselinge/sprongsgewijze en substantiële toename van gebruik van opslag-, CPU-, geheugen- en/of netwerkcapaciteit;
2. Het gestaag doch geleidelijk benaderen van de grenzen van de aanwezige capaciteit, zulks ter inschatting van ICTS. Wat hierbij de exacte grens is, hangt af van de beschikbare capaciteit, tolerantie van het betreffende systeem bij tekorten en de snelheid waarmee het gebruik toeneemt.

ICTS beschouwt en onderzoekt het eerste geval als potentieel beveiligingsincident. In het tweede geval wordt een waarschuwing gegeven aan de betreffende technisch beheerder van het systeem.

10.3.2 Systeemacceptatie

Er behoren aanvaardingscriteria te worden vastgesteld voor nieuwe informatiesystemen, upgrades en nieuwe versies en er behoort een geschikte test van het systeem of de systemen te worden uitgevoerd tijdens ontwikkeling en voorafgaand aan de acceptatie.

Systeemacceptatie maakt onderdeel uit van de procedures voor wijzigingsbeheer.

De implementatie van nieuwe informatiesystemen en grotere wijzigingen worden getoetst aan alle vooraf vastgelegde acceptatiecriteria. Toetsing dient tijdig plaats te vinden. Een impactanalyse moet hebben aangetoond dat het nieuwe informatiesysteem geen nadelige invloed heeft op bestaande systemen. Pas na formele acceptatie brengt ICTS nieuwe toepassingen over naar de productieomgeving.

Acceptatiecriteria dienen binnen het ingerichte project in een vroeg stadium te worden vastgesteld en gedocumenteerd. Hierbij wordt gebruik gemaakt van het hulpmiddel Projectdossier Informatiebeveiliging om gedurende de looptijd van het project de te controleren en gecontroleerde beveiligingsaspecten vast te leggen. Het is aan de (toekomstige) Eigenaar om de specifieke set van te toetsen acceptatiecriteria goed te keuren.

Voor nieuwe systemen en bij grotere wijzigingen vindt te allen tijde een geautomatiseerde kwetsbaarheidsscan plaats. De resultaten van de scan worden geanalyseerd en waar nodig wordt het systeem aangepast voordat het in productie wordt genomen.

Websites en –applicaties, ontwikkeld en opgeleverd door externe partijen buiten ICTS, zijn eveneens aan systeemacceptatie onderhevig. De Eigenaar ziet hier op toe.

10.4 Bescherming tegen virussen en ‘mobile code’

Doelstelling:
Beschermen van de integriteit van programmatuur en informatie.

10.4.1 Maatregelen tegen virussen en 'malicious code'

Er behoren maatregelen te worden getroffen voor detectie, preventie en herstellen om te beschermen tegen virussen en er behoren geschikte procedures te worden ingevoerd om het bewustzijn van de gebruikers te vergroten.

De controle op virussen, trojans en andere malware vindt plaats op meerdere schakels binnen de infrastructuur:

1. Inkomende en uitgaande e-mails worden inclusief bijlagen gecontroleerd;
2. Fileservers zijn voorzien van antivirussoftware;
3. Desktops en laptops zijn voorzien van antivirussoftware.
    a. ICTS beheerde desktops en laptops zijn voorzien van antivirussoftware. De gebruiker kan deze software en de automatische update niet uitschakelen;
    b. De gebruikersovereenkomst voor desktops en laptops van ICTS die de gebruiker zelf beheert, bepaalt dat de gebruiker ervoor moet zorgen dat de machine continu is voorzien van antivirussoftware;
    c. Gebruikers van eigen desktop en laptops dienen zorg te dragen dat het systeem is voorzien van antivirussoftware.
4. Waar mogelijk dienen mobiele devices voorzien te zijn van antivirussoftware;
5. De update voor de detectiedefinities vindt tenminste één keer per dag (automatisch) plaats;
6. Voor de verschillende schakels binnen de infrastructuur past ICTS antivirussoftware van verschillende leveranciers toe.
7. Er behoort voor te worden gezorgd dat er bescherming is tegen malware tijdens onderhouds- en noodprocedures die de normale beschermingsmaatregelen tegen malware zouden kunnen omzeilen.

8. ICTS informeert gebruikers over bescherming tegen malware en hoe de benodigde software kan worden verkregen. ICTS maakt deze informatie beschikbaar op de website van de instelling.
9. ICTS waarschuwt gebruikers regelmatig voor het blindelings, zonder nadenken volgen van links (URL's), openen van bijlagen en downloaden van bestanden, foto's, et cetera. ICTS maakt informatie met betrekking tot de gevaren hiervan beschikbaar op de website van de instelling.

10.4.2 Maatregelen tegen 'mobile code'

Als gebruik van 'mobile code' is toegelaten, behoort de configuratie te bewerkstelligen dat de geautoriseerde 'mobile code' functioneert volgens een duidelijk vastgesteld beveiligingsbeleid, en behoort te worden voorkomen dat onbevoegde 'mobile code' wordt uitgevoerd.

Mobiele code is software die van elders is verkregen en lokaal op de eigen apparatuur wordt uitgevoerd. Websites passen mobile code (zoals Java, JavaScript, ActiveX en XML (AJAX)) veelal toe om dynamische pagina's te genereren. Documenten (zoals van MS Office, Adobe PDF en grafische afbeeldingen) kunnen ook mobile code bevatten.

Om de risico's van mobile code te beperken treft ICTS op verschillende niveaus maatregelen:

Infrastructuur
ICTS treft maatregelen op netwerkniveau (firewall) om bekende malafide websites (die bv. kwaadaardige mobile code verspreiden) te blokkeren. Hiertoe wordt zoveel mogelijk gebruik gemaakt van actuele bronnen.

Applicatieniveau
Relevante applicaties (browser software, MS Office, Outlook) op desktops/laptops zijn zodanig geconfigureerd dat:

1. Overbodige mobile code functionaliteit is uitgezet;
2. Mobile code niet automatisch wordt uitgevoerd tenzij de gebruiker goedkeuring verleent of vastgesteld is dat de mobile code afkomstig is van een betrouwbare bron. Bij voorkeur worden extra voorzieningen (extensions/plugins) geactiveerd om dit te realiseren;
3. Beschikbare browser functionaliteit om malafide websites te blokkeren wordt benut;
4. Grafische afbeeldingen, documenten niet automatisch worden gedownload tenzij de gebruiker goedkeuring verleent of als sprake is van een betrouwbare bron (bijvoorbeeld van de instelling zelf);
5. De securityinstellingen van applicaties op ICTS beheerde desktops en laptops zoveel mogelijk worden benut. Benodigde instellingen worden bepaald aan de hand van betrouwbare security guides, benchmarks en best practices. De gebruiker kan de instellingen niet wijzigen.
6. De gebruiker gewone werkzaamheden met een standaard account verricht (zonder extra privileges).

De gebruikershandleiding van "ICTS selfservice desktops en laptops" besteedt aandacht aan bescherming tegen kwaadaardige mobile code en verwijst naar relevante security guides.

10.5 Back-up

Doelstelling:
Handhaven van de integriteit en beschikbaarheid van informatie en IT-voorzieningen.

10.5.1 Reservekopieën maken (back-ups)

Er behoren back-up kopieën van informatie en programmatuur te worden gemaakt en regelmatig te worden getest overeenkomstig het vastgestelde back-upbeleid.

Ten aanzien van het maken van back-ups gelden de volgende richtlijnen:

1. Van alle informatiesystemen wordt een back-up gemaakt;
2. De back-up-procedures en -processen zijn gedocumenteerd;
3. Er zijn (geteste) procedures voor back-up en recovery van informatie voor herinrichting en foutherstel van verwerkingen;
4. Back-upstrategieën zijn vastgesteld op basis van het soort gegevens (bestanden, databases, et cetera), de maximaal toegestane periode waarover gegevens verloren mogen raken, en de maximaal toelaatbare back-up- en hersteltijd;
5. Back-ups worden bewaard op twee zodanig geografisch gescheiden locaties, dat een incident op de ene locatie niet leidt tot het verloren gaan van de back-up op de andere locatie;

6. Van back-upactiviteiten en de verblijfplaats van de media wordt een registratie bijgehouden, met een kopie van de registratie op een andere locatie. De andere locatie is zodanig gekozen dat een incident op de oorspronkelijke locatie niet leidt tot schade aan of toegang tot de kopie van die registratie;
7. De fysieke en logische toegang tot de back-ups, zowel van systeemschijven als van data, is zodanig geregeld dat alleen geautoriseerde personen zich toegang kunnen verschaffen tot deze back-ups;
8. Back-ups behoren periodiek te worden getest, om:
    a. Te waarborgen dat ze betrouwbaar zijn en in geval van nood kunnen worden gebruikt;
    b. De vaardigheden die nodig zijn voor herstel te borgen in de organisatie.
9. Het als test terugzetten van enkele individuele bestanden vindt tenminste maandelijks plaats;
10. Herstelprocedures behoren regelmatig te worden gecontroleerd en getest, om te waarborgen dat:
    a. Ze doeltreffend zijn;
    b. Ze kunnen worden uitgevoerd binnen de daarvoor volgens operationele herstelprocedures gestelde tijd;
    c. Benodigde vaardigheden op niveau blijven.
11. Het testen van het complete herstel van bedrijfskritische informatiesystemen met ‘schone’ hardware vindt tenminste jaarlijks plaats;
12. Behandeling van back-ups dient in overeenstemming te zijn met het vastgestelde beveiligingsniveau van het betrokken informatiesysteem.

Procedures voor het maken van back-ups voor afzonderlijke systemen behoren regelmatig te worden getest om te waarborgen dat aan de eisen van bedrijfscontinuïteitsplannen wordt voldaan (zie Hoofdstuk 14).

Voor bedrijfskritische informatiesystemen behoren de procedures voor het maken van back-ups alle systeeminformatie, toepassingen en gegevens te omvatten, die nodig zijn om het gehele informatiesysteem binnen een gestelde maximale termijn na algeheel verlies te herstellen.

10.6 Beheer van netwerkbeveiliging

Doelstelling:
Bewerkstelligen van de bescherming van informatie in netwerken en bescherming van de ondersteunende infrastructuur.

10.6.1 Maatregelen voor netwerken

Netwerken behoren adequaat te worden beheerd en beheerst om ze te beschermen tegen bedreigingen en om beveiliging te handhaven voor de systemen en toepassingen die gebruikmaken van het netwerk, waaronder informatie die wordt getransporteerd.

Netwerkbeheerders voeren beheersmaatregelen in voor het waarborgen van de beveiliging van informatie in netwerken en van aangesloten diensten tegen ongeoorloofde toegang. Hierbij dient in het bijzonder rekening te worden gehouden met de volgende punten:

1. De operationele verantwoordelijkheid voor netwerken (netwerkbeheer) wordt waar nodig gescheiden van de verantwoordelijkheid voor computerbewerkingen (serverbeheer);
2. Netwerkapparatuur staat opgesteld in een fysiek beveiligde ruimten;
3. De verantwoordelijkheden en procedures voor het beheer van apparatuur op afstand, zijn vastgesteld. Er zijn afspraken en voorzieningen getroffen:
    a. zodat beheer op afstand alleen mogelijk is vanuit beheernetten;
    b. zodat LoA3 (2-factor authenticatie) voor de toegangsbeveiliging van toepassing is, zie Bijlage 2;
    c. omtrent het monitoren van netwerkapparatuur.
4. Er behoort een passende registratie en controle te worden toegepast om handelingen die van belang zijn voor de beveiliging te kunnen vastleggen;
5. Beheeractiviteiten behoren nauwkeurig te worden gecoördineerd, om de dienstverlening aan de organisatie te optimaliseren en om te waarborgen dat beveiligingsmaatregelen consistent worden toegepast over de informatieverwerkende infrastructuur als geheel.

10.6.2 Beveiliging van netwerkdiensten

Beveiligingskenmerken, niveaus van dienstverlening en beheerseisen voor alle netwerkdiensten behoren te worden geïdentificeerd en opgenomen in elke overeenkomst voor netwerkdiensten, zowel voor diensten die intern worden geleverd als voor uitbestede diensten.

Er zijn overeenkomsten met leveranciers van netwerkdiensten. De gemandateerde onder wiens verantwoordelijkheid de overeenkomst met de derde partij is aangegaan (contracteigenaar) is verantwoordelijk

voor het opnemen van onderkende beveiligingskenmerken, niveaus van dienstverlening en beheereisen in de overeenkomst.

Voor netwerkdiensten die intern worden geleverd zijn aspecten omtrent verantwoordelijkheden, gebruik, beschikbaarheid en beveiligingskenmerken opgenomen in de ICTS dienstencatalogus (PDC).

10.7 Behandeling van media

Doelstelling:
Voorkomen van onbevoegde openbaarmaking, modificatie, verwijdering of vernietiging van bedrijfsmiddelen en onderbreking van bedrijfsactiviteiten.

10.7.1 Beheer van verwijderbare media

Er behoren procedures te zijn vastgesteld voor het beheer van verwijderbare media.

Onder verwijderbare media wordt verstaan: geheugensticks, tapes, flashgeheugenkaarten, verwijderbare harde schijven, cd's, dvd's en dergelijke, inclusief gedrukte media.

De gebruiker is in beginsel zelf verantwoordelijk voor het gebruik van hem toevertrouwde verwijderbare media. Dit betreft zaken zoals het (tijdig) verwijderen van gevoelige gegevens, het veiligstellen van unieke bestanden en het veilig opbergen.

De gebruiker dient ervoor te zorgen dat als vertrouwelijk of hoger geclassificeerde informatie uitsluitend versleuteld wordt opgeslagen op verwijderbare media.

ICTS wijst de gebruiker van verwijderbare media middels de website van de instelling en gebruikshandleidingen op de risico's van opslag van vertrouwelijk of hoger geclassificeerde informatie op verwijderbare media (bewustwording).

De gebruiker dient maatregelen te nemen om het risico van diefstal van verwijderbare media zoveel mogelijk te beperken.

Er is een procedure voor het melden en afhandelen van diefstal of verlies van door de instelling verstrekte verwijderbare media.

Als de levensduur van de verwijderbare media (volgens de specificaties van de fabrikant) korter is dan de beschikbaarheidstermijn van de informatie die erop is opgeslagen dan dient deze informatie ook elders te worden opgeslagen om verlies van informatie te voorkomen.

10.7.2 Verwijdering van media

Media behoren op een veilige en beveiligde manier te worden verwijderd als ze niet langer nodig zijn, overeenkomstig formele procedures.

Als media (zoals harde schijven of back-up-tapes) worden afgedankt, welke mogelijk vertrouwelijk of hoger geclassificeerde informatie bevat, dienen deze onleesbaar gemaakt te worden alvorens ze af te voeren.

Onleesbaar maken van de media kan gedaan worden door de media te overschrijven met willekeurige data. Het verwijderen van bestanden of het “formatteren” van de media is niet toereikend.

In voorkomende gevallen waarbij media moeten worden ingenomen door de leverancier, bijvoorbeeld in verband met garantie, dienen sluitende afspraken te worden gemaakt met de leverancier aangaande eventuele als vertrouwelijk of hoger geclassificeerde informatie op de media.

ICTS, i.c. Divisie Klant, is het verzamelpunt voor het afdanken van media.. ICTS kan hierbij gebruik maken van afgesloten verzamelcontainers op diverse plekken in de gebouwen van UvA en HvA. ICTS draagt zorg voor verantwoorde vernietiging van ingeleverde media met inachtneming van paragraaf 9.2.6.

Ook tijdens interne verhuizingen dienen media met als vertrouwelijk of hoger geclassificeerde informatie verantwoord te worden afgedankt.

De gebruiker is verantwoordelijk voor het verantwoord afdanken van documenten met vertrouwelijke informatie. Voor het vernietigen van documenten met als vertrouwelijk of hoger geclassificeerde informatie zijn op diverse plekken in de gebouwen van UvA en HvA afgesloten papiercontainers aanwezig. Gebruikers kunnen alle andere documenten afdanken via centraal opgestelde papiercontainers.

10.7.3 Procedures voor de behandeling van informatie

Er behoren procedures te worden vastgesteld voor de behandeling en opslag van informatie om deze te beschermen tegen onbevoegde openbaarmaking of misbruik.

Voor informatie van de categorie “openbaar” gelden geen specifieke procedures om die informatie te behandelen, te verwerken, op te slaan en te communiceren. Het is derhalve de eigen verantwoordelijkheid van de medewerker om zorgvuldig met dit soort informatie om te gaan, waarbij tenminste moet zijn voldaan aan wet- en regelgeving.

Voor informatie van de vertrouwelijkheidscategorie “intern” geldt dat deze zonder beperkingen gehanteerd mag worden door medewerkers en, als daar noodzaak toe bestaat, ook door derden.

Voor informatie van de categorie ‘vertrouwelijk’ en hoger geldt dat deze alleen gehanteerd mag worden door medewerkers en derden op basis van een “need-to-know”, waarbij derden uitsluitend toegang mogen hebben nadat geheimhouding is overeengekomen, zie 10.8.1. Hieronder valt tevens de behandeling van privacy-gevoelige informatie, zoals personeelsdossiers, verslagen van functioneringsgesprekken en CV's van sollicitanten. Hierbij moet zijn voldaan aan geldende privacy wet- en regelgeving.

Voor informatie van de categorie 'geheim' geldt bovendien dat zij alleen maar mag worden opgeslagen op door de Eigenaar aangewezen locaties en media.

Bovenstaande is van toepassing op documenten, multimedia, mobiele en telefonische communicatie, (draagbare) computerapparatuur, multifunctionals, (mobiele) netwerken, postdiensten/-voorzieningen en andere media en apparatuur.

Aanvullend zijn de richtlijnen uit paragraaf 7.2.2 van toepassing.

10.7.4 Beveiliging van systeemdocumentatie

Systeemdocumentatie behoort te worden beschermd tegen onbevoegde toegang.

Voor systeemdocumentatie gelden dezelfde richtlijnen als voor beheersmaatregel 10.7.3.

10.8 Uitwisseling van informatie

Doelstelling:
Handhaven van beveiliging van informatie en programmatuur die wordt uitgewisseld binnen een organisatie en met enige externe entiteit.

10.8.1 Beleid en procedures voor informatie-uitwisseling

Er behoren formeel beleid, formele procedures en formele beheersmaatregelen te zijn vastgesteld om de uitwisseling van informatie via het gebruik van alle typen communicatiefaciliteiten te beschermen.

Om onbevoegde kennisname te voorkomen dient een gebruiker geen vertrouwelijke of geheime informatie onbeheerd achter te laten op afdrukvoorzieningen (zoals multifunctionals, kopieermachines, printers en faxapparaten),. Voor het afdrukken van dergelijke informatie wordt bij voorkeur gebruik gemaakt van secure printing.

Om onnodige of ongewenste verspreiding of onbevoegde kennisname te voorkomen dient de mailvoorziening automatisch doorzenden van e-mail naar externe mailadressen te beletten.

Het gebruik van privé e-mail door medewerkers voor werkzaamheden ten behoeve van de instelling is vanwege de risico's die dit met zich meebrengt (met name het uitlekken van vertrouwelijke of geheime informatie) niet toegestaan.

De leidinggevenden dienen medewerkers erop te wijzen dat zij passende voorzorgen behoren te nemen, bijvoorbeeld om geen vertrouwelijke of geheime informatie te onthullen via het opvangen of afluisteren van telefoongesprekken, vooral bij gebruik van mobiele telefoons;

Voor het uitwisselen van informatie geldt verder het volgende:

1. Openbare informatie kan zonder beperkingen worden uitgewisseld;
2. Interne informatie kan tussen medewerkers onderling zonder beperkingen worden uitgewisseld. Uitwisseling met derden is mogelijk als daar noodzaak toe bestaat en het de belangen van de instelling en gebruikers niet schaadt. Zulks ter beoordeling van de medewerker die het initiatief tot uitwisseling neemt;
3. Vertrouwelijke informatie mag alleen worden uitgewisseld met partijen die een “need to know” hebben, als dat noodzakelijk is voor de werkzaamheden. Zulks ter beoordeling aan de eigenaar van de informatie. Vertrouwelijke informatie wordt alleen uitgewisseld op basis van beveiligde protocollen. Voor zover het medewerkers van de instelling betreft gelden geen verdere beperkingen. Voor derde partijen geldt dat voorafgaand aan uitwisseling een geheimhoudingsovereenkomst moet zijn overeengekomen;
4. Voor informatie die als ‘geheim’ geclassificeerd is, geldt bovendien:
    a. De informatie wordt bij voorkeur niet digitaal ter beschikking van derden gesteld;
    b. Afschriften van de betreffende informatie worden genummerd uitgegeven en op zo kort mogelijke termijn teruggevorderd (en bij voorkeur vervolgens vernietigd);
    c. Bij digitaal uitgegeven informatie wordt van de ontvangende partij expliciet geëist dat de informatie na gebruik wordt vernietigd en dat de vernietiging wordt gerapporteerd aan de eigenaar;
    d. De eigenaar van de informatie houdt een administratie bij waarin is opgenomen:
        i. Welk afschrift aan wie ter beschikking wordt gesteld;
        ii. Aan wie een digitale kopie ter beschikking is gesteld;
        iii. Of het afschrift reeds is terug ontvangen dan wel de kopie reeds is vernietigd.

10.8.2 Uitwisselingsovereenkomsten

Er behoren overeenkomsten te worden vastgesteld voor de uitwisseling van informatie en programmatuur tussen de organisatie en externe partijen.

Bij het uitwisselen van informatie en/of software tussen de instelling en een externe partij dient beveiliging bijzondere aandacht te krijgen.

Er behoren beleid, procedures en normen te worden vastgesteld en onderhouden om uitwisseling (waaronder al dan niet digitale transporten) te beschermen (zie ook paragraaf 10.8.3). In uitwisselingsovereenkomsten dient hier naar te worden verwezen.

Onderwerpen die aandacht moeten krijgen zijn onder meer:

1. Het eigenaarschap van informatie en/of software en de verantwoordelijkheid voor de gegevensbescherming, auteursrechten, licenties van software;
2. Maatregelen om betrouwbaarheid - waaronder traceerbaarheid en onweerlegbaarheid - van gegevens te waarborgen;
3. Verantwoordelijkheid en aansprakelijkheid in het geval van informatiebeveiligingsincidenten alsmede procedures over melding van incidenten.

Indien mogelijk wordt binnenkomende software (zowel op fysieke media als gedownload) gecontroleerd op ongeautoriseerde wijzigingen aan de hand van een door de leverancier via een gescheiden kanaal geleverde checksum of certificaat.

De beveiligingsinhoud van elke uitwisselingsovereenkomst behoort in overeenstemming te zijn met de classificatie van de betreffende informatie.

10.8.3 Fysieke media die worden getransporteerd

Media die informatie bevatten behoren te worden beschermd tegen onbevoegde toegang, misbruik of corrumperen tijdens transport buiten de fysieke begrenzing van de organisatie.

Transport van fysieke media (gegevensdragers) met als vertrouwelijk of hoger geclassificeerde informatie dient tot een absoluut minimum te worden beperkt en dient te geschieden met goedgekeurde middelen, waardoor de inhoud niet zichtbaar, niet kenbaar en inbreuk detecteerbaar is.

Mogelijke beveiligingsmaatregelen zijn:

1. Bescherming door fysieke maatregelen, zoals afgesloten containers;
2. Gebruik van verpakkingsmateriaal waaraan te zien is of getracht is het te openen;
3. Persoonlijke aflevering;
4. Opsplitsing van zendingen in meerdere delen en eventueel verzending via verschillende routes;
5. Gebruik maken van betrouwbare transport- en koeriersdiensten in combinatie met identiteitscontroles van koeriers.

10.8.4 Elektronische berichtenuitwisseling

Informatie die een rol speelt bij elektronische berichtuitwisseling behoort op geschikte wijze te worden beschermd.

Elektronisch berichtenverkeer zoals e-mail, elektronische gegevensuitwisseling via een service bus (zoals SAP PI, integratieplatform SIS, etc.) en 'instant messaging' kan vertrouwelijke of geheime informatie bevatten. Deze berichten dienen derhalve op basis van classificatie op een afdoende hoog niveau te worden beveiligd. Gebruikers dienen op verantwoorde wijze van elektronische berichtenuitwisseling gebruik te maken.

Er dient te worden zorggedragen voor onder meer

1. Beschermen van berichten tegen toegang door onbevoegden, wijziging of weigeren van dienst;
2. Waarborgen van correcte adressering en transport van berichten;
3. Bescherming tegen spam en malware;
4. Toepassen van 'state of the art' versleuteling (encryptie) bij classificatie 'vertrouwelijk' of 'geheim'.

10.8.5 Systemen voor bedrijfsinformatie

Beleid en procedures behoren te worden ontwikkeld en geïmplementeerd om informatie te beschermen die een rol speelt bij de onderlinge koppeling van systemen voor bedrijfsinformatie.

Wanneer er bij nieuwbouw of wijzigingen sprake is van onderlinge koppeling van eigen informatiesystemen of koppeling van eigen informatiesystemen met systemen van derden, moet per geval de beveiligingsproblematiek aan de hand van een risicoanalyse worden geïnventariseerd en dienen passende beveiligingsmaatregelen te worden vastgesteld. Er dient tenminste aandacht te zijn voor:

1. Classificatie van de via de koppeling uit te wisselen informatie;
2. Identificatie en authenticatie;
3. Waarborging vertrouwelijkheid en integriteit door passende bescherming van de gegevensoverdracht;
4. Bescherming van toegang tot de uitgewisselde informatie;
5. Bescherming van toegang tot koppelingsfunctionaliteit;
6. Eventuele beïnvloeding van beschikbaarheid (kan het uitwisselen de beschikbaarheid van de gekoppelde systemen beïnvloeden?).

10.9 Diensten voor e-commerce

Doelstelling:
Bewerkstelligen van de beveiliging van diensten voor e-commerce, en veilig gebruik ervan.

10.9.1 E-commerce

Informatie die een rol speelt bij e-commerce en die via openbare netwerken wordt uitgewisseld, behoort te worden beschermd tegen frauduleuze activiteiten, geschillen over contracten en onbevoegde openbaarmaking en modificatie.

Er wordt vooralsnog in beperkte mate gebruik gemaakt van elektronische handel (onder andere betaling collegegelden).

Elektronische handel is gevoelig voor een aantal dreigingen die kunnen resulteren in frauduleuze handelingen, contractuele geschillen en ongewenste openbaarmaking of wijziging van informatie. Om risico's te beheersen dient bij elektrische handel:

1. De vertrouwelijkheid en integriteit van transacties, betalingsinformatie, adresgegevens van de ontvanger en ontvangstbevestiging te worden gewaarborgd;
2. Gebruik te worden gemaakt van veilige authenticatiemethoden;
3. De keuze te worden gemaakt voor de meest geschikte vorm van betalen om fraude te voorkomen; waar vereist kan ook gebruik worden gemaakt van de diensten van vertrouwde derden (bijvoorbeeld iDeal).

10.9.2 Online transacties

Informatie die een rol speelt bij onlinetransacties behoort te worden beschermd om onvolledige overdracht, onjuiste routing, onbevoegde wijziging van berichten, onbevoegde openbaarmaking, onbevoegde duplicatie of weergave van berichten te voorkomen.

Voor online transacties geldt:

1. De betrokken partijen zijn geauthentiseerd en de privacy van partijen is gewaarborgd;
2. Een transactie wordt geautoriseerd door een (gekwalificeerde) wilsuiting van de gebruiker;
3. De communicatieprotocollen tussen partijen zijn beveiligd;
4. De informatie in een transactie is versleuteld.

10.9.3 Openbaar beschikbare informatie

De betrouwbaarheid van de informatie die beschikbaar wordt gesteld op een openbaar toegankelijk systeem behoort te worden beschermd om onbevoegde modificatie te voorkomen.

Het plaatsen en wijzigen van informatie op de publieke websites van de instelling is voorbehouden aan een beperkt aantal daartoe specifiek aangewezen en gemachtigde medewerkers (redacteuren). Deze medewerkers zijn verantwoordelijk voor wijzigingen die zij in de inhoud aanbrengen en andere (beheer)handelingen die zij plegen.

Er behoort een formeel goedkeuringsproces te worden doorlopen voordat de informatie openbaar toegankelijk wordt gemaakt. Bovendien behoort alle invoer, die van buitenaf aan het systeem wordt geleverd, voorafgaand aan publicatie te worden gecontroleerd en goedgekeurd.

10.10 Controle

Doelstelling:
Ontdekken van onbevoegde informatieverwerkingsactiviteiten.

10.10.1 Aanmaken audit-logbestanden

Activiteiten van gebruikers, uitzonderingen en informatiebeveiligingsgebeurtenissen behoren te worden vastgelegd in audit-logbestanden. Deze logbestanden behoren gedurende een overeengekomen periode te worden bewaard, ten behoeve van toekomstig onderzoek en toegangscontrole.

Activiteiten van gebruikers, uitzonderingen en informatiebeveiligingsgebeurtenissen behoren te worden vastgelegd in auditlogbestanden. Deze informatie kan gebruikt worden voor fraude preventie, auditdoeleinden en voor het detecteren en verhelpen van incidenten.

Auditlogbestanden worden ten behoeve van toekomstig onderzoek en toegangscontrole tenminste drie maanden bewaard, echter niet langer dan noodzakelijk en door wet- en regelgeving toegestaan De Eigenaar kan verzoeken om logbestanden voor een bepaald informatiesysteem langer te bewaren.

Voor alle systemen moeten tenminste de navolgende gebeurtenissen worden geregistreerd:

1. Inlogpogingen zowel op systeemniveau als op toepassingsniveau (als de toepassing inloggen vereist);
2. Alle vormen van directe toegang op systeemniveau;
3. Herstarten van het systeem en het stoppen en starten van toepassingen;
4. Afwijkingen als gedetecteerd door file-integriteitschecks alsmede het feit of checks hebben plaatsgevonden.

Voor informatiesystemen welke het beveiligingsniveau “Kritiek” vereisen dienen tevens alle gebeurtenissen of combinatie van gebeurtenissen welke kunnen duiden op fraude te worden geregistreerd. De Eigenaar is

verantwoordelijk voor het opstellen van een lijst van dergelijke gebeurtenissen tijdens het ontwikkelen van een dergelijk informatiesysteem.

In de auditlogbestanden behoren de volgende gegevens te worden vastgelegd:

1. Gebruikers-ID's;
2. Data, tijdstippen en details van de geregistreerde gebeurtenissen;
3. Waar mogelijk de identiteit van de computer of de locatie.

Tijdstippen in logbestanden worden vastgelegd in UTC (Zie paragraaf 10.10.6 Synchronisatie van systeemklokken).

Wachtwoorden worden niet vastgelegd in auditlogbestanden.

De auditlogbestanden kunnen vertrouwelijke persoonlijke informatie bevatten. De bestanden dienen voldoende beveiligd te zijn en alleen op een “need to know” basis toegankelijk te zijn.

Alle informatiesystemen sturen hun beveiligingsgerelateerde loginformatie naar een centraal beheerd logsysteem. De technisch beheerder van dit logsysteem heeft geen systeembeheer-toegang tot andere systemen dan het centrale logsysteem (functiescheiding).

De beheerder van het centrale logsysteem ziet er op toe dat het logsysteem steeds voldoende (rest)capaciteit heeft.

10.10.2 Controle van systeemgebruik

Er behoren procedures te worden vastgesteld om het gebruik van IT-voorzieningen te controleren. Het resultaat van de controleactiviteiten behoort regelmatig te worden beoordeeld.

Dagelijks wordt door het Operations Control Center (OCC) van ICTS alle geregistreerde gebeurtenissen omtrent het functioneren van de systemen bekeken en beoordeeld. Er is tenminste voldoende aandacht voor:

1. Afwijkingen t.o.v. het normale patroon van het aantal mislukte inlogpogingen;
2. Afwijkingen t.o.v. het normale netwerkverkeerspatroon;
3. De tijdstippen waarop toegang tot het systeem op systeemniveau is gezocht;
4. De locatie vanaf waar toegang tot het systeem op systeemniveau is gezocht;
5. Herstarten van het systeem of stoppen/starten van toepassingen moeten verklaarbaar zijn op basis van een geplande wijziging of bekend incident;
6. Controleren van het correcte verloop van een back-up of restore;
7. Afwijkingen zoals gedetecteerd door systeemintegriteitschecks moeten verklaarbaar zijn (zoals nieuwe serverprocessen of juist de afwezigheid van serverprocessen);
8. Ontbreken van loginformatie.

Ten behoeve van het detecteren van beveiligingsincidenten vindt de analyse van logfiles centraal en geautomatiseerd plaats. Hierbij worden dubbele logberichten gefilterd en waar mogelijk logberichten gecorreleerd. Meldingen en alarmen worden op een overzichtelijke manier gepresenteerd en samengevat.

Voor informatiesystemen, waarvoor beveiligingsniveau “kritiek” van toepassing is, dienen tevens de specifiek voor dat systeem vastgelegde gebeurtenissen te worden bewaakt. Als over één van de bovengenoemde punten twijfel bestaat, dient nader onderzoek ingesteld te worden.

10.10.3 Bescherming van informatie in logbestanden

Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen inbreuk en onbevoegde toegang.

ICTS dient er voor te zorgen dat de loginformatie en het logsysteem beschermd is. De volgende richtlijnen zijn van kracht:

1. ICTS is verantwoordelijk voor het correct functioneren en zorgvuldig beheer van het logsysteem. ICTS neemt daarbij de afgesproken bewaartermijnen in acht. Alleen daartoe geautoriseerde beheerders hebben leestoegang tot logbestanden (ook back-ups) en toegang tot het logsysteem;
2. Logbestanden worden zodanig beschermd dat deze niet aangepast kunnen worden;

3. Voor wijziging van de logging voor toegang is goedkeuring van de Eigenaar nodig;
4. Wijzigingen van de logging en/of het logsysteem worden alleen aangebracht door daartoe geautoriseerde beheerders;
5. De beschikbaarheid van loginformatie is gewaarborgd binnen de termijn waarin loganalyse noodzakelijk wordt geacht, met een minimum van drie maanden.
6. Uitval van logging en het logsysteem wordt gedetecteerd.

10.10.4 Logbestanden van administrators en operators

Activiteiten van systeemadministrators en systeemoperators behoren in logbestanden te worden vastgelegd.

Voor alle systemen worden de gebeurtenissen zoals beschreven in paragraaf 10.10.1 vastgelegd.

Voor informatiesystemen waarvoor beveiligingsniveau “kritiek” van toepassing is, wordt in samenspraak met de Eigenaar bepaald in welke mate aanvullende logging van activiteiten van technisch beheerders nodig is.

10.10.5 Registratie van storingen

Storingen behoren in logbestanden te worden vastgelegd en te worden geanalyseerd en er behoren geschikte maatregelen te worden genomen.

ICTS registreert in haar IT-servicemanagementtool de storingen, gerapporteerd door gebruikers of door systeem software, die verband houden met problemen met informatiesystemen.

De afhandeling van storingen vindt plaats conform de afspraken die hiervoor binnen ICTS gemaakt zijn en waarvan het proces in het IT-servicemanagementtool is vastgelegd.

10.10.6 Synchronisatie van systeemklokken

De klokken van alle relevante informatiesystemen binnen een organisatie of beveiligingsdomein behoren te worden gesynchroniseerd met een overeengekomen nauwkeurige tijdsbron.

Ten behoeve van een betrouwbare analyse van logbestanden worden systeemklokken van ICTS beheerde systemen gesynchroniseerd met een betrouwbare centrale tijdbron. Deze wijkt ten hoogste 5 seconden af van UTC (Universal Coordinated Time).

11 Toegangsbeveiliging

11.1 Bedrijfseisen ten aanzien van toegangsbeheersing

Doelstelling:
Beheersen van de toegang tot informatie.

11.1.1 Toegangsbeleid

Er behoort toegangsbeleid te worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfseisen en beveiligingseisen voor toegang.

De toegang tot informatie en informatiesystemen dient voldoende te worden beheerst, zowel fysiek als logisch.

De instelling classificeert haar informatie en informatiesystemen. Naarmate de classificatie hoger is, is een betere toegangsbeveiliging nodig.

De instelling streeft via het hanteren van principes en procedures doorlopend naar het zo beperkt mogelijk houden van toegangsrechten en –mogelijkheden (“least privilege”). Voor het verlenen van toegang geldt daarnaast het principe 'standaard niet, tenzij het expliciet is toegestaan' (“deny-by-default”).

Voor toegang tot informatiesystemen en ruimten waarin zich informatie(middelen) bevinden heeft de gebruiker toegangsrechten nodig. Deze dienen door zijn leidinggevende schriftelijk, met gebruik van autorisatieformulieren, te worden toegekend op basis van het 'need-to' principe. Dit betekent dat de leidinggevende niet meer rechten aan de gebruiker toekent dan nodig is voor de uitoefening van zijn functie.

Ten aanzien van de toegang tot informatiesystemen geldt het volgende:

1. Toegang dient pas te worden verleend na authenticatie;
2. Toegang wordt verleend op basis van het persoonsgebonden instellingsaccount;
3. Classificatie van het informatiesysteem en of het informatiesysteem via internet te gebruiken is, bepaalt het vereiste LoA-niveau voor identificatie en authenticatie (zie Bijlage 2) en daarmee op welke wijze de instelling bij registratie de identiteit van de gebruiker moet vaststellen en de wijze van authenticatie (al dan niet multi-factor);
4. Tenminste LoA2 (2-factor authenticatie) is vereist voor informatiesystemen die via internet te gebruiken zijn èn vertrouwelijke of hoger geclassificeerde informatie verwerken.
5. Toegang tot besturingssystemen geschiedt op basis van LoA3 (2-factor authenticatie);
6. De instelling werkt zoveel mogelijk met standaard gebruikersprofielen voor veel voorkomende rollen, met beperkte toegangsrechten[13].
7. Bijzondere rechten moeten afdoende zakelijk gemotiveerd en terughoudend toegekend worden. De Toegekende bijzondere rechten worden geadministreerd, onder verantwoordelijkheid van de Eigenaar.
8. Alle gevoelige mutaties in informatiesystemen zijn, voor zover technisch mogelijk, herleidbaar naar een persoonsgebonden instellingsaccount;
9. Raadpleging van geheime informatie dient herleidbaar te zijn naar een persoonsgebonden instellingsaccount;
10. Toegang via niet-persoonsgebonden accounts, zoals groepsaccounts, is - behoudens incidentele geautoriseerde uitzonderingen - niet toegestaan. Zie verder Paragraaf 11.5.2.
11. De instelling streeft naar een centraal 2-factor authenticatiesysteem voor al haar informatiesystemen.

Toegangsrechten dienen zo snel mogelijk na vertrek van medewerkers of wisseling van functie te worden ingetrokken.

Directeur ICTS beoordeelt periodiek het toegangsbeleid en de toegangsbeveiliging. Leidinggevenden beoordelen periodiek de toegangsrechten van hun medewerkers.

11.2 Beheer van toegangsrechten van gebruikers

Doelstelling:
Toegang voor bevoegde gebruikers bewerkstelligen en onbevoegde toegang tot informatiesystemen voorkomen.

[13] Toegangsrechten zijn efficiënter en effectiever te beheren via gebruikersprofielen dan via individueel in te stellen rechten.

11.2.1 Registratie van gebruikers

Er behoren formele procedures voor het registreren en afmelden van gebruikers te zijn vastgesteld, voor het verlenen en intrekken van toegangsrechten tot alle informatiesystemen en -diensten.

De instelling kent beheerprocedures voor 1) het aanmelden, registreren en afmelden van gebruikers en 2) het toekennen en intrekken van toegangsrechten, voor UvAnet/HvAnet en diverse bedrijfstoepassingen (zoals SAP en Corsa). Dit soort procedures behandelen onder meer:

1. Wijze van registratie, met name vaststelling en verificatie van de identiteit van de gebruiker overeenkomstig het toepasselijke Level of Assurance (LoA, zie bijlage 2);
2. Autorisatie (ligt bij de Eigenaar en/of de leidinggevende) en controle hierop (verificatie);
3. Registratievorm: ICTS registreert voor veel toepassingen de gebruikers in een centraal IDM-systeem;
4. Het gebruik van een persoonsgebonden instellingsaccount, zodat handelingen kunnen worden herleid tot individuele gebruikers en gebruikers verantwoordelijk kunnen worden gesteld voor gepleegde handelingen;
5. Controle op toepasselijkheid van toegangsrechten (niet te hoog in verhouding tot de functie en toepassing);
6. Controle op conflicten door toekenning van toegangsrechten (zoals het in gevaar brengen van functiescheiding);Schoning inclusief periodieke controle op en verwijderen of blokkeren van overtollige gebruikers;
7. Aansluiting op procedures zoals 'uit dienst' en ‘wijziging van functie’ (voor het zo snel mogelijk intrekken of blokkeren van toegangsrechten van gebruikers die van functie of rol zijn veranderd of de instelling hebben verlaten);
8. Autorisatie van niet-persoonsgebonden accounts (zie paragraaf 11.5.2);
9. Het aanreiken van de Acceptable Use Policy (AUP) en ICT-gedragsregels aan de gebruiker en akkoordverklaring.

Slechts na identificatie aan de hand van een geldig identiteitsbewijs[14], in persoon (face-to-face) en al dan niet direct of indirect via een gezaghebbende instellingsbron zoals SAP, wordt het persoonsgebonden instellingsaccount aangemaakt en de gebruiker met bijbehorende authenticatiemiddelen aangereikt;

Ook accounts voor externe gebruikers mogen slechts worden aangemaakt en toegangsrechten mogen slechts worden ingesteld, nadat de beheerprocedures geheel zijn doorlopen.

11.2.2 Beheer van speciale bevoegdheden

De toewijzing en het gebruik van speciale bevoegdheden behoren te worden beperkt en beheerst.

Toewijzing en wijziging van speciale bevoegdheden - zoals benodigd voor technisch beheer - verloopt via een formele autorisatieprocedure (zelfde als de normale procedure).

Speciale bevoegdheden (zoals toegang tot bijzondere applicaties en commando’s) worden terughoudend toegekend, alleen als zij noodzakelijk zijn voor de uitoefening van de functie (“least privilege”). Zakelijke motivatie is daarbij nodig.

Speciale bevoegdheden worden geregistreerd. De autorisatieprocedure dient te zijn voltooid alvorens gebruik mag worden gemaakt van de bevoegdheden.

Voor speciale bevoegdheden in informatiesystemen worden aparte accounts gebruikt, zoals accounts voor functioneel beheer en technisch beheer. Beheerders:

1. Hebben een 'normaal' account voor reguliere kantooractiviteiten en een apart account voor het plegen van beheer;
2. Gebruiken standaard het normale account;
3. Gebruiken het beheeraccount alleen voor het plegen van een of meer beheerhandelingen, waarna zij direct uitloggen[15] en verder zo minimaal mogelijk;
4. Kunnen aan hun scherm zien of zij onder een beheeraccount of een normaal account zijn ingelogd.

Bijzondere accounts mogen niet onderling worden gedeeld. Afwijking van deze regel moet gepaard gaan met een afdoende schriftelijke en zakelijke motivatie.

---

[14] Identiteitskaart, paspoort of rijbewijs.

[15] 'Normale' werkzaamheden, zoals het documenteren van wijzigingen, behoren niet via een beheeraccount te worden gepleegd.

Systeemprocessen draaien onder een eigen systeemaccount en hebben niet meer rechten dan strikt nodig (“least privilege”).

Direct leidinggevenden zijn verantwoordelijk voor het (laten) intrekken van overbodig c.q. ongewenst geworden bevoegdheden bij verandering van rol, functie of afdeling.

11.2.3 Beheer van gebruikerswachtwoorden

De toewijzing van wachtwoorden behoort met een formeel beheerproces te worden beheerst.

Er is een wachtwoordregeling van kracht[16].

Voordat een gebruiker een nieuw token, toegangscode of (tijdelijk) wachtwoord wordt verstrekt, dient eerst zijn identiteit te zijn gecontroleerd aan de hand van een geldig legitimatiebewijs (paspoort, rijbewijs of identiteitskaart).

Bij het aanmaken van een nieuw wachtwoord of bij verlies van een wachtwoord, wordt een wachtwoord voor eenmalige toegang gegenereerd, met als doel dat de gebruiker zo spoedig mogelijk na ontvangst een nieuw persoonlijk wachtwoord kan instellen. Gebruikers moeten gedwongen zijn voorafgaand aan verder gebruik eerst het tijdelijke wachtwoord te wijzigen.

Tijdelijke wachtwoorden moeten voldoen aan de wachtwoordregeling, uniek voor een gebruiker zijn, op een veilige manier worden aangereikt aan de gebruiker en moeten een beperkte geldigheidsduur hebben.

Gebruikers mogen hun wachtwoorden nimmer onbeveiligd in leesbare vorm (digitaal) opslaan (nergens in: niet in wachtwoordlijsten, configuratiebestanden, programmacode, et cetera) of zichtbaar nabij de werkplek tonen. Het gebruik van een digitale wachtwoordenkluis is toegestaan, mits deze op veiligheid is getest en is beveiligd middels 2-factor authenticatie (bij voorkeur) of een sterk wachtwoord.

Wachtwoorden mogen niet in leesbare vorm worden getransporteerd door een netwerk.

Als opslag of transport noodzakelijk is, dient een kwalitatief hoogwaardig hash- of encryptie-algoritme te worden gebruikt.

Standaardwachtwoorden van systemen en software dienen direct na installatie te worden gewijzigd.

ICTS bewaart belangrijke sleutels en wachtwoorden van systeemaccounts in een veilig digitaal wachtwoordmanagementsysteem[17] en hanteert vastgestelde procedures voor toegang tot en het up-to-date houden van de wachtwoorden.

Hoe gebruikers dienen om te gaan met de middelen die hen zijn verstrekt voor het verkrijgen van toegang tot het netwerk en bedrijfstoepassingen (token, toegangscode en/of wachtwoorden) is door ICTS verwoord in de Acceptable Use Policy (AUP) en de ICT-gedragsregels.

Wachtwoorden hebben een geldigheidsduur van maximaal 1 jaar en mogen niet binnen 5 keer opnieuw gebruikt worden.

Het centrale IDM-systeem dwingt complexiteitseisen voor wachtwoorden af. Aan gebruikers wordt tijdig gemeld dat het wachtwoord verloopt.

11.2.4 Beoordeling van toegangsrechten van gebruikers

De directie behoort de toegangsrechten van gebruikers regelmatig te beoordelen in een formeel proces.

Eigenaren zijn verantwoordelijk voor het jaarlijks beoordelen van de inrichting en het gebruik van toegangsrechten tot hun informatie. Hierbij wordt aandacht besteed aan rollen/functiegroepen (te veel/weinig), toegekende rechten (vereiste functiescheiding, “least privilege”, te veel/weinig), niet-persoonsgebonden accounts (zo min mogelijk), et cetera.

---

16 “Wachtwoordregeling UvA en HvA” dd. 20 juni 2014.
17 Enterprise Password Management System (EPMS).

11.3 Verantwoordelijkheden van gebruikers

Doelstelling:
Voorkomen van onbevoegde toegang door gebruikers, en van beschadiging of diefstal van informatie en IT-voorzieningen.

11.3.1 Gebruik van wachtwoorden

Gebruikers behoren goede beveiligingsgewoontes in acht te nemen bij het kiezen en gebruiken van wachtwoorden.

Om toegang te krijgen tot de ICT-diensten van de instelling moet de gebruiker inloggen via normale authenticatie.

Het centrale IDM-systeem dwingt een goede kwaliteit van wachtwoorden technisch af conform de wachtwoordregeling (complexiteit, minimale lengte). Daarnaast reikt ICTS gebruikers ten minste de volgende gedragsregels aan:

1. Deel je persoonlijke account niet met anderen. Houd persoonlijke toegangscodes, wachtwoorden e.d. voor jezelf (geheim);
2. Wijzig het wachtwoord direct als je vermoedt dat het is uitgelekt;
3. Gebruik moeilijk te raden toegangscodes en wachtwoorden;
4. Wijzig je wachtwoorden tenminste eenmaal per jaar (advies: elke drie maanden). Informatiesystemen dienen dit zoveel mogelijk af te dwingen. Voor accounts met speciale rechten (zoals accounts voor technisch en functioneel beheer) gelden striktere regels gespecificeerd in de wachtwoordregeling;
5. Schrijf wachtwoorden nooit op;
6. Bewaar wachtwoorden nimmer in een browser. Gebruik eventueel een digitale wachtwoordenkluis, mits deze op veiligheid is getest en is beveiligd middels 2-factor authenticatie (bij voorkeur) of een sterk wachtwoord;
7. Gebruik wachtwoorden niet in automatische inlogprocedures, zoals onder een functietoets of in een macro;
8. Gebruik wachtwoorden die je voor de instelling gebruikt niet elders (zoals privé of bij een andere werkgever) en andersom;
9. Overtuig jezelf ervan dat je je gebruikersnaam en wachtwoord alleen invoert op webpagina's die van de instelling zijn.

ICTS voorziet in een veilige reset-procedure voor wachtwoorden.

11.3.2 Onbeheerde gebruikersapparatuur

Gebruikers behoren te bewerkstelligen dat onbeheerde apparatuur passend is beschermd.

Systemen dienen, ongeacht wie ze beheert, voorzien te zijn van automatische vergrendeling die na 15 minuten inactiviteit in werking treedt (= passieve vergrendeling). ICTS voorziet de door haar beheerde systemen van een automatische vergrendeling;

De instelling verlangt van gebruikers dat zij hun sessie vergrendelen zodra zij hun werkplek voor langere duur verlaten (= actieve vergrendeling).

Voor mobiele apparatuur zoals laptops, tablets en smartphones geldt bovendien:

1. Gebruikers zijn verantwoordelijk voor apparatuur die zij onbeheerd achterlaten.
2. Gebruikers dienen apparatuur veilig achter te laten, zo veel mogelijk:
    a. Achter slot en grendel;
    b. Uit het zicht;
    c. Vastgeketend;
    d. Na het systeem te hebben uitgezet, te zijn uitgelogd of de schermvergrendeling te hebben geactiveerd.

Tablets en smartphones dienen automatisch te vergrendelen na 5 minuten niet te zijn gebruikt.

Een en ander is door ICTS verder uitgewerkt in de Gebruiksvoorwaarden Mobiele Apparatuur.

11.3.3 'Clean desk' - en 'clear screen' -beleid

Er behoort een 'clean desk' beleid voor papier en verwijderbare opslagmedia en een 'clear screen' beleid voor IT-voorzieningen te worden ingesteld.

Clean desk regel
Gebruikers worden geacht waardevolle bedrijfsmiddelen achter slot en grendel op te bergen alvorens ze de werkplek voor langere duur verlaten en zelf niet (langer)voldoende toezicht kunnen houden (zoals voor een overleg, lunch of aan het einde van de werkdag). Het gaat hierbij om:

1. Documenten met vertrouwelijke of geheime informatie;
2. Informatie die door contractuele verplichtingen of wet- en/of regelgeving bescherming behoeft;
3. Alle soorten authenticatiemiddelen zoals: sleutels, smartcards en pasjes, maar ook gegevensdragers, tablets, smartphones, et cetera.

De clean desk regel geldt ook voor plekken waar vertrouwelijke informatie zich onbeheerd kan ophopen, zoals bij multifunctionals, postbussen (-bakken/-vakken) en in vergaderzalen (gezamenlijke verantwoordelijkheid).

Bij afdrukken van niet-publieke informatie wordt gebruik gemaakt van beveiligd printen.

De instelling draagt zorg voor voldoende bergmiddelen.

Clear screen regel
Zie Beheersmaatregel 11.3.2 Onbeheerde Gebruikersapparatuur. Daarnaast dienen gebruikers zodanig met informatie op schermen om te gaan dat kennisname door niet bevoegden wordt tegengegaan.

Algemeen
De instelling brengt de clean desk regel en clear screen regel regelmatig onder de aandacht van de gebruiker. De direct leidinggevende is verantwoordelijk voor toezicht op naleving.

11.4 Toegangsbeheersing voor netwerken

Doelstelling:
Het voorkomen van onbevoegde toegang tot netwerkdiensten.

11.4.1 Beleid ten aanzien van het gebruik van netwerkdiensten

Gebruikers behoort alleen toegang te worden verleend tot diensten waarvoor ze specifiek bevoegd zijn.

'Netwerkdiensten' zijn diensten die voor netwerkconnectiviteit[18] zorgen.

Het toegangsbeleid (zie paragraaf 11.1.1) is tevens op netwerkdiensten van toepassing. Dit betekent dat gebruikers zich dienen te authentiseren alvorens gebruik te maken van het instellingsnetwerk. Bepaalde segmenten van het instellingsnetwerk zijn uitsluitend bedoeld voor vertrouwde systemen. In dat geval is tevens authenticatie van het systeem vereist.

Gebruikers van netwerkdiensten dienen te verklaren zich te houden aan de Acceptable Use Policy en de ICT-gedragsregels.

11.4.2 Authenticatie van gebruikers bij externe verbindingen

Er behoren geschikte authenticatiemethoden te worden gebruikt om toegang van gebruikers op afstand te beheersen.

Systemen die in beginsel niet rechtstreeks toegankelijk zijn vanaf het Internet, zijn uitsluitend bereikbaar via VPN. De toegangsbeveiliging van VPN vindt tenminste plaats op basis van het persoonsgebonden instellingsaccount.

[18] Denk aan het toestaan van diensten als http, https, vpn (LAN-access), citrix, ssh (nimmer telnet), e-mail, instant messaging, voip, et cetera.

Voor het verkrijgen van toegang tot bedrijfskritische informatiesystemen via VPN geldt tenminste LoA2 (2-factor authenticatie, zie Bijlage 2).

11.4.3 Identificatie van netwerkapparatuur

Automatische identificatie van apparatuur behoort te worden overwogen als methode om verbindingen vanaf specifieke locaties en apparatuur te authentiseren.

Wel of niet toepassen van automatische identificatie van apparatuur is de verantwoordelijkheid van de Eigenaar.

11.4.4 Bescherming op afstand van poorten voor diagnose en configuratie

De fysieke en logische toegang tot poorten voor diagnose en configuratie behoort te worden beheerst.

Fysiek
Door ICTS beheerde centrale systemen zijn gehuisvest in een beveiligde serverruimte of datacenter (zie 9.1.1). Apparatuur bevindt zich standaard in een vergrendelde toestand, zodat toegang via het toetsenbord en monitor voor een onbevoegde niet mogelijk is.

Logisch
Voor het beheersen van logische toegang op afstand tot poorten voor diagnose en configuratie past ICTS de volgende richtlijnen toe:

1. Beheer op afstand vindt plaats op basis van LoA3 (2-factor authenticatie);
2. Toegang is alleen mogelijk vanaf de beheersystemen op het beheersegment;
3. Alleen de poorten die nodig zijn voor beheer op afstand zijn actief. ICTS deactiveert poorten en voorzieningen voor beheer op afstand, die niet actief worden gebruikt;
4. Als ondersteuning op afstand door een leverancier noodzakelijk is, maakt ICTS dit slechts voor de duur van de ondersteuning mogelijk en alleen voor het te ondersteunen systeem.

11.4.5 Scheiding van netwerken

Groepen informatiediensten, gebruikers en informatiesystemen behoren op netwerken te worden gescheiden.

Voor het beveiligen van het netwerk wordt het netwerk opgesplitst in afzonderlijke logische segmenten met een gelijk functioneel doel en/of gelijk gebruiksrisico[19].

Verkeer tussen de verschillende segmenten is alleen toegestaan indien noodzakelijk en legitiem (‘deny by default’).

Ten behoeve van netwerkbeheer dient voorzien te zijn in middelen om de hoeveelheid en aard van het netwerkverkeer op en tussen de verschillende segmenten te kunnen monitoren.

Operationeel beleid omtrent verkeer tussen segmenten is vastgesteld (met o.a. ‘deny by default’, logging, inspectie).

ICTS houdt bij van informatiesystemen in welk segment ze zijn geplaatst.

Wijzigingen in de toegang op netwerkniveau ten opzichte van de oorspronkelijke inrichting zijn alleen mogelijk na instemming van de Eigenaar en een positief advies van de ISM.

Er wordt periodiek, minimaal één keer per twee jaar, geëvalueerd of een informatiesysteem zich nog steeds in het juiste segment bevindt dan wel of deze verplaatst dient te worden.

[19] Voor het vaststellen van het gebruiksrisico wordt de standaard classificatiemethode toegepast.

11.4.6 Beheersmaatregelen voor netwerkverbindingen

Voor gemeenschappelijke netwerken, vooral waar deze de grenzen van de organisatie overschrijden, behoren de toegangsmogelijkheden voor gebruikers te worden beperkt, overeenkomstig het toegangsbeleid en de eisen van bedrijfstoepassingen.

Waar nodig beperkt ICTS de connectiviteit op netwerk- en/of applicatieniveau via technieken zoals routering, netwerkfiltering (op bron- en bestemmingsadressen en -poorten), adrestranslatie, firewalling, proxying en filtering op applicatieniveau (bijvoorbeeld via URL-blacklisting). ICTS is hierbij verantwoordelijk voor een robuuste invulling.

Op applicatieniveau kan aanvullend validatie van de gebruiker (authenticatie) plaatsvinden.

11.4.7 Beheersmaatregelen voor netwerkroutering

Netwerken behoren te zijn voorzien van beheersmaatregelen voor netwerkroutering, om te bewerkstelligen dat computerverbindingen en informatiestromen niet in strijd zijn met het toegangsbeleid voor de bedrijfstoepassingen.

Door middel van technieken op netwerkniveau beheerst ICTS de door het netwerk geboden connectiviteit in overeenstemming met het toegangsbeleid. De mate van beheersing wordt periodiek, minimaal één keer per twee jaar, getoetst.

Op de koppelvlakken met externe netwerken worden maatregelen getroffen om alleen valide netwerkverkeer te routeren door bijvoorbeeld IP-spoofing onmogelijk te maken. Routeringsgegevens worden alleen met vertrouwde partijen uitgewisseld.

11.5 Toegangsbeveiliging voor besturingssystemen

Doelstelling:
Voorkomen van onbevoegde toegang tot besturingssystemen.

11.5.1 Beveiligde inlogprocedures

Toegang tot besturingssystemen behoort te worden beheerst met een beveiligde inlogprocedure.

Inlogprocedures dienen (in het algemeen) aan de volgende richtlijnen te voldoen (minimale eis voor alle informatiesystemen):

1. Toegang tot besturingssystemen vindt tenminste plaats op basis van LoA3 (2-factor authenticatie, zie Bijlage 2);
2. Toegangscode/wachtwoord wordt niet getoond en nimmer onversleuteld over het netwerk verzonden (dit sluit bijvoorbeeld het gebruik van telnet uit);
3. Het systeem geeft geen systeemgegevens of hulpberichten prijs voordat het inloggen met succes is voltooid;
4. Bij het inloggen toont het systeem:
    a. Een melding dat het systeem uitsluitend mag worden gebruikt door geautoriseerde gebruikers;
    b. Wanneer voor het laatst door de gebruiker is ingelogd;
5. Validatie vindt pas plaats nadat alle gegevens die nodig zijn voor het inloggen, zijn ingevuld. Het systeem verstrekt geen informatie m.b.t. fouten;
6. Inlogpogingen worden gelogd. Afwijkend inloggedrag wordt gesignaleerd.

Om brute-force aanvallen te weerstaan is een blokkeringsmechanisme ingesteld, dat in werking treedt na een aantal mislukte inlogpogingen.

11.5.2 Gebruikersidentificatie en -authenticatie

Elke gebruiker behoort over een unieke identificatiecode te beschikken (gebruikers-ID) voor uitsluitend persoonlijk gebruik, en er behoort een geschikte authenticatietechniek te worden gekozen om de geclaimde identiteit van de gebruiker te bewijzen.

Zie Paragrafen 11.2.1, 11.2.2 en 11.2.3.

Gebruikers krijgen beschikking over een persoonsgebonden instellingsaccount. Dit account is uitsluitend voor persoonlijk gebruik bedoeld. Gelogde handelingen zijn hierdoor te herleiden tot de gebruiker die de handeling feitelijk heeft gepleegd.

Toegang via niet-persoonsgebonden accounts is - behoudens incidentele geautoriseerde uitzonderingen - niet toegestaan omdat dit herleiding naar een natuurlijk persoon onmogelijk maakt. Voor eventuele niet-persoonsgebonden accounts geldt:

1. Er dient een zakelijke grondslag te zijn. Baten dienen aantoonbaar te zijn;
2. Een alternatieve werkwijze is niet mogelijk om technische redenen of vanwege hoge kosten;
3. De Eigenaar van het betreffende informatiesysteem autoriseert niet-persoonsgebonden accounts. Voor informatiesystemen die gebruik maken van het centrale IDM-systeem autoriseert de IDM-systeemeigenaar in samenspraak met de ISO en /of ISM;
4. De rechten van het niet-persoonsgebonden account worden zoveel mogelijk ingeperkt;
5. Het account kent een verantwoordelijke;
6. Het account heeft een beperkte geldigheidsduur.

De Eigenaar documenteert de toestemming of afwijzing, de zakelijke grondslag, wie verantwoordelijk is voor het niet-persoonsgebonden account en de geldigheidsduur.

11.5.3 Systemen voor wachtwoordbeheer

Systemen voor wachtwoordbeheer behoren interactief te zijn en moeten bewerkstelligen dat wachtwoorden van geschikte kwaliteit worden gekozen.

De instelling maakt voor wachtwoordbeheer gebruik van een centraal IDM-systeem. De volgende functionaliteit is vereist:

1. Mogelijkheid tot wijziging van het wachtwoord;
2. Afdwingen van de juiste kwaliteit van door de gebruiker gekozen wachtwoord;
3. Beletten van hergebruik;
4. Gedwongen periodieke wijziging van wachtwoord;
5. Afdwingen wijziging tijdelijke (initiële) toegangscode bij eerste login;
6. Mechanisme om te voorzien in een veilige resetprocedure voor wachtwoorden;
7. Afgeschermde opslag van wachtwoorden via een kwalitatief hoogwaardig hash-algoritme (en dus niet omkeerbaar).

11.5.4 Gebruik van systeemhulpmiddelen

Het gebruik van hulpprogrammatuur waarmee systeem- en toepassingsbeheersmaatregelen zouden kunnen worden gepasseerd behoort te worden beperkt en behoort strikt te worden beheerst.

Het gebruik van tools, waarmee systemen kunnen beheerd, is een speciale bevoegdheid en moet als zodanig worden geautoriseerd. Verder zijn de volgende richtlijnen voor ICTS-beheerde systemen van kracht:

1. Voor het gebruik van systeemhulpmiddelen zijn speciale rechten nodig. Standaardgebruikers beschikken niet over deze rechten.
2. Rechten worden alleen aan gekwalificeerde gebruikers toegekend. De gebruiksduur dient te worden beperkt. Bij de toekenning dient rekening gehouden te worden met handhaving van functiescheiding.
3. Normale gebruikerssystemen (desktops en laptops) zijn zoveel mogelijk ontdaan van systeemhulpmiddelen.

11.5.5 Time-out van sessies

Inactieve sessies behoren na een vastgestelde periode van inactiviteit te worden uitgeschakeld.

Sessies worden na een vastgestelde periode van inactiviteit vergrendeld. Afhankelijk van het beveiligingsniveau en gebruikersgemak bepaalt de Eigenaar de periode in overleg met de ISO en/of ISM.

11.5.6 Beperking van verbindingstijd

De verbindingstijd behoort te worden beperkt als aanvullende beveiliging voor toepassingen met een verhoogd risico.

In geval van een verhoogd beveiligingsrisico bepaalt de Eigenaar de maximale verbindingstijd in overleg met de ISO en/of ISM.

11.6 Toegangsbeheersing voor toepassingen en informatie

Doelstelling:
Voorkomen van onbevoegde toegang tot informatie in toepassingssystemen.

11.6.1 Beperken van toegang tot informatie

Toegang tot informatie en functies van toepassingssystemen door gebruikers en ondersteunend personeel behoort te worden beperkt overeenkomstig het vastgestelde toegangsbeleid.

Via het realiseren van toegangsbeperkingen wordt het toegangsbeleid gehandhaafd en nageleefd. Eigenaren dragen hiervoor de eindverantwoordelijkheid.

Autorisaties op applicatieniveau worden volgens het “least privilege” beginsel verstrekt door of namens de Eigenaar, waarbij deze tevens rekening houdt met eventueel vereiste functiescheiding. Hiertoe wordt door de Eigenaar voor ieder informatiesysteem een procedure ingericht voor het aanvragen en verkrijgen van de benodigde autorisaties.

Uitgegeven toegangsrechten dienen zoveel mogelijk te worden beperkt (“least privilege”, zie paragraaf 11.1.1). Dit betekent ook dat de gebruikersregistraties (gebruikers + rechten) van informatiesystemen periodiek moeten worden geschoond.

Voor elk informatiesysteem (applicatie) voorziet de functioneel beheerder de corresponderende Eigenaar tenminste elk half jaar van een overzicht van gebruikers en uitgegeven (toegangs-)rechten. De Eigenaar controleert deze lijst kritisch en communiceert binnen een week de te plegen correcties naar de functioneel beheerder. De Eigenaar let op:

1. Gebruikers die uit dienst zijn;
2. Gebruikers die gewisseld zijn van functie en met minder of geen rechten toe kunnen;
3. Externe gebruikers waarvan het gebruik is beëindigd (indien van toepassing);
4. Wijzigingen in en validiteit van speciale bevoegdheden.

De functioneel beheerder voert benodigde correcties vervolgens binnen een dag uit.

Voor systemen met meer dan 50 gebruikers kan worden volstaan met een relevante steekproef. Leidinggevenden leveren een bijdrage via periodieke beoordeling van actuele toegangsrechten van gebruikers binnen hun team/afdeling.

Bij het ontwikkelen van nieuwe informatiesystemen of plegen van wijzigingen aan bestaande informatiesystemen dient de Eigenaar rekening te houden met het toegangsbeleid en draagt hij (eind)verantwoordelijkheid voor een correct functionerende toegangsbeperking.

11.6.2 Isoleren van gevoelige systemen

Gevoelige systemen behoren een eigen, vast toegewezen (geïsoleerde) computer omgeving te hebben.

ICTS huisvest door haar beheerde centrale systemen zonder uitzondering en ongeacht de gegeven classificatie in serverruimten en/of datacenters.

Onderlinge negatieve afhankelijkheid en/of beïnvloeding van informatiesystemen dient zoveel mogelijk te worden voorkomen, met name ten gevolge van:

Conflict / Risico	**Mogelijke maatregel(en)**
Verschil in classificatie (wezenlijk ander doel of belang)	Logische of fysieke scheiding door virtualisatie of huisvesting op aparte systemen (voorbeeld: een financiële toepassing niet op hetzelfde systeem als een onderwijstoepassing)
Netwerkcapaciteit	Switching, segmentering, gescheiden routering

Conflict / Risico	Mogelijke maatregel(en)
Processorcapaciteit	Huisvesting op aparte systemen, toekenning processorcapaciteit
Fraude	Huisvesting op apart, gereserveerd systeem (voorbeeld: gereserveerde terminal voor financiële transacties)
Uitval	Huisvesting op aparte systemen, gescheiden voeding
Beheer door verschillende partijen	Huisvesting op aparte systemen

ICTS is verantwoordelijk voor het correct, onafhankelijk functioneren van de diverse informatiesystemen en kan bij (dreigende) conflicten of risico's besluiten tot isolatie.

11.7 Draagbare computers en telewerken

Doelstelling:
Waarborgen van informatiebeveiliging bij het gebruik van draagbare computers en faciliteiten voor telewerken.

11.7.1 Draagbare computers en communicatievoorzieningen

Er behoort formeel beleid te zijn vastgesteld en er behoren geschikte beveiligingsmaatregelen te zijn getroffen ter bescherming tegen risico's van het gebruik van draagbare computers en communicatiefaciliteiten.

Ten aanzien van mobiele apparatuur gelden de volgende richtlijnen:

1. ICTS voorziet door haar beheerde mobiele apparatuur van toegangsbeveiliging, inclusief automatische vergrendeling;
2. Verwijderbare gegevensdragers zoals USB-sticks en externe harde schijven, en mobiele apparatuur zoals laptops, tablets en smartphones, mogen in beginsel niet worden gebruikt voor de opslag en/of verwerking van vertrouwelijke of geheime informatie. Als opslag noodzakelijk is, slaat de gebruiker dergelijke informatie uitsluitend versleuteld op;
3. Overdracht van vertrouwelijke of geheime informatie tussen mobiele apparatuur en systemen van de instelling vindt altijd plaats middels beveiligde communicatieprotocollen;
4. ICTS wijst gebruikers van mobiele apparatuur op de risico's van opslag van vertrouwelijke of geheime informatie op mobiele apparaten (bewustwording);
5. De gebruiker dient maatregelen te nemen om het risico van diefstal zoveel mogelijk te beperken.
6. Er is een procedure voor het melden en afhandelen van diefstal of verlies van door ICTS beheerde mobiele apparatuur.

Leenapparatuur
Als een gebruiker mobiele apparatuur van de instelling leent, mag hij op deze apparatuur geen vertrouwelijke of geheime informatie van de instelling bewaren[20], en is hij zelf verantwoordelijk voor het veiligstellen van gegenereerde informatie en bescherming tegen verlies en diefstal.

ICTS schoont uitgeleende apparatuur direct na retournering.

Privé apparatuur
De instelling staat vanwege de risico's die dit met zich meebrengt het gebruik van privé mobiele apparatuur onder de volgende voorwaarden toe:

1. De gebruiker zorgt er voor dat de privé apparatuur voldoende is beveiligd, met tenminste een toegangsbeveiliging (pincode, wachtwoord of iets dergelijks);
2. De gebruiker verwerkt geen vertrouwelijke of geheime informatie van de instelling op de privé apparatuur;
3. De privé apparatuur dient geen storingen te (kunnen) veroorzaken.

[20] Bij verlies dient de schade beperkt te zijn tot alleen de waarde van de apparatuur.

11.7.2 Telewerken

Er behoren beleid, operationele plannen en procedures voor telewerken te worden ontwikkeld en geïmplementeerd.

De instelling heeft een telewerkbeleid inclusief een Acceptable Use Policy (AUP) en ICT-gedragsregels. Dit telewerkbeleid behandelt onder meer onder welke voorwaarden thuiswerken of anderszins op afstand werken is toegestaan alsmede de wijze waarop de gebruiker wordt geautoriseerd om te telewerken, over welke middelen de gebruiker beschikking krijgt en welke zaken de gebruiker in acht dient te nemen (veilig werken, plichten en verantwoordelijkheden).

ICTS maakt ten behoeve van tijd- en plaatsonafhankelijk werken toegang op afstand, vanaf locaties buiten de instelling, mogelijk. Toegang via Internet is alleen mogelijk via speciaal daarvoor ingerichte voorzieningen zoals een instellings-VPN. Dit is een minimum eis – er kunnen aanvullende eisen worden gesteld aan de toegang en het gebruik.

Toegang tot informatiesystemen van de instelling, waarvoor het beveiligingsniveau gevoelig of hoger is, is in beginsel uitsluitend toegestaan vanaf “vertrouwde segmenten”. Voor toegang tot bedrijfsapplicaties is toestemming (autorisatie) van de Eigenaar nodig.

Met betrekking tot laptops, die niet door ICTS worden beheerd, geldt dat deze worden beschouwd als gelijk aan een willekeurig systeem op Internet. Deze systemen krijgen alleen toegang via speciaal daarvoor bestemde netwerksegmenten. Deze netwerksegmenten worden niet beschouwd als vertrouwde segmenten van het UvAnet/HvAnet.

12 Verwerving, ontwikkeling en onderhoud van informatiesystemen

12.1 Beveiligingseisen voor informatiesystemen

Doelstelling:
Bewerkstelligen dat beveiliging integraal deel uitmaakt van informatiesystemen.

12.1.1 Analyse en specificatie van beveiligingseisen

In bedrijfseisen voor nieuwe informatiesystemen of uitbreidingen van bestaande informatiesystemen behoren ook eisen voor beveiligingsmaatregelen te worden opgenomen.

Als er sprake is van:

- verwerving van nieuwe informatiesystemen via aanschaf of uitbesteding, of van
- ontwikkeling van nieuwe informatiesystemen of grote wijzigingen aan bestaande informatiesystemen, waaronder uitbreidingen,

wordt onder verantwoordelijkheid van de Eigenaar met betrokkenheid van de ISO en/of ISM, in een vroeg stadium een classificatie van het informatiesysteem uitgevoerd wat betreft beschikbaarheid, integriteit en vertrouwelijkheid.

Voor beveiligingsklasse “standaard” en “gevoelig” kan worden volstaan met beveiligingseisen conform deze baseline. Is sprake van beveiligingsklasse “kritiek” dan dient met betrokkenheid van de ISO en/of ISM een aanvullende risicoanalyse te worden uitgevoerd. Deze risico-afweging resulteert in gedocumenteerde, aanvullend te stellen en te beantwoorden beveiligingseisen.

Alle gestelde beveiligingseisen (baseline en aanvullend) maken deel uit van de acceptatiecriteria (Projectdossier Informatiebeveiliging, zie 10.3.1) en dienen in balans te zijn met de waarde van de informatie en het informatiesysteem voor de organisatie en de kans op en mogelijke negatieve gevolgen van een aantasting van beschikbaarheid, integriteit en/of vertrouwelijkheid.

Standaard inrichtingseisen
ICTS kent standaardeisen voor de inrichting van nieuwe (productie)systemen, waaronder:

1. ICTS werkt zoveel mogelijk met inrichtingsstandaarden voor veel gebruikte systemen (zoals verschillende servers, serverapplicaties, desktops en netwerkapparatuur);
2. Na installatie dienen standaardwachtwoorden direct te worden gewijzigd;
3. Direct inloggen op een account met beheerdersrechten dient niet mogelijk te zijn;
4. Systemen dienen zoveel mogelijk te worden ontdaan van overbodige functionaliteit, services, programmatuur, et cetera;
5. Eisen m.b.t. back-up van gegevens (zie 10.5.1), (installatie van) beveiligingspatches (zie 12.6.1), bestrijding van malware (zie 10.4.1), logging en monitoring (zie onder meer 10.10), authenticatie van gebruikers en beheerders (zie 11.5) en capaciteitsbeheer (zie 10.3.1).

ICTS baseert inrichtingsstandaarden[21] op betrouwbare best-practice bronnen, o.a. van kenniscentra (zoals CIS Security Benchmarks, NCSC en NIST), softwareproducenten en leveranciers. Indien mogelijk wordt de correcte inrichting en configuratie met behulp van een hulpmiddel geverifieerd (zoals de Microsoft Baseline Security Analyzer, MBSA).

Beveiligingseisen Webapplicaties
Als er sprake is van verwerving of ontwikkeling van webapplicaties, ziet de Eigenaar er op toe dat voldaan wordt aan ICT-beveiligingsrichtlijnen voor webapplicaties van het Nationaal Cyber Security Centrum (NCSC) en de OWASP Top 10 (www.owasp.org). Deze richtlijnen vormen een leidraad voor het veiliger ontwikkelen, beheren

[21] Een inrichtingsstandaard is de vertaling van richtlijnen en uitgangspunten naar gedocumenteerde, concrete te plegen instellingen in het besturingssysteem (zoals Windows, Linux, OSX, IOS), mailservers (zoals MS Exchange), directory-servers (LDAP, AD), fileservers, printservers, etcetera.

en aanbieden van webapplicaties en bijbehorende infrastructuur. De beveiligingsrichtlijnen zijn breed toepasbaar voor ICT- oplossingen die gebruik maken van webapplicaties[22].

Bij uitbesteding
Als er sprake is van uitbesteding (van systeemontwikkeling) of aanschaf van kant en klare oplossingen, ziet de Eigenaar er op toe dat:

1. De formele inkoopprocedure wordt gevolgd;
2. De aanschaf van gecertificeerde producten of diensten wordt overwogen;
3. Te stellen beveiligingseisen worden opgenomen in contracten met leveranciers;
4. Voorafgaand aan aanschaf het voldoen aan beveiligingseisen getest en geëvalueerd wordt en dat op basis van resultaten van aanschaf kan worden afgezien. De beslissing hieromtrent en de acceptatie van risico ligt bij de Eigenaar;
5. De risico's die voortkomen uit overtollige functionaliteit beoordeeld en zo nodig opgelost worden.

12.2 Correcte verwerking in toepassingen

Doelstelling:
Voorkomen van fouten, verlies, onbevoegde modificatie of misbruik van informatie in toepassingen.

12.2.1 Validatie van invoergegevens

Gegevens die worden ingevoerd in toepassingen behoren te worden gevalideerd om te bewerkstelligen dat deze gegevens juist en geschikt zijn.

Er moeten controles worden uitgevoerd op de invoer van gegevens.

De controles worden geautomatiseerd uitgevoerd door het betreffende informatiesysteem en/of worden handmatig uitgevoerd door gebruikers die (geautoriseerd) bij het invoerproces zijn betrokken.

Daarbij wordt minimaal gecontroleerd op grenswaarden, ongeldige tekens, onvolledige gegevens, gegevens die niet aan het juiste format voldoen (syntax controles) en inconsistentie van gegevens (verbandscontroles).

12.2.2 Beheersing van interne gegevensverwerking

Er behoren validatiecontroles te worden opgenomen in toepassingen om eventueel corrumperen van informatie door verwerkingsfouten of opzettelijke handelingen te ontdekken.

In informatiesystemen dienen voldoende (geautomatiseerde) functies te bestaan om verwerkings- en andere fouten, ook opzettelijke, in reeds ingevoerde gegevens te kunnen detecteren en corrigeren.

12.2.3 Integriteit van berichten

Er behoren eisen te worden vastgesteld, en geschikte beheersmaatregelen te worden vastgesteld en geïmplementeerd, voor het bewerkstelligen van authenticiteit en het beschermen van integriteit van berichten in toepassingen.

In informatiesystemen met integriteitsclassificatie "gevoelig" en hoger dienen maatregelen te worden genomen, zoals encryptie en/of digitale handtekening, om de authenticiteit en integriteit (juistheid en volledigheid) te waarborgen van berichten die worden uitgewisseld.

[22] Het document "ICT-beveiligingsrichtlijnen voor webapplicaties deel 1" bevat een beschrijving van de beveiligingsrichtlijnen op hoofdlijnen. In deel 2 worden de maatregelen verder uitgewerkt en gedetailleerd met voorstellen voor inrichting, beheer en ontwikkeling.

12.2.4 Validatie van uitvoergegevens

Gegevensuitvoer uit een toepassing behoort te worden gevalideerd, om te bewerkstelligen dat de verwerking van opgeslagen gegevens op de juiste manier plaatsvindt en geschikt is gezien de omstandigheden.

De uitvoerfuncties van informatiesystemen maken het mogelijk om de volledigheid en juistheid van de uitgevoerde gegevens te kunnen vaststellen (bijvoorbeeld door vierkantscontroles, checksums).

Bij uitvoer van gegevens wordt er voor gezorgd dat deze met het juiste niveau van vertrouwelijkheid beschikbaar gesteld worden (bijvoorbeeld via beveiligd printen).

Alleen gegevens die een gebruiker nodig heeft voor de uitvoering van zijn opgedragen werkzaamheden worden uitgevoerd (need to know).

12.3 Cryptografische beheersmaatregelen

Doelstelling:
Beschermen van de vertrouwelijkheid, authenticiteit of integriteit van informatie met behulp van cryptografische middelen.

12.3.1 Beleid voor het gebruik van cryptografische beheersmaatregelen

Er behoort beleid te worden ontwikkeld en geïmplementeerd voor het gebruik van cryptografische beheersmaatregelen voor de bescherming van informatie.

Bij de inzet van cryptografische middelen dient een afweging te worden gemaakt van de risico's aangaande locaties, processen en behandelende partijen in relatie tot de te beveiligen gegevens.

Hierbij kan gebruik gemaakt worden van de tabel met beveiligingseisen in Paragraaf 7.2.

De cryptografische beveiligingsvoorzieningen dienen blijvend te voldoen aan algemeen gangbare beveiligingscriteria (zoals FIPS 140-2).

12.3.2 Sleutelbeheer

Er behoort sleutelbeheer te zijn vastgesteld ter ondersteuning van het gebruik van cryptografische technieken binnen de organisatie.

Als cryptografische sleutels worden gebruikt, dient hiervoor beheer te worden ingericht.

De beheerder draagt zorgt voor:

1. Het genereren en tijdig intrekken c.q. deactiveren van interne (logische) sleutels en certificaten inclusief het genereren en/of plaatsen van certificaten op smartcards. Certificaten dienen aan een beperkte geldigheidsduur onderhevig te zijn;
2. Het zorgvuldig beheren van certificaten verkregen van externe partijen;
3. Het verspreiden van certificaten onder geautoriseerde gebruikers;
4. Het bijhouden van een registratie van sleutels en certificaten, inclusief geldigheidsduur;
5. Het bewaken van de geldigheidsduur en tijdig actualiseren van sleutels en certificaten;
6. Het fysiek beschermen van systemen die worden gebruikt bij het genereren, opslaan en archiveren van sleutelparen en certificaten;
7. Het registreren (in een logbestand) en beoordelen van activiteiten die verband houden met sleutelbeheer.

Er dient een procedure vastgesteld te zijn waarin is bepaald hoe de instelling omgaat met gecompromitteerde sleutels.

12.4 Beveiliging van systeembestanden

Doelstelling:
Beveiliging van systeembestanden bewerkstelligen.

12.4.1 Beheersing van operationele programmatuur

Er behoren procedures te zijn vastgesteld om de installatie van programmatuur op productiesystemen te beheersen.

De installatie van software op productiesystemen dient te worden beheerst om het risico van verstoringen tot een minimum te beperken. Daarvoor zijn de volgende richtlijnen van kracht:

1. Installatie van software op de productieomgeving vindt alleen plaats wanneer er een zakelijke aanleiding of een anderszins dwingende reden toe is;
2. Software-installaties op productiesystemen worden nimmer automatisch bijgewerkt. Dit geldt zowel voor upgrades als updates;
3. Installatie vindt uitsluitend plaats na goedkeuring nadat alle (acceptatie)tests met positief resultaat zijn doorlopen;
4. ICTS documenteert en verwerkt uitgevoerde installaties conform de vastgestelde Change Management procedure;
5. ICTS identificeert en beoordeelt vooraf de risico's gemoeid met installatie van software. Risicovollere installatiewijzigingen worden uitgevoerd aan de hand van een plan met een vooraf opgesteld terugdraaiscenario;
6. Productiesystemen bevatten alleen goedgekeurde software. Ontwikkel- of testversies zijn niet toegestaan;
7. Voorafgaand aan installatie vergewist ICTS zich van de veiligheid en robuustheid van nieuwe versies en patches;
8. ICTS neemt installatie-aanwijzingen en -instructies van leveranciers in acht;
9. ICTS houdt afdoende rekening met de beschikbaarheid van ondersteuning door leveranciers en de risico's van het werken met niet-ondersteunde programmatuur;
10. ICTS bewaakt en controleert installaties uitgevoerd door leveranciers.

12.4.2 Bescherming van testdata

Testgegevens behoren zorgvuldig te worden gekozen, beschermd en beheerst.

Voor testdata gelden de volgende richtlijnen:

1. Testdata dient speciaal voor het testdoel te zijn samengesteld en dient een zo getrouw mogelijke weergave te zijn van de operationele gegevens uit de productieomgeving;
2. De toegang tot belangrijke of gevoelige testdata is via een logische en fysieke toegangsbeveiliging afdoende beveiligd.
3. Gegevens, die als vertrouwelijk of hoger geclassificeerd zijn, gebruiken als testgegevens dient zoveel mogelijk te worden vermeden. Als het om gegronde redenen toch noodzakelijk is om met dit soort gegevens te testen, dient de Eigenaar (van de gegevens) hier expliciet toestemming voor te geven. Hieraan kan de voorwaarde worden verbonden dat eerst alle gevoelige details en inhoud dienen te worden verwijderd, of aangepast zodat deze onherkenbaar zijn, of dienen extra maatregelen te worden getroffen en gelden tenminste dezelfde beveiligingseisen als welke voor de productieomgeving van kracht zijn.
4. Persoonlijke of anderszins vertrouwelijke testgegevens dienen niet langer dan strikt noodzakelijk te worden bewaard.

12.4.3 Toegangsbeheersing voor broncode van programmatuur

De toegang tot broncode van programmatuur behoort te worden beperkt.

De toegang tot broncode wordt zoveel mogelijk beperkt om de code tegen onbedoelde wijzigingen te beschermen.

Alleen geautoriseerde personen hebben toegang tot broncode.

12.5 Beveiliging bij ontwikkelings- en ondersteuningsprocessen

Doelstelling:
Beveiliging van toepassingsprogrammatuur en -informatie handhaven.

12.5.1 Procedures voor wijzigingsbeheer

De implementatie van wijzigingen behoort te worden beheerst door middel van formele procedures voor wijzigingsbeheer.

Zie Paragraaf 10.1.2.

12.5.2 Technische beoordeling van toepassingen na wijzigingen in het besturingssysteem

Bij wijzigingen in besturingssystemen behoren bedrijfskritische toepassingen te worden beoordeeld en getest om te bewerkstelligen dat er geen nadelige gevolgen zijn voor de activiteiten of beveiliging van de organisatie.

Als het besturingssysteem moet worden gewijzigd van een systeem waarop een bedrijfskritische toepassing operationeel is, beoordeelt ICTS vooraf,- en test ICTS zo nodig in een testomgeving - of ze met de wijziging geen concessies doet aan de effectiviteit van bestaande beveiligingsmaatregelen. Het gaat hierbij met name om de werking van de logische toegangsbeveiliging, logging en monitoring naast de integriteit van gegevens en (correcte werking van) functionaliteit.

ICTS dient voldoende tijd en middelen (waaronder menskracht en expertise) te reserveren voor de beoordeling, eventuele tests en verslaglegging daarvan.

12.5.3 Restricties op wijzigingen in programmatuurpakketten

Wijzigingen in programmatuurpakketten behoren te worden ontmoedigd, te worden beperkt tot noodzakelijke wijzigingen, en alle wijzigingen behoren strikt te worden beheerst.

Kant-en-klaar geleverde software wordt zoveel mogelijk ongewijzigd gebruikt. Alleen wanneer er een zakelijke aanleiding of andere dwingende reden bestaat, vinden wijzigingen plaats, waarbij rekening gehouden wordt met:

1. Het risico dat ingebouwde beveiligingsmaatregelen niet meer naar behoren werken;
2. Het mogelijk niet langer zonder meer kunnen installeren van upgrades en/of updates;
3. Gevolgen voor de ondersteuning door de leverancier.

Als wijzigingen noodzakelijk zijn, worden deze afdoende getest en gedocumenteerd (om ze in toekomstige upgrades aan te kunnen brengen). Tevens archiveert ICTS de oorspronkelijke versie van de software en worden de wijzigingen uitsluitend aangebracht in een duidelijk gemarkeerde kopie.

12.5.4 Uitlekken van informatie

Er behoort te worden voorkomen dat zich gelegenheden voordoen om informatie te laten uitlekken.

Als er sprake is van aanschaf van nieuwe informatiesystemen of grote wijzigingen of uitbreidingen aan bestaande informatiesystemen, besteedt de instelling de nodige aandacht aan het voorkomen van het uitlekken van niet-openbare informatie.

Aspecten waar aandacht aan kan worden besteed, zijn:

1. Ongewenste informatie in informatiestromen, zoals in berichten en uitgewisselde documenten;
2. Onnodig prijsgeven van informatie door systemen (zoals type besturingssysteem, softwareversies, configuratie-informatie, et cetera);
3. Het loggen en monitoren van systeemactiviteiten en handelingen door gebruikers, waar dat onder de vigerende wet- en regelgeving is toegestaan.

12.5.5 Uitbestede ontwikkeling van programmatuur

Uitbestede ontwikkeling van programmatuur behoort onder supervisie te staan van en te worden gecontroleerd door de organisatie.

Uitbestede ontwikkeling van software komt tot stand onder supervisie en verantwoordelijkheid van de in het uitbestedingscontract genoemde gemandateerde functionaris. Deze ziet er op toe dat maatregelen worden overeengekomen om rechten, beschikbaarheid, kwaliteit en vertrouwelijkheid te waarborgen.

Als de instelling ontwikkeling van software uitbesteedt, moet rekening worden gehouden met de volgende punten:

1. Licentieovereenkomsten, eigendom van de broncode en intellectuele eigendomsrechten (zie Paragraaf 15.1.2);
2. Beoordeling van de kwaliteit en nauwkeurigheid van het uitgevoerde werk;
3. Zorgen voor een waarborg indien een leverancier in gebreke blijft;
4. Toegangsrechten voor het uitvoeren van een audit op de kwaliteit en nauwkeurigheid van het uitgevoerde werk;
5. Contractuele eisen voor de kwaliteit en beveiligingsfunctionaliteit van de broncode;
6. Security audit voorafgaand aan installatie.

12.6 Beheer van technische kwetsbaarheden

Doelstelling:
Risico's verminderen als gevolg van benutting van gepubliceerde technische kwetsbaarheden.

12.6.1 Beheersing van technische kwetsbaarheden

Er behoort tijdig informatie te worden verkregen over technische kwetsbaarheden van de gebruikte informatiesystemen. De mate waarin de organisatie blootstaat aan dergelijke kwetsbaarheden behoort te worden geëvalueerd en er behoren geschikte maatregelen te worden genomen voor behandeling van daarmee samenhangende risico's.

Ten aanzien van de beheersing van kwetsbaarheden gelden de volgende richtlijnen:

1. Voor alle systemen in de productieomgeving – hardware en software –wordt door de verantwoordelijke technisch en functioneel beheerders bijgehouden welke nieuwe kwetsbaarheden door producenten, leveranciers of andere bronnen bekend worden gemaakt en welke middelen c.q. methodes beschikbaar zijn om de ontdekte kwetsbaarheid te elimineren.
   NB. Een complete bijgewerkte registratie van de systemen in productieomgeving (met bijbehorende details) is hiervoor een absolute vereiste.
2. Relevante, te bewaken nieuwsbronnen dienen voor de verschillende systemen in productieomgeving te worden vastgesteld. Deze vaststelling moet worden onderhouden. Hierbij wordt rekening gehouden met wijzigingen in het gebruik van systemen en/of nieuwsbronnen.
3. Voor iedere nieuw bekend geworden kwetsbaarheid wordt de ernst vastgesteld aan de hand van de set van betrokken systemen in productieomgeving, een risico-afweging, classificaties van de kwetsbaarheid en de betrokken systemen en de vereiste opvolging. Beveiligingspatches en/of bedrijfskritische (informatie)systemen dienen een hogere urgentie te krijgen.
4. Als een beveiligingspatch (‘security-update’) beschikbaar is, moet worden ingeschat wat de risico's zijn van het installeren van de patch en moeten deze risico's worden vergeleken met de risico's van het niet installeren van de patch.
5. Opvolgacties worden zo snel als mogelijk uitgevoerd via de formele procedures voor wijzigingsbeheer. Voorafgaand aan installatie dienen beveiligingspatches altijd afdoende te worden getest en beoordeeld in de testomgeving, om zekerheid te verkrijgen wat betreft correcte werking en mogelijke verstoring(en).
6. Als een beveiligingspatch (nog) niet voorhanden is, wordt het beschikbaar komen van een patch actief bewaakt en moeten andere maatregelen worden overwogen, zoals:
   1. Het inactiveren van software (bijvoorbeeld services);
   2. Het treffen van maatregelen op andere systemen, zoals firewalls, proxies, IPS/IDS, routers, et cetera;
   3. Verhoogde alertheid op misbruik van de kwetsbaarheid;
   4. Verhoogd bewustzijn aangaande de aard van de kwetsbaarheid.
7. Ondernomen acties – met al dan niet geïnstalleerde beveiligingspatches – worden gedocumenteerd (gelogd).
8. Voor ieder systeem in productieomgeving is geregistreerd welke beveiligingspatches zijn geïnstalleerd.

13 Beheer van informatiebeveiligingsincidenten

13.1 Rapportage van informatiebeveiligingsgebeurtenissen en zwakke plekken

Doelstelling:
Bewerkstelligen dat informatiebeveiligingsgebeurtenissen en zwakheden die verband houden met informatiesystemen zodanig kenbaar worden gemaakt dat tijdig corrigerende maatregelen kunnen worden genomen.

13.1.1 Rapportage van informatiebeveiligingsgebeurtenissen

Informatiebeveiligingsgebeurtenissen behoren zo snel mogelijk via de juiste leidinggevende niveaus te worden gerapporteerd.

Een informatiebeveiligingsgebeurtenis, ofwel 'beveiligingsincident', is een geconstateerde dan wel vermoede aantasting van de vertrouwelijkheid, integriteit en/of de beschikbaarheid van informatie of informatievoorzieningen alsmede situaties die het ontstaan van een aantasting in de hand werken.

De volgende gebeurtenissen merkt de instelling als (beveiligings-)incident aan:

1. Ongewenst gebruik of misbruik, of pogingen daartoe, van:
    a. Bevoegdheden en/of rechten;
    b. Voorzieningen zoals e-mail, internet en accounts (wachtwoorden);
    c. Bedrijfsmiddelen als laptops, tablets, smartphones en gegevensdragers (documenten, USB-sticks, et cetera);
    d. Beveiligde ruimten of opbergmiddelen;
2. Ongeautoriseerd gebruik van en inbraak op informatiesystemen;
3. Lekken van, misbruik van en/of onzorgvuldig omgaan met niet-openbare informatie van de instelling;
4. Schending van de Wet Bescherming Persoonsgegevens (WBP) en/of andere wetgeving;
5. Het plaatsen of versturen van berichten of teksten van aanstootgevende of beledigende aard, of anderszins in strijd met wetten en/of zeden;
6. Verdachte pogingen tot het (ongeautoriseerd) verkrijgen van vertrouwelijke of geheime informatie, waaronder phishing;
7. Vermissing, verlies of diefstal van apparatuur (laptops, tablets, smartphones, et cetera) of gegevensdragers (documenten, USB-sticks, et cetera) mogelijk resulterend in het lekken van informatie;
8. Alle vormen van fraude inclusief identiteitsfraude;
9. (Ver)storingen, zoals uitval, malwarebesmetting.

Een vastgestelde procedure voor het melden van een beveiligingsincidenten is van kracht, met onder meer wat voor soort incidenten waar dienen te worden gemeld (loket), de vereiste handelingen na melding en een escalatieprocedure. De instelling maakt de meldingsprocedure aan alle gebruikers bekend.

Registratie en afhandeling van beveiligingsincidenten vindt door twee verschillende oplosgroepen plaats, al naar gelang de aard van het incident:

1. Service Management van ICTS coördineert de afhandeling van incidenten betreffende de beschikbaarheid van systemen. Na bepaling van het type incident zorgt Service Management voor de juiste "routing".
2. Na melding (al of niet door tussenkomst van de leidinggevende of de daartoe aangestelde functionaris) handelen CERT-HvA en CERT-UvA incidenten af betreffende vertrouwelijkheid en/of integriteit (zoals systeemcompromittatie).

Zowel Service Management als CERT-HvA/CERT-UvA voeren een zodanige centrale registratie dat zij in staat zijn om op verzoek over een willekeurige periode een incidentenrapportage op te leveren. Hiertoe registreren zij per beveiligingsincident tenminste:

1. Aanvangstijdstip en tijdstip afgehandeld
2. Aard van het incident
3. Oorzaak van het incident (bron)
4. Wijze van afhandeling
5. Betrokken personen

In aanvulling op het melden van beveiligingsincidenten door gebruikers, gebruikt de instelling logging en monitoring voor het detecteren van incidenten (zie Paragraaf 10.10).

Informatie over de beveiligingsrelevante handelingen, bijvoorbeeld loggegevens, foutieve inlogpogingen, van de gebruiker wordt regelmatig nagekeken. De ISO bekijkt maandelijks een samenvatting van de informatie.

13.1.2 Rapportage van zwakke plekken in de beveiliging

Van alle werknemers, ingehuurd personeel en externe gebruikers van informatiesystemen en -diensten behoort te worden geëist dat zij alle waargenomen of verdachte zwakke plekken in systemen of diensten registreren en rapporteren.

De instelling vraagt in haar ICT-gedragsregels alle gebruikers van informatiesystemen en -diensten waargenomen of verdachte zwakke plekken in de beveiliging van systemen of diensten zo snel mogelijk te melden bij de ICTS Servicedesk.

In aanvulling op het melden van zwakke plekken door gebruikers gebruikt de instelling logging en monitoring voor het ontdekken van zwakke plekken (zie Paragraaf 10.10).

13.2 Beheer van informatiebeveiligingsincidenten en -verbeteringen

Doelstelling:
Bewerkstelligen dat een consistente en doeltreffende benadering wordt toegepast voor het beheer van informatiebeveiligingsincidenten.

13.2.1 Verantwoordelijkheden en procedures

Er behoren leidinggevende verantwoordelijkheden en procedures te worden vastgesteld om een snelle, doeltreffende en ordelijke reactie op informatiebeveiligingsincidenten te bewerkstelligen.

Incidentrespons is de wijze van reageren op verschillende typen beveiligingsincidenten. Ze heeft als eerste doel het bewerkstelligen van een beheerste situatie en het ‘normale beveiligingsniveau’, om daarna het nodige herstel te initiëren.

De instelling hanteert de volgende richtlijnen voor incidentrespons:

1. De instelling stelt standaard procedures op voor het afhandelen van verschillende typen incidenten die een grotere kans van optreden hebben.
2. Incidentprocedures kunnen de volgende aspecten behandelen (zie ook Paragraaf 13.2.2):
   - Analyse en identificatie van de oorzaak van het incident;
   - Inperking van het incident;
   - Zo nodig planning en implementatie van preventieve maatregelen om herhaling te voorkomen;
   - Hoe te communiceren met degenen die worden getroffen door, of zijn betrokken bij, het herstel van het incident;
   - Rapporteren van de genomen maatregelen aan de Directeur ICTS en de ISO.
3. ‘Audit trails’ en soortgelijk bewijsmateriaal dienen voor zover mogelijk en nodig te worden verzameld (zie Paragrafen 13.2.2 en 13.2.3) en veilig te worden opgeslagen zodat ze geschikt zijn voor:
   - Interne probleemanalyse;
   - Gebruik als forensisch bewijsmateriaal in geval van mogelijke contractbreuk of bij het overtreden van wettelijke voorschriften, of in civiele of strafrechtelijke procedures, bijvoorbeeld bij computermisbruik of overtreding van wetgeving voor gegevensbescherming;
   - Onderhandeling over compensatie van leveranciers van diensten en software (als bewijs van wanprestatie).
4. Handelingen die nodig zijn om schendingen van de beveiliging en systeemstoringen te corrigeren en te herstellen, moeten zorgvuldig en formeel worden beheerst. De procedures moeten te waarborgen dat:
   - Alleen duidelijk vastgestelde en bevoegde personen toegang krijgen tot operationele systemen en gegevens (zie ook Paragraaf 6.2 inzake bevoegde toegang door externe partijen);
   - Alle uitgevoerde noodmaatregelen tot in detail zijn gedocumenteerd;
   - Noodmaatregelen aan het verantwoordelijke management worden gerapporteerd en op een ordentelijke wijze worden beoordeeld;
   - De correcte werking van operationele systemen en beheersmaatregelen zo snel mogelijk kan worden bevestigd.

13.2.2 Leren van informatiebeveiligingsincidenten

Er behoren mechanismen te zijn ingesteld waarmee de aard, omvang en kosten van informatiebeveiligingsincidenten kunnen worden gekwantificeerd en gecontroleerd.

De instelling registreert beveiligingsincidenten (zie Paragraaf 13.1.1), onder meer ten behoeve van analyse en evaluatie van de oorzaak, het verloop en de kosten van het incident. De analyse en evaluatie is met name gericht op het verbeteren van beheersmaatregelen en daarmee het verkleinen van risico's.

De informatiebeveiligingsfunctionarissen van de instelling (ISO en ISM's) evalueren tenminste eenmaal per jaar de beveiligingsincidenten. Deze evaluatie resulteert in schriftelijke aanbevelingen ter verbeteringen van beheersmaatregelen.

13.2.3 Verzamelen van bewijsmateriaal

Waar een vervolgprocedure tegen een persoon of organisatie na een informatiebeveiligingsincident juridische maatregelen omvat (civiel of strafrechtelijk), behoort bewijsmateriaal te worden verzameld, bewaard en gepresenteerd overeenkomstig de voorschriften voor bewijs die voor het relevante rechtsgebied zijn vastgelegd.

Algemene richtlijnen voor het verzamelen van bewijsmateriaal zijn:

1. Het verkrijgen van bewijsmateriaal geschiedt uitsluitend in opdracht van CSO en/of Directeur ICTS;
2. Het bewijsmateriaal dient op legale wijze te worden verkregen en veilig gesteld;
3. Het bewijsmateriaal dient voldoende kracht te hebben voor een vervolgprocedure;
4. Het verzamelen van bewijsmateriaal gebeurt waar mogelijk door twee onafhankelijke personen gelijktijdig, zodat deze personen elkaars getuige kunnen zijn;
5. Het bewijsmateriaal dient te worden gedocumenteerd (tenminste: datum, plaats, vinder, getuige).

In voorkomende gevallen besteedt de instelling het onderzoek ter zake uit aan een daartoe bevoegd en deskundig onderzoeksbureau.

14 Bedrijfscontinuïteitsbeheer

14.1 Informatiebeveiligingsaspecten van bedrijfs-continuïteitsbeheer

Doelstelling:
Onderbreken van bedrijfsactiviteiten tegengaan en kritische bedrijfsprocessen beschermen tegen de gevolgen van omvangrijke storingen in informatiesystemen of rampen en om tijdig herstel te bewerkstelligen.

14.1.1 Informatiebeveiliging opnemen in het proces van bedrijfscontinuïteitsbeheer

Er behoort een beheerd proces voor bedrijfscontinuïteit in de gehele organisatie te worden ontwikkeld en bijgehouden, voor de naleving van eisen voor informatiebeveiliging die nodig zijn voor de continuïteit van de bedrijfsvoering.

Het bestuur van de instelling is eigenaar van het proces Bedrijfscontinuïteit en verantwoordelijk voor de instandhouding van dit proces. Hieronder valt ook het stellen van continuïteitseisen aan ICT-voorzieningen. Doel van het proces is onder meer:

1. Het ontwikkelen van een strategie voor algehele bedrijfscontinuïteit en - als afgeleide hiervan - de continuïteit van de informatievoorziening in het bijzonder;
2. Het verkrijgen van een actueel inzicht in risico's die de bedrijfscontinuïteit kunnen beïnvloeden;
3. Inzicht verkrijgen en behouden in de gevolgen van ernstige verstoringen voor bedrijfsprocessen en -activiteiten;
4. Het in kaart hebben van bedrijfskritische middelen (waaronder ICT-voorzieningen) en middelen die essentieel zijn voor het (kunnen) herstellen c.q. overleven van calamiteiten[23]. Denk aan gegevens, documenten, sleutels, speciale hardware, maar ook aan specifieke kennis en ervaring;
5. Het vaststellen en financieren van vereiste preventieve en repressieve continuïteitsmaatregelen;
6. Toezicht op opzet, bestaan en werking van continuïteitsmaatregelen.

Het bestuur van de instelling kan de coördinatie van (delen van) het proces bedrijfscontinuïteit delegeren, maar blijft (eind)verantwoordelijk.

Tenminste een maal per kalenderjaar wordt het onderwerp bedrijfscontinuïteit geagendeerd in het bestuursoverleg. De CSO neemt hiertoe het initiatief. Tot de aspecten waar het bestuursoverleg zich in aanwezigheid van de CSO over buigt behoren:

1. Status van (de implementatie van) maatregelen, waaronder de opzet, bestaan en werking van calamiteitenplannen;
2. Resultaten van de jaarlijkse uitwijk-, noodstroom- en hersteltesten;
3. (Ernstige) Incidenten in de afgelopen periode;
4. Beoordeling van bestaande en nieuwe bedreigingen en risico's voor de bedrijfscontinuïteit en de continuïteit van de informatievoorziening.

Van dit overleg wordt in ieder geval de risicobeoordeling, besluiten en actiepunten schriftelijk vastgelegd.

Tussendoor wordt bedrijfscontinuïteit extra geagendeerd indien daartoe aanleiding is.

14.1.2 Bedrijfscontinuïteit en risicobeoordeling

Gebeurtenissen die tot onderbreking van bedrijfsprocessen kunnen leiden, behoren te worden geïdentificeerd, tezamen met de waarschijnlijkheid en de gevolgen van dergelijke onderbrekingen en hun gevolgen voor informatiebeveiliging.

Tenminste eenmaal per jaar buigen de ISO, Informatiemanagers en eventuele belanghebbenden tijdens een bijeenkomst zich over risico's die de continuïteit van de informatievoorziening, en daarmee van bedrijfsprocessen, ernstig in gevaar kunnen brengen. Bij deze risicobeoordeling wordt:

[23] Calamiteiten zijn die gebeurtenissen, die bedrijfsprocessen in ernstige mate kunnen ontwrichten en daarmee het bereiken van de bedrijfsdoelstellingen direct in gevaar brengen of zelfs het voortbestaan van de organisatie in gevaar kunnen brengen. Een calamiteit kan resulteren in een crisis(situatie).

1. Geïnventariseerd welke reeds onderkende en nieuwe risico's mogelijk kunnen leiden tot een gebeurtenis die een ernstige ontwrichting van bedrijfsprocessen betekent;
2. Voor bedrijfskritische informatiesystemen en andere bedrijfskritische middelen de maximaal toelaatbare uitvalduur en/of verstoring bepaald of heroverwogen (inclusief de maximaal toelaatbare hoeveelheid gegevensverlies);
3. Op basis van de uitkomsten van de voorgaande punten:
    a. De strategie voor bedrijfscontinuïteit bijgesteld;
    b. Een selectie gemaakt van de gebeurtenissen (c.q. gebeurtenisscenario's) die de instelling met preventieve maatregelen wenst te voorkomen en/of waar de instelling via het paraat hebben van repressieve (onderdrukkende) maatregelen op voorbereid wil zijn;
    c. Een set van preventieve en repressieve continuïteitsmaatregelen vastgesteld, waaronder het opstellen van specifieke calamiteitenplannen[24].

De risicobeoordeling richt zich met name op ICT-voorzieningen. Ze maakt onderdeel uit van een jaarlijkse risicobeoordeling in het kader van bedrijfscontinuïteit die de gehele bedrijfsvoering van de instelling als scope heeft.

De ISO bereidt de risicobeoordeling voor en legt de uitkomsten van de beoordeling schriftelijk vast, inclusief besluiten en actiepunten.

Voorts berust bij het bestuur, de ISO en de leidinggevenden van de instelling de taak en verantwoordelijkheid voortdurend alert te zijn op nieuwe bedreigingen van en risico's voor de bedrijfscontinuïteit, deze te signaleren en onder de aandacht van belanghebbenden te brengen.

14.1.3 Continuïteitsplannen ontwikkelen en implementeren waaronder informatiebeveiliging

Er behoren plannen te worden ontwikkeld en geïmplementeerd om de bedrijfsactiviteiten te handhaven of te herstellen en om de beschikbaarheid van informatie op het vereiste niveau en in de vereiste tijdspanne te bewerkstelligen na onderbreking of uitval van kritische bedrijfsprocessen.

De instelling stelt alleen calamiteitenplannen op voor een aantal specifieke, tijdens de risicobeoordeling als relevant onderkende gebeurtenissen of gebeurtenisscenario's (zie Paragraaf 14.1.2). Deze hebben met name als doel:

1. Het zoveel mogelijk beperken van schade;
2. Het mogelijk maken van voortzetting van bedrijfskritische processen op een minimaal vereist, gedefinieerd niveau.

Het is niet zinnig en ook niet mogelijk om op al het mogelijke voorbereid te zijn. De instelling kiest bewust waar ze ten minste, maar ook ten hoogste op voorbereid wil zijn. De volgende elementen kunnen in een calamiteitenplan aan bod komen:

1. **Activatie en escalatie**
   Onder welke omstandigheden en voorwaarden treedt het plan in werking en onder welke omstandigheden volgt escalatie, de-escalatie of de-activatie. Aanvaardbaar verlies van gegevens en/of uitval van diensten kunnen hierbij een rol spelen;
2. **Calamiteiten- c.q. crisisbeheer**
   De wijze waarop de calamiteit dient te worden beheerst met daarbij behorende doelstellingen, prestatie-eisen en prioriteiten. Het kan hier gaan om vooraf voorbereide procedures voor overleg en besluitvorming, (nood)procedures, tijdelijke operationele procedures, uitwijkprocedures, herstartprocedures, et cetera, die dienen te worden gevolgd. Hierbij dient een goede balans te worden gevonden tussen enerzijds uitwerking en detaillering en anderzijds improvisatie.
   Ter bestrijding van de calamiteit kunnen operationele draaiboeken worden gebruikt, zoals voor fysieke uitwijk of logische uitwijk naar een andere locatie of voor communicatie;
3. **Betrokkenen inclusief contactgegevens**
   Een overzicht van het calamiteitenteam en de organisatie daaromheen, met alle personen (intern en extern, direct en indirect) en instanties die betrokken moeten of kunnen worden bij het bestrijden en beheersen van de calamiteit, inclusief bereikbaarheidsgegevens, verantwoordelijkheden en mandaten (bevoegdheden) voor het uitvoeren van onderdelen van het calamiteitenplan en procedures en vervangers;
4. **Vindplaatsen**
   Vindplaatsen van middelen (anders dan personen en instanties) die nodig zijn voor calamiteitenbeheer. Denk

[24] De term 'calamiteitenplan' wordt gehanteerd in plaats van 'continuïteitsplan', 'bedrijfscontinuïteitsplan' of 'crisisplan'.

aan gedocumenteerde procedures, afspraken met leveranciers en samenwerkingspartijen, verzekeringspapieren, andere documentatie, reserve hardware, sleutels, back-ups, enzovoorts;

5. **Herstel**
   Operationele procedures gericht op het herstellen van de oorspronkelijke situatie nadat de calamiteit is beteugeld;
6. **Uitgangspunten en randvoorwaarden**
   De uitgangspunten en principes waarop het plan berust en de voorwaarden waaraan voldaan moet zijn wil het plan zijn werking kunnen hebben (bijvoorbeeld de aanwezigheid van specifieke kennis en ervaring zoals crisisbeheer en systeemkennis);
7. **Onderhoud, Testen en Training**
   De wijze waarop het plan actueel wordt gehouden, de wijze van testen van het operationele gedeelte van het plan (testplan) en hoe wordt gezorgd voor voldoende parate kennis in de organisatie van het plan (scholing).

Calamiteitenplannen kennen een eigenaar en dienen zoveel mogelijk door betrokkenen, bijvoorbeeld naar aanleiding van een grote wijziging, actueel te worden gehouden. De eigenaar ziet hier op toe.

Kopieën van de laatste versies van calamiteitenplannen dienen op een externe locatie op voldoende afstand beschikbaar te zijn.

14.1.4 Kader voor de bedrijfscontinuïteitsplanning

Er behoort een enkelvoudig kader voor bedrijfscontinuïteitsplannen te worden gehandhaafd om te bewerkstelligen dat alle plannen consistent zijn, om eisen voor informatiebeveiliging op consistente wijze te behandelen en om prioriteiten vast te stellen voor testen en onderhoud.

Kwaliteitscriteria voor calamiteitenplannen zijn:

1. Kort en bondig;
2. Inhoudelijk toereikend en up-to-date;
3. Helder, duidelijk, overzichtelijk en leesbaar.

NB. Calamiteitenplannen hoeven niet zo compleet mogelijk en verregaand gedetailleerd te zijn, maar moeten voldoende handvatten bieden om snel en adequaat te kunnen handelen.

14.1.5 Testen, onderhoud en herbeoordelen van bedrijfscontinuïteitsplannen

Bedrijfscontinuïteitsplannen behoren regelmatig te worden getest en geüpdatet, om te bewerkstelligen dat ze actueel en doeltreffend blijven.

Om calamiteitenplannen actueel en doeltreffend te houden hanteert de instelling de volgende richtlijnen:

1. Calamiteitenplannen kennen een eigenaar die (eind)verantwoordelijk is voor het actueel houden en zijn van het plan;
2. Calamiteitenplannen bevatten een paragraaf m.b.t. het onderhoud van het plan;
3. Bij ter zake doende veranderingen zoals wijziging van bedrijfsstrategie, wetgeving, leveranciers, bedrijfsprocessen, et cetera, zien eigenaren er op toe dat calamiteitenplannen worden bijgewerkt;
4. Calamiteitenplannen bevatten een testplan en worden op basis van testresultaten en evaluatie geactualiseerd en bijgesteld.
5. Elk onderdeel van een plan wordt tenminste eenmaal per jaar getest.
6. Calamiteitenplannen worden tenminste eenmaal per jaar beoordeeld. Hierbij dient tenminste te worden gelet op het actueel zijn van:
   a. Namen van direct, indirect, intern en extern betrokkenen en eventueel betrokken partijen als leveranciers, klanten, samenwerkingspartners, et cetera;
   b. Adressen en telefoonnummers;
   c. Aansluiting op bedrijfsstrategie, bedrijfsprocessen en wetgeving;
   d. Locaties, voorzieningen en vindplaatsen.
7. De procedures voor wijzigingsbeheer (zie ook Paragraaf 10.1.2) voorzien in het actualiseren van calamiteitenplannen naar aanleiding van uitgevoerde wijzigingen, alsmede het bijwerken van overige (hulp)middelen die noodzakelijk zijn voor de uitvoering van het plan.

15 Naleving

15.1 Naleving van wettelijke voorschriften

Doelstelling:
Voorkomen van schending van enige wetgeving, wettelijke en regelgevende of contractuele verplichtingen, en van enige beveiligingseisen.

15.1.1 Identificatie van toepasselijke wetgeving

Alle relevante wettelijke en regelgevende eisen en contractuele verplichtingen en de benadering van de organisatie in de naleving van deze eisen, behoren expliciet te worden vastgesteld, gedocumenteerd en actueel te worden gehouden voor elk informatiesysteem en voor de organisatie.

ICTS houdt centraal voor de informatiesystemen waarvoor dit relevant is een registratie bij met daarin per informatiesysteem:

1. Een korte omschrijving van het doel van het informatiesysteem (waartoe dient het);
2. Wie de Eigenaar is van het betreffende informatiesysteem;
3. De van toepassing zijnde wettelijke vereisten waaraan het systeem en de instelling moet voldoen;
4. De van toepassing zijnde contractuele vereisten waaraan het systeem en de instelling moet voldoen.

Het is de verantwoordelijkheid van de Eigenaar te bepalen welke wettelijke en contractuele vereisten van toepassing zijn.

15.1.2 Intellectuele eigendomsrechten (Intellectual Property Rights, IPR)

Er behoren geschikte procedures te worden geïmplementeerd om te bewerkstelligen dat wordt voldaan aan de wettelijke en regelgevende eisen en contractuele verplichtingen voor het gebruik van materiaal waarop intellectuele eigendomsrechten kunnen berusten en het gebruik van programmatuur waarop intellectuele eigendomsrechten berusten.

Ten aanzien van het voldoen aan de wettelijke en regelgevende eisen en contractuele verplichtingen die betrekking hebben op intellectuele eigendomsrechten zijn de volgende richtlijnen van kracht:

1. De ICT-gedragsregels bevatten een richtlijn omtrent het gebruik, de aankoop en de installatie van software met daarin de waarschuwing dat disciplinaire maatregelen (kunnen) worden genomen als men hiermee in strijd handelt;
2. ICTS inventariseert waar nodig periodiek via een scan welke software in gebruik is en spiegelt de uitkomsten tegen het actuele aantal licenties. Zo nodig wordt het aantal licenties uitgebreid of afgebouwd.
3. ICTS behoudt zich het recht voor het netwerk en de werkstations regelmatig en steekproefsgewijs te scannen op software die niet rechtmatig is geïnstalleerd.

15.1.3 Bescherming van bedrijfsdocumenten

Belangrijke registraties behoren te worden beschermd tegen verlies, vernietiging en vervalsing, overeenkomstig wettelijke en regelgevende eisen, contractuele verplichtingen en bedrijfsmatige eisen.

Belangrijke registraties zijn registraties die ten gevolge van wet- en regelgeving, contractuele vereisten en/of om redenen van de bedrijfsvoering onderhevig zijn aan specifieke betrouwbaarheidseisen, zoals waarborgen aangaande beschikbaarheid (nu en in de toekomst), volledigheid, correctheid, authenticiteit/herkomst en/of vertrouwelijkheid. Voorbeelden: personeelsadministratie, studentenadministratie en contractenregistratie.

Ten aanzien van belangrijke registraties zijn de volgende richtlijnen van kracht:

1. De instelling onderhoudt een lijst van de belangrijkste registraties, met vermelding van:
    a. De (eind)verantwoordelijke Eigenaar;
    b. Wijze van opslag (mediumkeuze);
    c. Bewaartermijn.
2. Registraties worden gecategoriseerd naar type (zoals administratieve registratie, boekhoudkundige registraties, databaserecords, transactielogbestanden, auditlogbestanden en operationele procedures);

3. De Eigenaar bepaalt de richtlijnen voor het bewaren, opslaan, behandelen en verwijderen van records en informatie;
4. ICTS implementeert in samenspraak met de Eigenaar geschikte beheersmaatregelen om belangrijke registraties te beschermen tegen verlies, vernietiging en vervalsing;
5. ICTS selecteert systemen voor gegevensopslag zodanig dat vereiste gegevens kunnen worden opgevraagd binnen een aanvaardbare tijdspanne en in een aanvaardbaar formaat, afhankelijk van de eisen waaraan moet worden voldaan;
6. Procedures voor opslag en behandeling van opslagmedia dienen in lijn te zijn met de aanbevelingen van de fabrikant. De instelling houdt rekening met de mogelijkheid dat de kwaliteit van gebruikte opslagmedia afneemt;
7. Opslagsystemen waarborgen een duidelijke identificatie van registraties en hun bewaartermijn, waar van toepassing in overeenstemming met wet- of regelgeving. De registraties moeten na afloop van die termijn, als de instelling ze niet meer nodig heeft, op geschikte wijze worden vernietigd;
8. Waar elektronische opslagmedia worden gebruikt, stelt ICTS procedures vast om te waarborgen dat de informatie gedurende de gehele bewaarperiode toegankelijk blijft (leesbaarheid van zowel de media als van het gegevensformaat), om te voorkomen dat de informatie verloren gaat als gevolg van toekomstige technologische veranderingen;
9. Enige cryptografische sleutels of software die verband houden met versleutelde archieven, of digitale handtekeningen moeten zorgvuldig worden bewaard om ontcijfering mogelijk te maken tijdens de bewaarperiode.

15.1.4 Bescherming van gegevens en geheimhouding van persoonsgegevens

De bescherming van gegevens en privacy behoort te worden bewerkstelligd overeenkomstig relevante wetgeving, voorschriften en indien van toepassing contractuele bepalingen.

De instelling bewerkstelligt de bescherming van gegevens en privacy overeenkomstig de Wet Bescherming Persoonsgegevens (WBP), voorschriften en de contractuele bepalingen die van toepassing zijn. Zo geldt dat persoonsgegevens slechts mogen worden gebruikt op een wijze die in overeenstemming is met de WBP en dat voor het afhandelen van verzoeken om inzage en correctie van gegevens door betrokkenen aparte richtlijnen beschikbaar dienen te zijn. Naleving van de WBP betekent onder meer dat:

1. De instelling persoonsgegevens niet langer bewaart, in een vorm die het mogelijk maakt de betrokkene te identificeren, dan noodzakelijk is voor de verwerkelijking van de doeleinden waarvoor de gegevens zijn verzameld en worden verwerkt;
2. De instelling persoonsgegevens niet langer bewaart dan in punt 1 bepaald, voor zover ze voor historische, statistische of wetenschappelijke doeleinden worden bewaard, en de Eigenaar[25] de nodige voorzieningen heeft getroffen ten einde te verzekeren dat de desbetreffende gegevens uitsluitend voor deze specifieke doeleinden worden gebruikt;
3. De instelling persoonsgegevens slechts verwerkt voor zover zij (gelet op de doeleinden waarvoor zij zijn verzameld en worden verwerkt) toereikend, ter zake dienend en niet bovenmatig zijn;
4. De Eigenaar de nodige maatregelen treft opdat persoonsgegevens (gelet op de doeleinden waarvoor zij zijn verzameld en worden verwerkt) juist en nauwkeurig zijn;
5. Een ieder die handelt onder het gezag van de Eigenaar of van de bewerker, alsmede de bewerker zelf, voor zover deze toegang hebben tot persoonsgegevens, deze slechts verwerkt in opdracht van de verantwoordelijke, behoudens afwijkende wettelijke verplichtingen;
6. De personen, als in punt 5 bedoeld, voor wie niet reeds uit hoofde van ambt, beroep of wettelijk voorschrift een geheimhoudingsplicht geldt, verplicht zijn tot geheimhouding van de persoonsgegevens waarvan zij kennis nemen, behoudens voor zover enig wettelijk voorschrift hen tot mededeling verplicht of uit hun taak de noodzaak tot mededeling voortvloeit. Artikel 272, tweede lid, van het Wetboek van Strafrecht is niet van toepassing;
7. De Eigenaar passende technische en organisatorische maatregelen ten uitvoer legt om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.

Als de verantwoordelijke persoonsgegevens laat verwerken door een bewerker, dan betekent dit onder meer dat:

[25] De Eigenaar is in eerste instantie verantwoordelijk. Het bestuur van de instelling delegeert de zorg naar de Eigenaar maar behoudt de eindverantwoordelijkheid.

8. De Eigenaar zorg draagt dat de bewerker voldoende waarborgen biedt ten aanzien van de technische en organisatorische beveiligingsmaatregelen met betrekking tot de te verrichten verwerkingen. De Eigenaar ziet toe op de naleving van die maatregelen.
9. De uitvoering van verwerkingen door een bewerker geregeld wordt in een overeenkomst of krachtens een andere rechtshandeling waardoor een verbintenis ontstaat tussen de bewerker en de instelling.
10. De Eigenaar zorg draagt dat de bewerker:
    a. De persoonsgegevens verwerkt in overeenstemming met punt 5 en
    b. De verplichtingen nakomt die op de instelling rusten ingevolge punt 7.
11. Met het oog op het bewaren van het bewijs, dienen de onderdelen van de overeenkomst of de rechtshandeling die betrekking hebben op de bescherming van persoonsgegevens, alsmede de beveiligingsmaatregelen als bedoeld in punt 7, schriftelijk te worden vastgelegd.

Eigenaren van registraties die onder de WBP vallen zijn zelf (eind)verantwoordelijk voor het naleven van de hierboven gegeven richtlijnen.

De instelling stelt een (centrale) functionaris voor de gegevensbescherming (FG) aan. Deze is onder meer verantwoordelijk voor 1) het onderhouden van een centraal overzicht van registraties (gegevensverzamelingen) die onder de WBP vallen en 2) het voldoen aan de meldplicht.

15.1.5 Voorkomen van misbruik van IT-voorzieningen

Gebruikers behoren ervan te worden weerhouden IT-voorzieningen te gebruiken voor onbevoegde doeleinden.

1. De ICT-gedragsregels bevatten gedragsregels met betrekking tot het gebruiken van informatiesystemen en ICT-voorzieningen en tevens een omschrijving welk gebruik niet geoorloofd is en welke sancties bij overtreding van toepassing (kunnen) zijn;
2. Rechten van gebruikers worden voor zover mogelijk zoveel mogelijk ingeperkt (“least privilege”), zie Paragraaf 11.1.1;
3. Het gebruik van informatiesystemen en ICT-voorzieningen wordt op aanwijzing van de Eigenaar gelogd en gemonitord.
4. De instelling onderhoudt voor logging en monitoring een protocol welke vastlegt:
    a. Onder welke voorwaarden registratie is toegestaan;
    b. Onder welke voorwaarden de registratie kan worden ingezien;
    c. Door wie de registratie kan worden ingezien, inclusief eventuele daartoe bevoegde (externe) autoriteiten;
    d. Op welke wijze de registratie kan worden ingezien.

Geconstateerd ongeoorloofd gebruik van informatiesystemen en/of ICT-voorzieningen wordt conform de geldende sanctieregeling (zie Paragraaf 8.2.3) afgehandeld.

15.1.6 Voorschriften voor het gebruik van cryptografische beheersmaatregelen

Cryptografische beheersmaatregelen behoren overeenkomstig alle relevante overeenkomsten, wetten en voorschriften te worden gebruikt.

Voor het gebruik van cryptografische hard- of software zijn geen specifieke wettelijke restricties of voorschriften van kracht.

15.2 Naleving van beveiligingsbeleid en -normen en technische naleving

Doelstelling:
Bewerkstelligen dat systemen voldoen aan het beveiligingsbeleid en de beveiligingsnormen van de organisatie.

15.2.1 Naleving van beveiligingsbeleid en -normen

Managers behoren te bewerkstelligen dat alle beveiligingsprocedures die binnen hun verantwoordelijkheid vallen correct worden uitgevoerd om naleving te bereiken van beveiligingsbeleid en -normen.

Het lijnmanagement is verantwoordelijk voor de naleving van het Informatiebeveiligingsbeleid en de Baseline Informatiebeveiliging.

De ISO zorgt voor het toezicht op de uitvoering van het Informatiebeveiligingsbeleid en de Baseline Informatiebeveiliging. Daarbij behoren ook periodieke beveiligingsaudits. Deze kunnen worden uitgevoerd door of vanwege de ISO dan wel door interne of externe auditteams.

De ISO rapporteert in de P&C cyclus over informatiebeveiliging. Standaardonderdelen zijn hierbij:

1. Status uitvoering actiepunten jaarplan IB
2. Status preventieve en corrigerende maatregelen, waaronder bewustwordingsactiviteiten
3. Resultaten logging en monitoring, waaronder van de logische en fysieke toegang

15.2.2 Controle op technische naleving

Informatiesystemen behoren regelmatig te worden gecontroleerd op naleving van implementatie van beveiligingsnormen.

1. De instelling maakt gebruik van publieke best practices op het gebied van ICT-security voor de inrichting en configuratie van systemen;
2. De instelling voert jaarlijks een penetratietest of kwetsbaarheidsscan uit op delen van de ICT-infrastructuur;
3. Contracteigenaren zijn verantwoordelijk voor het jaarlijks (laten) controleren van de naleving van gemaakte beveiligingsafspraken;
4. De ISO laat steekproeven uitvoeren als daar aanleiding toe is.

15.3 Overwegingen bij audits van informatiesystemen

Doelstelling:
Doeltreffendheid van audits van het informatiesysteem maximaliseren en verstoring als gevolg van systeemaudits minimaliseren.

15.3.1 Beheersmaatregelen voor audits van informatiesystemen

Eisen voor audits en andere activiteiten waarbij controles worden uitgevoerd op productiesystemen, behoren zorgvuldig te worden gepland en goedgekeurd om het risico van verstoring van bedrijfsprocessen tot een minimum te beperken.

De initiator van de audit neemt de volgende richtlijnen in acht:

1. De auditeisen moeten met de juiste managers worden overeengekomen;
2. De reikwijdte van de controle (scope) moet vooraf worden gedefinieerd en daarna worden nageleefd;
3. De controles moeten worden beperkt tot alleen-lezen-toegang (‘read-only’) tot software en gegevens;
4. Andere toegang dan ‘alleen lezen’ moet uitsluitend worden toegelaten voor geïsoleerde kopieën van systeembestanden, die na beëindiging van de audit weer moeten worden gewist of op een juiste wijze behoren worden beschermd indien de audit-documentatie dit vereist;
5. Hulpmiddelen voor de uitvoering van de controles moeten expliciet worden vastgesteld en beschikbaar worden gesteld. Daarbij:
    a. Als auditors toegang nodig hebben tot een systeem, dient daartoe een speciaal account te worden aangemaakt met niet meer rechten dan noodzakelijk (“least privilege”). Na gebruik door de auditor wordt dit account direct geblokkeerd en na correcte afronding van de audit verwijderd;
    b. Als het noodzakelijk is dat met een bestaand account wordt ge-audit, wordt het wachtwoord na gebruik door de auditor direct gewijzigd, of tijdelijk een ander sterk wachtwoord ingesteld.
6. Eisen voor bijzondere of aanvullende verwerking moeten worden vastgesteld en overeengekomen;
7. Alle toegang moet worden gecontroleerd en vastgelegd in een logbestand om een ‘reference trail’ te produceren; voor geheime informatie of bedrijfskritische informatiesystemen moet een ‘reference trail’ met tijdregistratie worden overwogen;
8. Alle procedures, methodieken, eisen en verantwoordelijkheden worden gedocumenteerd in een auditplan;
9. De persoon/personen of de externe partij die de audit uitvoert/uitvoeren, mag/mogen geen belangen hebben bij de activiteiten die worden ge-audit.

15.3.2 Bescherming van hulpmiddelen voor audits van informatiesystemen

Toegang tot hulpmiddelen voor audits van informatiesystemen behoort te worden beschermd om mogelijk misbruik of compromittering te voorkomen.

Audittools - voor zover in het bezit van de instelling - dienen alleen toegankelijk te zijn voor bevoegde auditors.

Alle middelen die een externe auditpartij gebruikt voor audits ten behoeve van de instelling , dienen bekend te zijn en door de Information Security Manager (ISM) te zijn goedgekeurd.

Bijlage 1 Eigenaarschap

Het concept 'Eigenaarschap' is belangrijk als het duidelijk moet zijn **wie** binnen de organisatie ergens toe bevoegd is (zoals het nemen van beslissingen, regie) maar ook wie verantwoordelijkheid draagt en op (wan)prestaties kan worden aangesproken.

Bij informatiebeveiliging onderscheiden we voor eigenaarschap drie type bedrijfsmiddelen: informatiesystemen, gegevensverzamelingen en losse, ongestructureerde informatie. Denk bij informatiesystemen aan DLWO, Corsa, UvAmail en Blackboard, bij gegevensverzamelingen aan studenten- of personeelsadministraties en bij losse informatie aan een los bestand of document.

Deze bijlage verwoordt het eigenaarschap van gegevensverzamelingen en van informatiesystemen. Beiden zijn grotendeels gelijk, maar verschillen op een aantal punten. Doorgaans valt het eigenaarschap van een specifiek informatiesysteem en gegevensverzameling samen en is er sprake van één eigenaar.

Eigenaarschap Gegevensverzameling
Belangrijke gegevens hebben een eigenaar die onder meer verantwoordelijk is voor hun integriteit, vertrouwelijkheid, kwaliteit en beschikbaarheid[26]. De eigenaar besluit onder meer over wijzigingen, bepaalt bewaartermijnen (met wet- en regelgeving als uitgangspunt) en risicoclassificering en is verantwoordelijk voor financiering en het inrichten van processen om de kwaliteit van de gegevens te beheersen. De Eigenaar kan zich laten ondersteunen door andere functionarissen, zoals functioneel beheerders, sleutel-gebruikers, ISO en/of ISM, maar blijft te allen tijde verantwoordelijk.

De bevoegdheden houden onder meer het volgende in:

1. Bevoegd om voor de aan hem toegewezen gegevensverzameling(en) de koers te bepalen en beslissingen te nemen inzake gebruik en beveiliging. Hij:
    a. Stelt de benodigde functiescheiding vast (via toegangsrechten);
    b. Beslist over het toegestane gebruik, bijvoorbeeld waar geheime informatie mag worden opgeslagen en het gebruik van niet-persoonsgebonden accounts;
    c. Bepaalt via een expliciete classificatie en/of risicoafweging in samenspraak met de ISO het vereiste betrouwbaarheidsniveau;
    d. Autoriseert gebruikers en legt deze autorisatie vast in een autorisatiematrix;
    e. Autoriseert bijzondere rechten en afwijkingen ten opzichte van de Baseline IB, waaronder toegang door (gebruikers van) een externe/derde partij, niet-persoonsgebonden accounts;
    f. Heeft een laatste stem in beveiligingsmaatregelen, met inbegrip van de bewaartermijn van logging, aanvullende logging van activiteiten van technisch beheerders (voor kritieke informatiesystemen), time out tijd van sessies, maximale verbindingstijd, wel/niet toepassen van automatische identificatie van apparatuur, et cetera.
    g. Autoriseert wijzigingen, waaronder het wijzigen van de toegang tot logging;
    h. Autoriseert het testen met gegevens die als *vertrouwelijk* of *hoger* geclassificeerd zijn.
2. Kan als enige persoon binnen de organisatie, vanuit zijn rol als Eigenaar, (rest)risico's accepteren als gevolg van functionele beperkingen en/of het niet (of niet volledig) implementeren van beveiligingsmaatregelen. Een dergelijke acceptatie dient gepaard te gaan met een acceptatieverslag.

De verantwoordelijkheden houden onder meer het volgende in:

1. Waarborgen van de beschikbaarheid en de kwaliteit, juistheid en vertrouwelijkheid van de gegevensverzameling, onder meer door toezicht te houden op:
    a. Implementatie en correcte werking van vereiste beveiligingsmaatregelen, waaronder toegangsbeperking;
    b. Naleving van afspraken binnen de instelling en met leveranciers;
    c. Het voorlichten van gebruikers over procedures en afspraken voor het juist en veilig gebruik en het naleven hiervan door gebruikers.
2. Het beschikbaar stellen van middelen om de beveiliging te laten voldoen aan de Baseline IB;
3. Inventariseren van beveiligingseisen voortkomend uit wet- en regelgeving (zoals Wet Bescherming Persoonsgegevens) en/of contracten met derden en toezien op implementatie van bijbehorende beveiligingsmaatregelen;
4. Bij externe verwerking:
    a. Volgen van formele inkoopprocedures;
    b. Bij verwerking van persoonsgegevens: Bewerkersovereenkomst;
    c. Afdoende aandacht voor risicobeheersing, onder meer door test en evaluatie vooraf;

[26] Conform Architectuurprincipes UvA/HvA Versie 1.0, 10 november 2014.

    d. Overwegen van het gebruik van gecertificeerde diensten;
    e. Formele dienstacceptatie door de instelling voorafgaand aan gebruik;
5. Bij fraude- of diefstalgevoelige informatie: het bepalen van te loggen en/of monitoren gebeurtenissen;
6. Het periodiek evalueren van het vereiste betrouwbaarheidsniveau, waaronder het vaststellen van de gebruikersidentiteit, en (de effectiviteit van) getroffen beveiligingsmaatregelen en het bijstellen hiervan;
7. Registratie zoals van bijzondere rechten;
8. Het afleggen van verantwoording over zijn eigenaarschap in de hiërarchische lijn, als onderdeel van de reguliere periodieke rapportages.

Eigenaarschap Informatiesysteem
Voor ieder informatiesysteem waarmee een bepaalde dienstverlening wordt ondersteund, is de rol van Eigenaar belegd bij de leidinggevende van de afdeling, divisie of dienst die de dienstverlening levert. De Eigenaar is verantwoordelijk voor onder meer de beschikbaarheid en kwaliteit van de informatiediensten die door het informatiesysteem geleverd worden. Hij is ook verantwoordelijk voor de begroting en exploitatie betreffende beheer, licenties en overige kosten voor het waarborgen van de continuïteit van het informatiesysteem. De Eigenaar kan zich laten ondersteunen door andere functionarissen, zoals functioneel beheerders, sleutel-gebruikers, ISO en/of ISM, maar blijft te allen tijde verantwoordelijk.

De bevoegdheden houden onder meer het volgende in:

1. Bevoegd om voor de aan hem toegewezen objecten de koers te bepalen en beslissingen te nemen inzake gebruik, ontwikkeling, productie, onderhoud en beveiliging. Hij:
    a. Stelt de benodigde functionaliteit en de daarbij horende functiescheiding vast;
    b. Beslist over het toegestane gebruik, bijvoorbeeld waar geheime informatie mag worden opgeslagen en het gebruik van niet-persoonsgebonden accounts;
    c. Bepaalt via een expliciete classificatie en/of risicoafweging in samenspraak met de ISO het vereiste betrouwbaarheidsniveau;
    d. Autoriseert gebruikers en functioneel beheerders, en legt deze autorisatie vast in een autorisatiematrix;
    e. Autoriseert bijzondere rechten en afwijkingen ten opzichte van de Baseline IB, waaronder toegang door (gebruikers van) een externe/derde partij, niet-persoonsgebonden accounts;
    f. Autoriseert acceptatiecriteria voor nieuw te ontwikkelen informatiesystemen en wijzigingen;
    g. Heeft een laatste stem in beveiligingsmaatregelen, met inbegrip van de bewaartermijn van logging, aanvullende logging van activiteiten van technisch beheerders (voor kritieke informatiesystemen), time out tijd van sessies, maximale verbindingstijd, wel/niet toepassen van automatische identificatie van apparatuur, et cetera.
    h. Autoriseert wijzigingen, waaronder het wijzigen van de toegang tot logging;
    i. Autoriseert het testen met gegevens die als *vertrouwelijk of geheim* geclassificeerd zijn.
2. Kan als enige persoon binnen de organisatie, vanuit zijn rol als Eigenaar, (rest)risico's accepteren die ten tijde van oplevering bekend zijn, als gevolg van functionele beperkingen en/of het niet (of niet volledig) implementeren van beveiligingsmaatregelen. Een dergelijke acceptatie dient gepaard te gaan met een acceptatieverslag.

De verantwoordelijkheden houden onder meer het volgende in:

1. Waarborgen van de beschikbaarheid van het systeem en de kwaliteit, juistheid en vertrouwelijkheid van de in het systeem verwerkte data, onder meer door toezicht te houden op:
    a. Implementatie en correcte werking van vereiste beveiligingsmaatregelen, waaronder toegangsbeperking;
    b. Naleving van afspraken binnen de instelling en met leveranciers;
    c. Het voorlichten van gebruikers over procedures en afspraken voor het juist en veilig gebruik en het naleven hiervan door gebruikers.
2. Het beschikbaar stellen van middelen om de beveiliging te laten voldoen aan de Baseline IB;
3. Gebruik van acceptatiecriteria bij systeemacceptatie en wijzigingsbeheer;
4. Inventariseren van beveiligingseisen voortkomend uit wet- en regelgeving (zoals Wet Bescherming Persoonsgegevens) en/of contracten met derden en toezien op implementatie van bijbehorende beveiligingsmaatregelen;
5. Bij uitbesteding:
    a. Volgen van formele inkoopprocedures;
    b. Afdoende aandacht voor risicobeheersing, onder meer door test en evaluatie vooraf;
    c. Overwegen van het gebruik van gecertificeerde producten en diensten;
    d. Formele systeemacceptatie door de instelling voorafgaand aan het in productie nemen. Geldt ook voor (eventueel extern gehoste) websites en webapplicaties;
6. Bij een fraudegevoelig systeem: het bepalen van te loggen en/of monitoren gebeurtenissen;
7. Het periodiek evalueren van het vereiste betrouwbaarheidsniveau, waaronder voor het vaststellen van de gebruikersidentiteit, en (de effectiviteit van) getroffen beveiligingsmaatregelen en het bijstellen hiervan;

8. Registratie van bijzondere rechten;
9. Registratie van in bruikleen gegeven middelen en toezicht op naleving van afspraken m.b.t. het gebruik van deze middelen (inclusief tijdige retournering);
10. Het afleggen van verantwoording over zijn eigenaarschap in de hiërarchische lijn, als onderdeel van de reguliere periodieke rapportages.

Bijlage 2 Level of Assurance (LoA)

Level of Assurance
De mate van zekerheid met wie je precies als gebruiker te maken hebt en dat het ook echt deze gebruiker is die inlogt, noemen we het Level of Assurance ofwel 'LoA'. Het niveau is afhankelijk van enerzijds de kwaliteit van de processen waarmee de identiteit geverifieerd en uitgeleverd wordt en anderzijds de wijze waarop authenticatie plaatsvindt. De instelling onderscheidt vijf LoA-niveaus, maar gebruikt alleen de eerste vier:

Level	Vertrouwen in de geclaimde of verzekerde identiteit	Minimum eis verificatie identiteit	Minimum eis authenticatie	Voorbeeld accounts/ toepassingen
LoA0 - Zeer laag	Weinig tot geen	"Self asserted", toetsing identiteit via geldig e-mailadres eventueel aangevuld met andere controles of op voordracht van een medewerker van de instelling	Gebruikers-ID en (al dan niet sterk) wachtwoord	HvAguests/ UvAguests: gastaccount voor UvA-HvA wireless
LoA1 - Laag	Enig	Toetsing via kopie/scan geldig identiteitsbewijs (paspoort, identiteitskaart, rijbewijs)	Gebruikers-ID en sterk (getoetst) wachtwoord	Persoonsgebon-den instellings-account(UvAnetID, HvAID)
LoA2 - Midden	Veel	Face-to-face, met origineel identiteitsbewijs	Gebruikers-ID plus meer dan één factor, zoals wachtwoord plus SMS	Beheer webapplicaties, webredactie, VPN, SAP zelfbediening
LoA3 - Hoog	Veel	Face-to-face, met origineel identiteitsbewijs en eventueel aanvullende controles	Gebruikers-ID plus meer dan één factor, zoals wachtwoord plus Yubikey, SecurID	Systeem- en netwerkbeheer, invoeren van cijfers
LoA4 - Zeer hoog	Zeer veel	Vergaande toetsing, tenminste face-to-face, aan de hand van origineel identiteitsbewijs, door meer dan een medewerker, check tegen officieel gezaghebbend register zoals GBA	Sterk, bv. via een bij registratie uitgegeven smartcard met certificaat, zo nodig context-specifiek (locatie, functie)	Niet in gebruik bij UvA-HvA

Verdere uitleg
Informatiesystemen kunnen vrijelijk toegankelijk zijn, zoals de publieke website van de instelling, maar vaak zijn toegangsrechten nodig voor het mogen inzien of muteren van informatie of het benutten van functionaliteit zoals het online of offline zetten van pagina's op een website. Om de dingen te doen die je wilt kunnen doen, moet je je in dat geval eerst als gebruiker registreren of moet je als gebruiker geregistreerd zijn en moet je toegangsrechten hebben gekregen van de eigenaar van het systeem. Hiervoor moet je een unieke digitale identiteit hebben gekregen, die aan jou verbonden is als persoon, waarmee je je bekend kunt maken op het moment dat je het systeem wilt gaan gebruiken. De eigenaar moet je vooraf als legitieme gebruiker hebben erkend en je gebruiksrechten hebben toegekend. Anders gezegd, hij moet je hebben geautoriseerd tot het gebruik van het systeem zoals dat van toepassing is voor jou, voor de rol of functie die je bekleedt. Bijvoorbeeld, bij toegang tot het Studenten Informatiesysteem (SIS) ligt dit anders voor studenten en docenten, hoewel je in principe beiden 'gebruiker' bent.

Het kan zijn dat het voor de eigenaar van het systeem minder relevant is wie precies van zijn systeem gebruik maakt. En daarom geen zekerheid wenst met betrekking tot bijvoorbeeld je werkelijke naam, je werkelijke leeftijd of je werkelijke geslacht. Het kan echter ook zo zijn dat de eigenaar er in zeer hoge mate zeker van wil zijn met wie hij te maken heeft, bijvoorbeeld om vast te stellen of je wel gerechtigd bent om het systeem te gebruiken of om in het geval van misbruik schade op je te verhalen. Kortom, de eigenaar wil in een bepaalde mate zekerheid hebben met betrekking tot wie/wat je werkelijk/feitelijk bent, voordat je een uniek persoonsgebonden account met bijbehorende gebruikersnaam krijgt. En verdere toegang.

Daarnaast kan de eigenaar ook zekerheid wensen dat alleen jij en slechts alleen jij met jouw unieke identiteit informatie hebt kunnen inzien of kunnen wijzigen. Denk hierbij bijvoorbeeld aan het inzien van medische gegevens van medewerkers of het invoeren van examenresultaten van studenten. In dat geval wil hij er 100% zeker van zijn dat Karel Pieterse ook echt de enige echte Karel Pieterse is, en niet iemand die zich voordoet als 'Karel Pieterse'. Hierbij moet dus de wijze van authentiseren een bepaalde mate van zekerheid bieden dat je te maken hebt met de enige echte legitieme gebruiker.

Bijlage 3 Beveiligingseisen Verwerking Informatie

	voorbeelden van soorten informatie ---->	*publieke deel van websites*	*memo's, notities, mails, instructies*	*studentinformatie, personeelsdossiers*	*notulen bestuursoverleg, strategische instellingsplannen, bijzondere persoonsgegevens*
	classificatie ---->	**openbaar**	**intern (laag)**	**vertrouwelijk (midden)**	**geheim (hoog)**
digitaal / elektronisch					
bewerken	instellings-eigen desktop, -laptop (beheerd)	Geen beperkingen	√	√	√
	instellings-eigen desktop, -laptop (onbeheerd)		√	√	X
	instellings-eigen mobiele apparatuur (smartphone, tablet)		√	√ (mits versleuteld)	X
	eigen (privé) mobiele apparatuur / BYOD		√	X	X
digitaal opslaan	op eigen infrastructuur: netwerkmap (file share: home, public), DMS - Doc Mgt Systeem		√	√	√ (bij voorkeur versleuteld+2FA)
	op eigen infrastructuur: samenwerkingsomgeving (bv. UvA Communities)		√	√	√ (mits versleuteld+2FA)
	private cloud: samenwerkingsomgeving (bv. DLWO)		√	√	√ (mits versleuteld+2FA)
	community cloud (bv SIS, SURFdrive)		√	√	√ (mits versleuteld+2FA)
	public cloud, instellingsgebonden (bv. Microsoft Office 365, Google Apps for Education)		√	√	√ (mits versleuteld+2FA)
	public cloud, overig (bv Dropbox, Google+, Yammer, Basecamp); NB. Alleen met instemming van de CISO kan in bepaalde gevallen van de beveiligingseisen worden afgeweken		√ (mits versleuteld) Afwijken alleen met instemming CISO	X Afwijken alleen met instemming CISO	X Geen afwijking mogelijk
	instellings-eigen mobiele opslagmiddelen (usb-stick, e.d.)		√	√ (mits versleuteld)	X
	niet-instellings-eigen mobiele opslagmiddelen (BYOD)		√	X	X
verspreiden/verzenden (e-mail, e.d.)	binnen de instelling		√	√	√ (mits versleuteld)
	naar (vertrouwde) samenwerkingspartijen		√	√ (mits versleuteld)	√ (mits versleuteld)
	overig (inclusief via social media zoals LinkedIn, Facebook of Twitter		X	X	X
papier en overige informatiedragers					
printen	multifunctional, printer, e.d.	Geen beperkingen	beveiligd		
bewaren	papieren documenten + overige informatiedragers (USB-stick, CD/DVD, geheugen(kaart), microfilm, e.d.)		in afgesloten kast of ladenblok (alleen Zone 1 en 2)	in afgesloten kast of ladenblok	in afgesloten kluis
fysiek transport	door medewerker zelf of betrouwbare koeriersdienst		√	slechts bij absolute noodzaak; in verpakking waardoor inhoud niet zichtbaar, niet kenbaar en inbreuk detecteerbaar	
afdanken	papieren documenten		in afgesloten papiercontainer (alleen Zone 1 en 2)	gebruik van papierversnipperaar	
	overige informatiedragers (USB-stick, CD/DVD, geheugen(kaart), microfilm, e.d.)		inleveren bij Servicedesk		ondersteuning vragen bij Servicedesk