Informatiebeveiligingsbeleid Avans Hogeschool

Vaststelling

Dit beleid is vastgesteld door het CvB van Avans Hogeschool en treedt in werking per 3 juli 2018. Het beleid geldt totdat het wordt herzien dan wel ingetrokken.

De richtlijnen zijn niet vrijblijvend. Afwijking van de richtlijnen is alleen acceptabel op basis van een zorgvuldige risicoafweging. Deze afweging is altijd een besluit van verantwoordelijk management.

Dienst ICT en Facilitaire Zaken
Team Integrale Veiligheid

11 juni 2018

Management samenvatting

Deze notitie beschrijft het informatiebeveiligingsbeleid voor Avans Hogeschool. Jaarlijks wordt het informatiebeveiligingsbeleid geevalueerd en indien nodig bijgesteld. Met dit document zet Avans Hogeschool de volgende stap om de beveiliging van persoonsgegevens en andere informatie binnen de organisatie op orde te houden.

Het informatiebeveiligingsbeleid heeft als doel het waarborgen van de betrouwbaarheidsaspecten van de informatievoorziening (beschikbaarheid, integriteit en vertrouwelijkheid), het minimaliseren van schade door het voorkomen van beveiligingsincidenten en het minimaliseren van eventuele gevolgen. Het informatiebeveiligingsbeleid voldoet aan geldende wet- en regelgeving.

Aan de hand van de kenmerken vertrouwelijkheid, integriteit en beschikbaarheid wordt informatie geclassificeerd. De classificatie is een hulpmiddel om een eenvoudige risico analyse uit te voeren. De classificatie bepaalt uiteindelijk het minimale beveiligingsniveau dat moet worden gehanteerd. In de context waarin informatie wordt verwerkt, kan gekozen worden voor een hoger beveiligingsniveau. Juist daarom ligt de verantwoordelijkheid voor classificatie bij de proceseigenaar (veelal de directie van een diensteenheid of academie).

Het informatiebeveiligingsbeleid gaat zeker niet alleen over ICT. Maatregelen die worden genomen om te komen tot een juist beveiligingsniveau zijn zowel fysiek, technisch als van organisatorische aard. Dit is een belangrijke reden om de organisatie vanuit één loket te ondersteunen: Team Integrale Veiligheid. Dit team acteert binnen de Dienst ICT & Facilitaire zaken en richt zich op alle aspecten van veiligheid, dus ook informatiebeveiliging. Daar waar gevraagd, ondersteunt het team de organisatie in de classificatie en uitvoering van maatregelen. Dit is inclusief regie op derden, audit en Privacy Impact Assesment (PIA). Het maakt onderdeel uit van de basisdienstverlening.

Er wordt aandacht geschonken aan twee belangrijke principes uit Avg: Privacy by design (het ontwerp) en privacy by default (de default instellingen in het proces). De rode draad die loopt door de Avg**:**

> **"*Als je aan de slag gaat met persoonsgegevens, denk van te voren goed na hoe je de rechten van de betrokkene optimaal respecteert, gebruik alleen die gegevens die je echt nodig hebt en zorg er voor dat je gegevens, nadat wettelijke bewaartermijnen zijn verstreken, vernietigt.*"**

Leeswijzer:
Het informatiebeveiligingsbeleid gaat een ieder aan. Hierbij is bijzondere rol weggelegd voor onze medewerkers die het beleid vertalen naar operatie en te maken krijgen met alledaagse vraagstukken. Mede daarom is deze notitie opgebouwd uit twee delen:

- Deel 1 is bedoeld voor management en beschrijft het informatiebeveiligingsraamwerk voor Avans Hogeschool. Dit deel gaat vooral in op de vraag waarom we beveiligen, welke doelen we nastreven, de uitgangspunten en principes die we hanteren en de wijze waarop we invulling geven aan de organisatie van informatiebeveiliging.
- Deel 2 is bedoeld voor specialisten (zoals architecten, security functionarissen, ICT-contactpersonen, privacy contactpersonen, functioneel- en technisch beheerders) en beschrijft de architectuur en beheersmaatregelen meer in detail.

Inhoudsopgave

Definities

Beschikbaarheid van informatievoorziening: De mate waarin informatie en/of functionaliteit op de juiste momenten beschikbaar zijn voor gebruikers. Informatie en functionaliteit dienen voor gebruikers zodanig beschikbaar te zijn dat zij hun taken optimaal kunnen uitvoeren.

Integriteit van de informatievoorziening: De mate waarin vast staat dat de informatie of functionaliteit volledig en juist is (dat er geen manipulatie van data kan plaatsvinden of heeft plaatsgevonden).

Vertrouwelijkheid van de informatievoorziening: De mate waarin de toegang tot (persoons)gegevens of functionaliteit beperkt is tot degenen die daartoe bevoegd zijn. Toegang tot (persoons)gegevens en functionaliteit is beperkt tot degenen die daartoe door de eigenaar hiervan is vastgesteld.

BIV-codering: Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV). De classificatie van informatie of functionaliteit is op basis van deze codering. Dit wordt ook wel de betrouwbaarheid van de informatievoorziening genoemd.

CSIRT: Computer Security Incident Response Team. Het CSIRT is een formeel team met bevoegdheden om beveiligingsincidenten te behandelen en direct maatregelen te nemen indien de situatie dat vereist.

Avg: Algemene Verordening Gegevensbescherming (Avg). De Avg zorgt onder meer voor versterking en uitbreiding van privacy rechten, meer verantwoordelijkheden voor organisaties en bevoegdheid voor toezichthouders om boetes uit te delen.

Informatiebeveiliging: Het treffen en onderhouden van een samenhangend pakket aan maatregelen om de kwaliteitsaspecten van de informatievoorziening (beschikbaarheid, integriteit en vertrouwelijkheid) te waarborgen. Hierbij gaat het ook om de controleerbaarheid van de maatregelen die genomen zijn om deze kwaliteitsaspecten te borgen.

PIA: (Data) Privacy Impact Assessment: Een onderzoek op de verwerking van persoonsgegevens waarbij privacy risico's in kaart worden gebracht en maatregelen worden voorgesteld om de risico's te verkleinen tot een acceptabel niveau.

Privacy by design: houdt in dat al tijdens het ontwerpen van producten en diensten (zoals informatiesystemen) ervoor wordt gezorgd dat persoonsgegevens goed worden beschermd. Vergelijk dit met de architectuur van een huis waarbij bijvoorbeeld een alarmsysteem en veilige deursloten worden opgenomen in het bestek en tekening. Ook niet meer gegevens verzamelen dan noodzakelijk voor het doel van de verwerking (dataminimalisatie) behoort dat Privacy by design. En dat de gegevens niet langer worden bewaard dan nodig (recordmanagement).

Privacy by default: het toepassen van default settings op een zodanige wijze dat de privacy zo optimaal mogelijk wordt gewaarborgd in het proces (de verwerking). Het betekent bijvoorbeeld dat het alarmsysteem van het huis alleen uitstaat als je thuis bent en dat ramen en deur standaard op slot zijn.

Dataminimalisatie: Alleen die persoonsgegevens die noodzakelijk zijn voor het doel van de verwerking, worden verwerkt. Dataminimalisatie geeft direct invulling aan de grondslag van de verwerking. Gegevens die niet nodig zijn voor de verwerking, moeten buiten beschouwing worden gelaten.

Anonimiseren: Bij anonimiseren worden persoonsgegevens zodanig bewaard, dat na toepassing ervan het herleiden van gegevens tot individuen niet meer mogelijk is. Het betreft een onomkeerbare actie. Na volledige anonimisering van gegevens is privacywetgeving niet meer van toepassing op die gegevens.

Pseudonimiseren: Met pseudonimiseren worden persoonsgegevens getransformeerd in een dataset die niet meer direct herleidbaar is tot een persoon. Om dit te doen worden de direct identificeerbare elementen van een persoonsgegeven weggehaald, zoals de naam, of de dataset wordt omgecodeerd tot een nummer. Vervolgens worden de gepseudonimiseerde dataset en de (sleutel tot de) brondata apart bewaard en zijn er waarborgen aanwezig die re-identificatie voorkomen (bijv. beleid of contracten). Belangrijk is dat de originele identificerende elementen, of de brondata, nog aanwezig zijn. Wanneer deze data vernietigd zijn, of re-identificatie anderszins onmogelijk is, is sprake van anonieme gegevens.

Encryptie: is het versleutelen van gegevens op basis van een bepaald algoritme. Het belangrijkste doel van encryptie is dat de veiligheid van gegevens gewaarborgd blijft, óók als derden toegang zouden verkrijgen tot het opslagmedium of het communicatiekanaal. De versleuteling zorgt er dan voor dat deze derden de gegevens niet kunnen lezen.

Penetratietest: Een penetratietest of pentest is een test van een of meer computersystemen op kwetsbaarheden, waarbij deze kwetsbaarheden ook werkelijk gebruikt worden om in deze systemen in te breken. Een penetratietest vindt normaal gesproken om rechtmatige redenen plaats, met toestemming van de eigenaars van de systemen die getest worden, met als doel de systemen juist beter te beveiligen.

DEEL 1:
DE BELEIDSKADERS EN DE ORGANISATIE VAN DE INFORMATIEBEVEILIGING

Kader van veiligheid: integrale veiligheid en daarmee ICT-veiligheid en veiligheid op de werkvloer

1 Informatiebeveiliging

1.1. Inleiding

De belangstelling en noodzaak voor informatiebeveiliging is de afgelopen jaren enorm toegenomen. Dit vanwege de alsmaar toenemende bedreigingen zoals cybercriminaliteit maar ook diverse ernstige beveiligingsincidenten zoals bijvoorbeeld bij Hogeschool Van Hall Larenstein[1] en Erasmus Universiteit[2].

Surf stelt jaarlijks een rapport op waarin de dreigingen voor het onderwijs in beeld zijn gebracht[3]. Hieruit blijkt dat de grootste dreigingen voor ons identiteitsdiefstal, verstoring van de ICT, diefstal van informatie en datalekken zijn. Vooral privacygevoelige informatie, aanbesteding-informatie en vertrouwelijke bedrijfsgegevens zoals tentamens moeten beschermd worden om schade te voorkomen of te beperken. De verplichtingen voortvloeiend uit de Avg hebben een rechtstreekse impact op de informatiebeveiliging bij Avans Hogeschool. Niet nakomen van deze verplichtingen kan leiden tot een boete van maximaal 10 miljoen euro, welke kan worden verdubbeld in het geval van een datalek.

Informatiebeveiliging is dus meer dan ICT, computers en automatisering. Het gaat ook wetgeving, mensen en processen. Het proces van informatiebeveiliging is dan ook gericht op bescherming van informatie door middel van technische en organisatorische maatregelen en nakomen van wetgeving. Het informatiebeveiligingsbeleid (dit document) geeft hier invulling aan.

1.2. Het doel van het informatiebeveiligingsbeleid

Het informatiebeveiligingsbeleid heeft als doel het borgen van de kwaliteit van de informatievoorziening (beschikbaarheid, integriteit en vertrouwelijkheid), het minimaliseren van schade door het voorkomen van beveiligingsincidenten en het minimaliseren van eventuele gevolgen. Het informatiebeveiligingsbeleid biedt een kader om aan huidige en toekomstige wet- en regelgeving te voldoen en biedt kansen om op veilige wijze nieuwe dienstverlening te ontwikkelen.

Om deze doelstelling te bereiken dient in het volgende te worden voorzien (deze onderwerpen worden in het vervolg van dit document uitwerkt):

Governance: Expliciet vastgestelde beveiligingsorganisatie: uitgangspunten en organisatie van informatiebeveiligingsfuncties zijn vastgelegd en worden gedragen door het bestuur, en afgeleid daarvan, door de hele instelling.

Compliance: Het beleid biedt de basis om te voldoen aan wettelijke voorschriften. Voor wat betreft Avg wordt het framework Privacy by Design[4] van de Privacy Group gevolgd. Dit framework biedt de zekerheid dat alle aspecten die onderdeel uitmaken van de Avg worden geadresseerd.

Normen: Voor de ondersteuning van Hogescholen bij het formuleren en realiseren van hun informatiebeveiligingsbeleid heeft de SURF Community voor Informatiebeveiliging en Privacy (SCIPR) een Normenkader Informatiebeveiliging HO 2105[5] en het Juridisch Normenkader Cloudservices HO[6] ontwikkeld, welke is gebaseerd op algemeen

1 https://nos.nl/artikel/2091324-hogeschool-mailt-per-ongeluk-gegevens-van-4400-studenten-rond.html

2 https://nos.nl/artikel/2143824-lek-erasmus-universiteit-betrof-ook-medische-gegevens-studenten.html

3 https://www.surf.nl/nieuws/2017/12/cyberdreigingsbeeld-2017-toont-belangrijkste-dreigingen.html

4 https://www.privacycompany.eu/factsheets/#%2Ffiles%2FPrivacy%20by%20Design%20Framework.pdf

5 https://www.surf.nl/diensten-en-producten/surfaudit/normenkader-surfaudit/index.html

6 https://www.surf.nl/binaries/content/assets/surf/nl/kennisbank/2013/juridisch<normenkader<cloudservices<hoger<onderwijs.pdf

geaccepteerde Nen-normen NEN/ISO 27001[7]. Door het Normenkader als basis te nemen wordt de kwaliteit van het Informatiebeveiligingsbeleid geborgd.

Maatregelen: De Baseline Informatiebeveiliging HO 2015[8] en de Baseline Informatiebeveiliging Rijksdienst[9] wordt als uitgangspunt genomen bij het vaststellen van maatregelen. Daarmee wordt geborgd dat maatregelen minimaal in overeenstemming zijn met wat algemeen geldend is binnen de overheid en het Hoger Onderwijs.

Proces: Zonder goed uitwerkt proces (PDCA) en controle op opzet, bestaan en werking zal de doelstelling niet worden behaald. Zoals eerder vastgesteld kent de vertaling van risico naar maatregel zowel een technische als een organisatorische component.

1.3. Reikwijdte van het beleid

Bij Avans Hogeschool wordt informatiebeveiliging breed geïnterpreteerd. Dit betreft dus alle vormen van informatie die verwerkt worden, al dan niet in digitale vorm. Persoonsgegevens vallen hier ook onder. Op dit punt is er een duidelijke overlap tussen het informatiebeveiligingsbeleid en het privacy beleid.

Bij het informatiebeveiligingsbeleid ligt de nadruk op die toepassingen die onder de verantwoordelijkheid van Avans Hogeschool vallen. Dit heeft zowel betrekking op gecontroleerde informatie, die door ons zelf is gegenereerd en wordt beheerd, als ook op niet- gecontroleerde informatie, bijv. uitspraken van medewerkers in discussies op elektronische platforms, persoonlijke websites of publieke forums, waarop Avans Hogeschool kan worden aangesproken.

Het informatiebeveiligingsbeleid heeft betrekking op alle medewerkers, studenten, gasten, bezoekers en externe relaties, alsmede op alle instellingsonderdelen en dienstverlening. Tevens vallen onder het informatiebeveiligingsbeleid alle devices die Avans Hogeschool in eigendom heeft. Ten aanzien van Bring your own devices (BYOD) wordt apart beleid opgesteld (beleid mobiele devices) maar in beginsel strekt het informatiebeveiligingsbeleid zich ook uit tot BYOD.

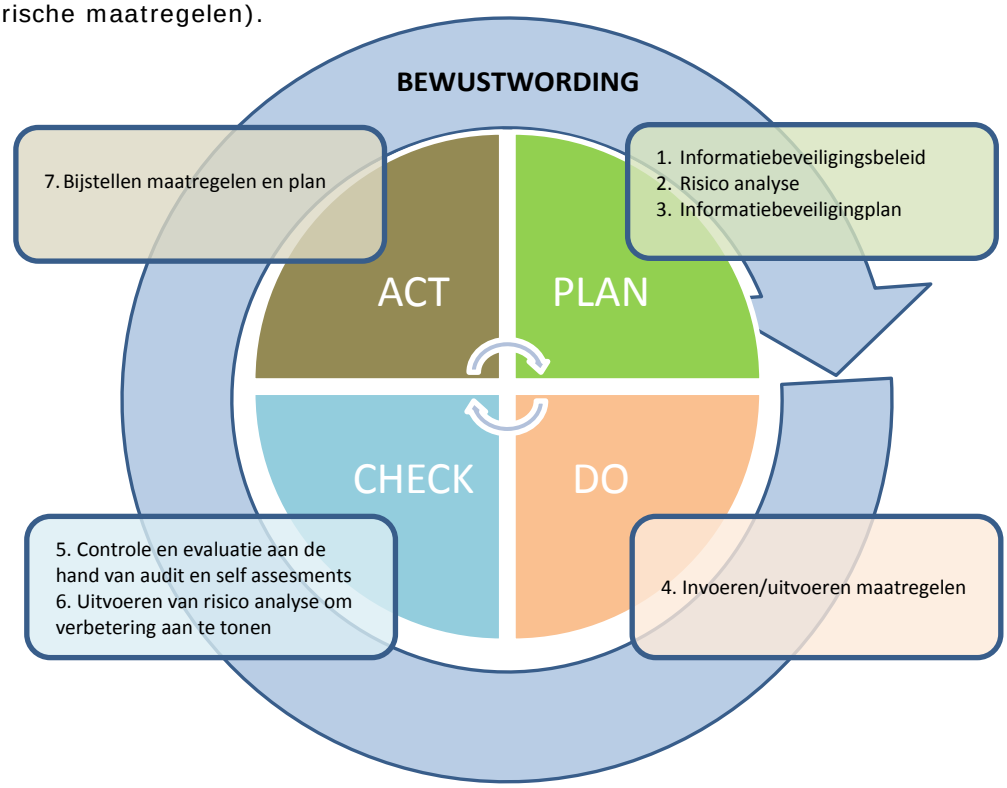
[7] Voluit: NEN-ISO/IEC 27001: Eisen aan Managementsystemen voor Informatiebeveiliging

[8] https://www.surf.nl/binaries/content/assets/surf/nl/2015/baseline-informatiebeveiliging-ho-2015.pdf

[9] BIR Tactisch Normenkader 1.0, 2012

2 Proces informatiebeveiliging

Informatiebeveiligingsmanagement wordt als proces ingericht op basis van “Plan, Do, Check, Act” (zie onderstaand figuur) en volgt PC-cyclus. Het informatiebeveiligingsplan geeft voor de komende jaren invulling aan het Informatiebeveiligingsbeleid en is een apart document. De uitvoering van dit plan komt tot uiting in het jaarlijks businessplan van DIF. De resultaten ervan worden geëvalueerd en vertaald naar nieuwe jaarplanningen. Het informatiebeveiligingsjaarplan zal als apart onderdeel binnen DIF worden vastgelegd en worden opgenomen in het DIF-businessplan, echter de maatregelen kunnen ook in de jaarplannen van de bedrijfsonderdelen naar voren komen (met name organisatorische maatregelen).



In deze planning en controlecyclus laten we ons leiden door de volgende generieke principes:

- Avans Hogeschool is pleitbezorger van goede beveiliging en privacy en de bijbehorende bewustwording.
- Avans Hogeschool is een instelling met een open karakter. Adequate beveiliging is daarbij wel een randvoorwaarde. Er wordt van medewerkers, studenten en derden verwacht dat ze zich qua techniek en ook qua houding ‘fatsoenlijk’ gedragen (eigen verantwoordelijkheid). Niet acceptabel is dat door al dan niet opzettelijk gedrag onveilige situaties ontstaan die leiden tot schade en/of imagoverlies. Het is om deze reden dat er gedragscodes zijn geformuleerd en geïmplementeerd.
- Het succes van beveiliging staat of valt met goede communicatie. Goede communicatie wordt daarom actief bevorderd, op en tussen alle niveaus in de instelling.
- Bij elke IT-inrichting wordt ter bevordering van informatiebeveiliging en privacy het principe van *least privileges* gehanteerd, wat wil zeggen dat ernaar wordt gestreefd om steeds niet meer dan die rechten te verlenen die nodig zijn voor adequate functie- en bedrijfsuitoefening.
- Informatiebeveiliging is een verantwoordelijkheid voor allen.

- Informatiebeveiliging is een continu proces. Technologische en organisatorische ontwikkelingen binnen en buiten Avans Hogeschool maken het noodzakelijk om periodiek te bezien of men nog wel op de juiste wijze bezig is de beveiliging te waarborgen. Extern treedt hierbij BE&C op als business partner op beleidsmatig vlak, terwijl het proces van vertaling van beleid naar operatie en de procesmatige uitvoering van de operatie zelf onderdeel uit maakt van de ISO certifiering van DIF. Daarnaast wordt binnen DIF intern controle uitgevoerd op de werking van de processen door de kwaliteitsmedewerker en op de inhoudelijke kwaliteit van de maatregelen door de Security Manager vanuit het Team Integrale Veiligheid.

- Eigendom van informatie: Avans Hogeschool is in beginsel eigenaar van de informatie die onder haar verantwoordelijkheid wordt geproduceerd. Daarnaast beheert Avans Hogeschool informatie, waarvan het intellectueel eigendom toebehoort aan derden. Medewerkers, studenten en derden dienen goed geïnformeerd te zijn over de regelgeving voor het (her)gebruik van deze informatie.

- Bij elke mutatie, zoals infrastructurele wijzigingen, (IT)projecten of de aanschaf van nieuwe systemen wordt reeds in het vroegst mogelijke stadium rekening gehouden met informatiebeveiliging. Dit sluit ook aan bij de Avg, welke in deel 2 van dit document wordt uitgewerkt.

- Avans Hogeschool stelt de benodigde mensen en middelen beschikbaar om haar eigendommen en werkprocessen te kunnen beveiligen volgens de wijze gesteld in dit beleid. Wanneer er sprake is van een investering zal hiervoor budget worden gevraagd in het informatiebeveiligingsplan.

- Iedere medewerker, zowel vast als tijdelijk, intern of extern is verplicht waar nodig gegevens en informatiesystemen te beschermen tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht en bij vermeende inbreuken hiervan melding te maken.

- Informatiebeveiligingsbeleid maakt onderdeel uit van Business Continuity Management (BCM) voor wat betreft de beschikbaarheid van de ICT systemen in het geval van een calamiteit (disaster recovery).

- Daar waar mogelijk en zinvol sluit Avans Hogeschool aan bij beleid en maatregelen aangereikt vanuit Surf en de Rijksoverheid waaronder de bij paragraaf 1.2. genoemde documenten.

3 Classificatie van informatie

3.1. Doel

Om te kunnen bepalen welke beveiligingsmaatregelen moeten worden getroffen t.a.v. informatie en functionaliteit is een risicoanalyse noodzakelijk. Hierin wordt vastgesteld welke risico's worden gelopen en hoe groot deze risico's zijn. Per risico wordt de kans van het optreden ervan bepaald en wordt vervolgens berekend wat de schade is die op zou kunnen optreden als een bedreiging zich daadwerkelijk voordoet.

Na de analyse wordt vastgesteld op welke wijze de risico's beheerst kunnen worden, of teruggebracht tot een aanvaardbaar niveau: het treffen van informatiebeveiligingsmaatregelen. Op voorhand hoeft niet ieder risico te worden afgedekt: wanneer de kosten van de maatregelen om een risico te beperken hoger zijn dan de mogelijke schade, kan worden besloten worden om het risico te accepteren.

Bij deze vertaling van risico naar maatregel is classificatie van informatie een belangrijk hulpmiddel om de ernst van een risico en de reikwijdte van een maatregel te kunnen bepalen. De verantwoordelijkheid hiervoor ligt bij de informatie-eigenaar (zie 6.1). Met het toekennen van classificatieniveaus[10] aan informatie en functionaliteit wordt zodoende het minimaal (vereiste) beschermingsniveau kenbaar gemaakt.

3.2. Uitgangspunten

De volgende principes zijn het uitgangspunt voor (data) classificatie:

- De informatie-eigenaar (zie 6,1) bepaalt de classificatie en het daarmee vereiste beschermingsniveau binnen de wettelijke kaders. De eigenaar van de gegevens bepaalt wie toegang krijgt tot welke gegevens.
- We streven naar een zo 'laag' mogelijk classificatieniveau; te hoge classificatie leidt tot onnodige kosten en beperking in werkbaarheid.
- De classificatie heeft betrekking op gegevensverzamelingen, gegevensdragers, informatiesystemen.
- Het object van classificatie is informatie. De classificatie die door de soort informatie bepaald wordt geldt ook voor het hogere niveau van informatiesystemen (of informatieservices), dat wil zeggen dat als een systeem geheime informatie verwerkt, het hele systeem als geheim wordt aangemerkt tenzij voor dat hogere niveau maatregelen genomen zijn binnen het informatiesysteem. Alle classificaties van alle bedrijfskritische systemen dienen centraal te zijn vastgelegd en jaarlijks gecontroleerd te worden.

Naarmate de gegevens een gevoeliger karakter hebben, of gezien de context waarin ze gebruikt worden een groter risico inhouden, dienen zwaardere eisen aan de beveiliging van die gegevens te worden gesteld. Dit maakt classificatie van informatie complex en een verantwoordelijkheid van de informatie-eigenaar (zie 6.1).
Voorbeelden:

- NAW wordt voor wat betreft de vertrouwelijkheid geclassificeerd als vertrouwelijk. Echter, NAW-gegevens van een collega in een blijf-van-lijf-huis maakt de classificatie 'geheim'.
- Geboortedatum kent een absolute integriteit in een P&O systeem, echter op een verjaardagskalender is de integriteit minder van belang en uit hoofde van grondslag is wellicht zelfs het gebruik van het geboortejaar niet toegestaan.
- De beschikbaarheidseisen t.a.v. van betalingsgegevens is laag maar op het tijdstip van de verwerking van incasso is beschikbaarheid essentieel.

[10] Handreiking dataclassificatie CIO platform 2016

3.3. Classificatie

Er wordt geclassificeerd op de volgende kenmerken van de informatievoorziening (zie hoofdstuk 1): beschikbaarheid, integriteit en vertrouwelijkheid.

De onderscheiden niveaus van vertrouwelijkheid zijn:

- **Openbaar**: Alle informatie die algemeen toegankelijk is voor eenieder. Er is geen schending van deze classificatie mogelijk.
- **Bedrijfsvertrouwelijk**: Informatie die toegankelijk mag of moet zijn voor alle medewerkers van de eigen organisatie(s). Vertrouwelijkheid is gering. Schending van deze classificatie kan enige (in)directe schade toebrengen.
- **Vertrouwelijk**: Informatie die alleen toegankelijk mag zijn voor een beperkte groep gebruikers. De informatie wordt ter beschikking gesteld op basis van vertrouwen. Schending van deze classificatie kan serieuze (in)directe schade toebrengen.
- **Geheim:** Dit betreft gevoelige informatie die alleen toegankelijk mag zijn voor de direct geadresseerde. Schending van deze classificatie kan zeer grote schade toebrengen.

De onderscheiden niveaus van integriteit zijn:

- **Niet zeker**: Deze informatie mag worden veranderd. Geen extra bescherming van integriteit noodzakelijk. Schending van integriteit heeft geen gevolgschade.
- **Beschermd**: Het bedrijfsproces dat gebruik maakt van deze informatie staat enkele integriteitsfouten toe. Een basisniveau van beveiliging is noodzakelijk. Schending van deze classificatie kan enige (in-)directe schade toebrengen
- **Hoog**: Het bedrijfsproces dat gebruik maakt van deze informatie staat zeer weinig integriteitsfouten toe. Bescherming van integriteit is absoluut noodzakelijk. Schending van deze classificatie kan serieuze (in)directe schade toebrengen.
- **Absoluut**: Het bedrijfsproces dat gebruik maakt van deze informatie staat geen integriteitsfouten toe. Schending van integriteit kan (zeer) grote schade toebrengen

De onderscheiden niveaus van beschikbaarheid zijn:

- **Niet nodig:** De gegevens kunnen zonder gevolgen langere tijd niet beschikbaar zijn. On beschikbaarheid heeft geen gevolgschade.
- **Noodzakelijk:** De informatie of service mag incidenteel uitvallen, het bedrijfsproces staat incidentele uitval toe. De continuïteit zal op redelijke termijn moeten worden hervat. Onbeschikbaarheid kan enige (in)directe schade toebrengen
- **Belangrijk:** De informatie of service mag bijna nooit uitvallen, het bedrijfsproces staat nauwelijks uitval toe. De continuïteit zal snel moeten worden hervat. Onbeschikbaarheid kan serieuze (in)directe schade toebrengen.
- **Essentieel:** De informatie of service mag alleen in zeer uitzonderlijke situaties uitvallen, bijvoorbeeld als gevolg van een calamiteit, het bedrijfskritische bedrijfsproces staat eigenlijk geen uitval toe. De continuïteit zal zeer snel moeten worden hervat. Onbeschikbaarheid kan (zeer) grote schade toebrengen.

Onderstaande classificatietabel kan worden beschouwd als een vereenvoudigde vorm van een risicoanalyse. Per kolom wordt geclassificeerd waardoor er per betrouwbaarheidsaspect een geadviseerd beveiligingsniveau ontstaat. Zo kan het beveiligingsniveau van 'vertrouwelijkheid' bijvoorbeeld laag zijn en integriteit hoog.

VERTROUWELIJKHEID	INTEGRITEIT	BESCHIKBAARHEID	BESCHERMINGSNIVEAU
Openbaar Informatie mag door iedereen worden ingezien *(Bijv. algemene informatie op de externe website)*	**Niet zeker** Informatie mag worden veranderd *(Bijv. templates en sjablonen)*	**Niet nodig** Gegevens kunnen zonder gevolgen langere tijd niet beschikbaar zijn *(Bijv.: ondersteunende tools als routeplanner)*	**GEEN**
Bedrijfsvertrouwelijk Informatie is toegankelijk voor alle medewerkers van de organisatie *(Bijv. informatie op intranet)*	**Beschermd** Het bedrijfsproces staat enkele (integriteit)-fouten toe *(Bijv. niet kritische rapportages)*	**Noodzakelijk** Informatie mag incidenteel niet beschikbaar zijn *(Bijv. administratieve systemen)*	**LAAG**
Vertrouwelijk Informatie is alleen toegankelijk voor een beperkte groep *(Bijv. persoonsgegevens)*	**Hoog** Het bedrijfsproces staat zeer weinig fouten toe *(Bijv. bedrijfsvoering informatie)*	**Belangrijk** Informatie moet vrijwel altijd beschikbaar zijn, continuïteit is een belangrijk *(Bijv. primair proces)*	**MIDDEN**
Geheim Informatie is alleen toegankelijk voor direct geadresseerden *(Bijv. behandeling klacht examencommissie)*	**Absoluut** Het bedrijfsproces staat geen fouten toe *(Bijv. informatie op de website)*	**Essentieel** Informatie mag alleen in uitzonderlijke situaties uitvallen, bijvoorbeeld bij calamiteiten *(Bijv. blackboard)*	**HOOG**

De eigenaar van informatie bepaalt wie toegang krijgt tot welke informatie en welke passende beheersmaatregelen van toepassing zijn (op basis van verdere risicoanalyse en beveiligingseisen). Hierbij ligt de **focus** zowel op **mens (gedrag, processen)** als op techniek **(ICT-infrastructuur).**

In bijlage 3 wordt een uitwerking gegeven van de beveiligingsniveaus in concrete beheersmaatregelen op het vlak van techniek. Daarnaast wordt in deel 2 in detail in gegaan op een aantal beheersmaatregelen zoals logische toegangsbeveiliging, versleuteling, zonering en filtering, applicatie controles, systeemintegriteit, onweerlegbaarheid, continuïteit, redundantie en logging en monitoring.

4 Avg

4.1. Privacy en Privacy Impact Assessment (PIA)

Er is een overlap tussen het informatiebeveiligingsbeleid en het Privacy beleid. Dit vereist enerzijds afstemming maar anderzijds versterkt het elkaar ook; Zo ontstaat er de mogelijkheid om de betrouwbaarheid van de informatievoorziening nog beter op de kaart te zetten. Daar waar vanuit het perspectief van informatiebeveiliging soms nog een afweging mogelijk is tussen het belang van de maatregel ten opzichte van de werkbaarheid en financiële consequentie, geeft de Avg minder ruimte.

Voor elke verwerking van persoonsgegevens die een hoog privacy risico oplevert, dient een PIA te worden uitgevoerd. Hierbij volgt Avans de criteria die door de Autoriteit Persoonsgegevens zijn opgesteld ter bepaling hiervan. De PIA is een verantwoordelijkheid van de proces eigenaar. De proces eigenaar wordt hierbij, indien gevraagd, ondersteunt door het Team Integrale Veiligheid (zie ook hoofdstuk 6). Het Team Integrale Veiligheid levert hierbij de expertise om het geheel aan fysieke, organisatorische en technische maatregelen te beoordelen. Dit past bij de activiteiten die DIF nu reeds uitvoert: Regie op derde partijen en de verantwoordelijkheid van DIF op het vlak van (informatie)beveiliging, gegevensuitwisseling en document management.

4.2. Privacy by design

Avans volgt voor de uitwerking van Avg het framework van de Privacy Group (zie bijlage 2). Het framework steunt op 2 belangrijke pijlers: privacy by design and privacy by default. De gedachte achter privacy by design loopt ook als een rode draad door de wet:

> "***Als je aan de slag gaat met persoonsgegevens, denk van tevoren goed na hoe je de rechten van de betrokkene optimaal respecteert, gebruik alleen die gegevens die je echt nodig hebt en zorg ervoor dat je gegevens nadat wettelijke bewaartermijnen zijn verstreken, vernietigt.***"

Privacy by default is uiteindelijk een invulling van deze gedachte. Naast het opnemen van deze pijlers in de architectuur principes van Avans en in de PMC-methodiek wordt daarom ook in de bewustwording campagnes nadrukkelijk ingezet op Privacy by Design.

Persoonsgegevens worden niet langer dan noodzakelijk bewaard. Voor Avans fungeert de zogenaamde Selectielijst Hogescholen als basis voor het archiverings- en bewaarbeleid. Die selectielijst bevat een 137-tal onderwijsprocessen, waarbij een bewaartermijn in acht genomen moet worden. Pér proces is opgenomen welke bewaartermijn geldt dan wel door Avans gehanteerd wordt. Hiervoor is binnen Avans Records Management opgezet (onderdeel functioneel beheer DIF Document Management) om de organisatie te voorzien van richtlijnen op het gebied van bewaren en verwijderen.

5 Wet- en regelgeving

Uitgangspunt is dat Avans voldoet aan alle van toepassing zijnde wet- en regelgeving, en zich voorbereidt om aan opkomende wetgeving tijdig te voldoen. Hoe Avans omgaat met relevante wet- en regelgeving staat beschreven in Bijlage 1 Wet- en regelgeving.

6 Rollen en verantwoordelijkheden

6.1. Algemeen

In deze paragraaf is beschreven hoe informatiebeveiliging is georganiseerd en wie waarvoor verantwoordelijk is. Wat betreft de benaming van rollen wordt zoveel mogelijk aangesloten bij het PvIB.[11]. Verantwoording is ingeregeld conform het bestaande Avans' besturingsmodel.

College van Bestuur
Het College van Bestuur (CvB) is eindverantwoordelijk voor de informatiebeveiliging binnen Avans en stelt het beleid en de basismaatregelen op het gebied van informatiebeveiliging vast. Zij laat zien dat zij informatiebeveiliging ondersteunt en zich betrokken voelt door het uitdragen en handhaven ervan. De informatiebeveiliging bij Avans is gemandateerd aan de directeur van de Dienst DIF.

CISO
De rol van CISO – Chief Information Security Officer – is belegd bij de directie van DIF. De CISO is verantwoordelijk voor de professionalisering en borging van de informatiebeveiliging van Avans. Hieronder wordt verstaan de beveiliging van de informatievoorziening (waaronder IT-infrastructuur), het inzichtelijk maken van risico's Avansbreed, het opstellen van kaders, het monitoren van de naleving daarvan, Business Continuity Management (BCM) en het doen van verbetervoorstellen om het beveiligingsniveau continu te verbeteren. De CISO rapporteert integraal over informatiebeveiliging bij Avans aan het College van Bestuur.

Team Integrale Veiligheid *(en daarmee ICT-veiligheid)*
Avans kiest ervoor om informatiebeveiliging als onderdeel van integrale veiligheid te positioneren om zodoende alle aspecten van beveiliging vanuit een overkoepelende risicoanalyse daadkrachtiger te kunnen benaderen.

Het Team Integrale Veiligheid vorm het aanspreekpunt voor de organisatie voor alle vragen op het gebied van veiligheid en ondersteunt de organisatie bij de classificatie en uitvoering van maatregelen, inclusief regie op applicaties van derden. Samen met de proceseigenaren speelt het team een rol bij de vertaling van de strategie naar tactische (en operationele) plannen. Op operationeel niveau wordt overlegd met de privacy officers, functionele beheerders en relevante (ICT) medewerkers. Er wordt aandacht geschonken aan de implementatie van de informatiebeveiligingsmaatregelen op alle niveaus. Team Integrale Veiligheid voert audit uit op de opzet, bestaan en werking van de ICT operatie.

DIF
DIF is verantwoordelijk voor de beveiliging van de ICT-infrastructuur en de adequate inrichting van de systemen waarvan DIF eigenaar is. Dit betekent dat deze zowel nu als in de toekomst blijft voldoen aan de eisen en wensen van de gebruikers en aan de uitgangspunten van het informatiebeveiligingsbeleid.

Directeuren van academies en diensten (inclusief DIF)
Implementatie en naleving van het Informatiebeveiligingsbeleid is onderdeel van de integrale bedrijfsvoering. Iedere directeur heeft de taak om periodiek ervoor te zorgen dat zijn medewerkers op de hoogte zijn van het beleid en actief toe te zien op de implementatie en naleving. Hiertoe krijgen de directeuren ondersteuning vanuit het Team Integrale Veiligheid en de service managers DIF.

[11] Functies in de informatiebeveiliging. Platform voor Informatiebeveiliging (PvIB), 2006

Medewerkers
Informatieveiligheid begint bij het individu. Dit houdt in dat medewerkers eindverantwoordelijk zijn voor hun eigen informatiebeveiliging. Medewerkers dienen de door Avans voorgeschreven beveiligingsmiddelen en informatiebeveiliging maatregelen te gebruiken en te volgen. Zij zijn zich bewust van relevante wet- en regelgeving en signaleren (potentiële) beveiligingsincidenten.

Functionaris Gegevensbescherming (FG)
De FG is de interne toezichthouder op toepassing en naleving van de privacywetgeving. De taak van FG is belegd bij de stafafdeling Beleidsevaluatie en -Control (BE&C). Voor verdere uitwerking van deze rol zie het Avans Privacy Beleid.

CSIRT
Om beveiligingsincidenten goed te kunnen behandelen, is een CSIRT noodzakelijk (Computer Security Incident Response Team). Het Computer Security Incident Response Team (CSIRT) is verantwoordelijk voor het incidentbeheer en – registratie. Incidentbeheer en –registratie heeft betrekking op de wijze waarop geconstateerde dan wel vermoede inbreuken op de informatiebeveiliging door medewerkers, studenten en derden gemeld worden en de wijze waarop deze worden afgehandeld. Het CSIRT bij Avans opereert binnen DIF en is aangesloten bij Surfnet Community van Incident Response Teams.

Het doel van het CSIRT is het zo mogelijk voorkomen van informatiebeveiligingsincidenten en deze te bestrijden zo ze zich voordoen en daarmee de continuïteit van Avans te ondersteunen en haar reputatie te beschermen. Het CSIRT houdt zich ook bezig met beveiligingsincidenten buiten Avans als daar eigen medewerkers in enige rol bij betrokken zijn. In zulke gevallen wordt in principe gebruik gemaakt van de diensten van Surfcert, die wereldwijd in verbinding staat met andere CSIRT's.

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

Informatie-eigenaar
De informatie-eigenaar is diegene die uit hoofde van de verantwoordelijkheid voor een bepaald proces of systeem verantwoordelijk is voor het veilig gebruik van informatie binnen dat proces of systeem. Andere namen voor de Informatie-eigenaar zijn dan ook de Proces-eigenaar of Systeem-eigenaar. Wanneer onderdelen van informatie naar een (externe) andere organisatie worden overgedragen, blijft de eindverantwoordelijkheid voor de bescherming van de informatie altijd van de eigenaar.

6.2. RACI-schema

Van belang is om aan te geven wie waarvoor verantwoordelijk is. Daarbij worden diverse rollen onderscheiden zowel op richtinggevend of strategisch, sturend of tactisch en uitvoerend niveau. Het aantal rollen is als regel groter dan het aantal personen dat die rollen vervult.

In onderstaand RACI-schema weergegeven:

Activiteit / Onderdeel	College van Bestuur	Bedrijfsonderdeel (incl DIF)	CISO - Directie DIF	Team Integrale Veiligheid	CSIRT	FG / BF&C
RICHTEN						
informatiebeveiliging (IB)-beleid	A	C	R	I		
Bepalen organisatie t.b.v. Informatiebeveiliging	A	C	R	I		
Informatiebeveiliging planning en control vaststellen		I	A	R		
Verzorgen communicatie naar management en organisatie		I	A	R	I	I
INRICHTTEN						
Uitwerking beleid naar plan		I	A	R		S
Organisatie inrichting		I	A	R		I
Ontwikkelen van IB-maatregelen (extra t.o.v. de baseline Informatiebeveiliing HO 2015)		A/R	I	C		C
Sturen op implementatie (realisatie) van IB-maatregelen		A/R		C		
Evalueren en bijstellen van IB-maatregelen		A/R		C		
Begeleiden externe audits		A/R	I	C		
Verzorgen communicatie naar proceseigenaren		A/R		C		
VERRICHTEN						
Implementeren van IB-maatregelen		A/R		C		
Registratie, coördinatie, oplossen en evalueren van beveiligingsincidenten			A	I	R	
Verzorgen communicatie naar eindgebruikers		A/R		C		
Dataclassifcatie		A/R		C		
Uitvoeren risicoanalyse [en Privacy Impact Assessments]		A/R		S		

Legenda:

R = Responsible: Verantwoordelijk voor het (doen) uitvoeren van de processtap. Verantwoording wordt afgelegd aan degene die Accountable is. Deze rollen kunnen in voorkomende gevallen bij één persoon liggen waarbij eigenlijk verantwoording wordt afgelegd aan het CvB.

A = Accountable: Bevoegd om een beslissing te nemen over de processtap.

C = Consulted: Deskundig voor het geven van advies, verplicht te consulteren.

I = Informed: Partij die over de processtap verplicht dient te worden geïnformeerd.

6.3. Documenten informatiebeveiliging

In het kader van informatiebeveiliging hanteert Avans de volgende documenten:

1. Informatiebeveiligingsbeleid (dit document)
Het Informatiebeveiligingsbeleid ligt ten grondslag aan de aanpak van informatiebeveiliging. In het Informatiebeveiligingsbeleid worden de randvoorwaarden en uitgangspunten vastgelegd en wordt richting gegeven aan de vertaling van het beleid in concrete maatregelen.

2. Baseline van informatiebeveiligingsmaatregelen
Deze baseline beschrijft de maatregelen die minimaal nodig zijn om Avans breed een minimaal niveau van informatiebeveiliging te kunnen waarborgen en is gebaseerd op de Baseline Informatiebeveiliging HO en het Normenkader HO (Zie hoofdstuk 1.2). De baseline wordt gemaakt door de functionele en technische beheerder en privacy contactpersonen in overleg met het Team Integrale Veiligheid en goedgekeurd door de CISO. Wanneer er systemen zijn die na een risicoanalyse hogere beveiligingseisen nodig hebben, dan worden aanvullende maatregelen genomen.

3. Informatiebeveiligingsplan
Het beleid wordt door middel van een jaarlijks informatiebeveiligingsplan geoperationaliseerd. Hierbij wordt een GAP-analyse uitgevoerd tussen de huidige situatie en de Baseline van informatiebeveiligingsmaatregelen. In het informatiebeveiligingsplan wordt beschreven welke maatregelen geïmplementeerd moeten worden maar ook welke maatregelen niet geïmplementeerd worden en waarom. Jaarlijks toetsen wij waar we staan ten opzichte van deze maatregelen en actualiseren op basis daarvan het Informatiebeveiligingsplan.

Het plan is mede gebaseerd op de resultaten van de periodieke controles/ audits. Er wordt o.a. ingegaan op incidenten, resultaten van risicoanalyses (incl. genomen maatregelen) en andere initiatieven die het afgelopen jaar hebben plaatsgevonden. Waar nodig wordt apart aandacht besteed aan specifieke systemen/applicaties.

4. Policies
Gedragscodes en richtlijnen voor medewerkers, studenten en derden, al dan niet voor specifieke doelgroepen, op het gebied van informatiebeveiliging. Met name:

- Avans protocol voorzieningen en huisregels
- Richtlijn melden security incidenten
- Richtlijn Authenticatie en Autorisatie
- Richtlijn classificatie
- IT Lifecycle management

5. Diensten overeenkomsten (SLA's), inhuur- en uitbestedingscontracten
Het informatiebeveiligingsbeleid is van toepassing op de de inhuur van personeel, maar ook bij de inkoop van middelen (met name hardware, software en applicatie/cloud platforms). Afspraken met betrekking tot verantwoordelijkheden worden in een contract met de leverancier vastgelegd. Als basis hiervoor dient het SURF Juridisch Normenkader Cloudservices Hoger Onderwijs[12].

Daarnaast is informatiebeveiliging is een vast onderdeel van het Business Continuity Management plan. Business Continuity Management (BCM) is de benaming van het proces dat potentiële bedreigingen voor een instelling identificeert en bepaalt wat de impact op de 'operatie' van de instelling is als deze bedreigingen daadwerkelijk manifest worden. Het product van BCM bestaat uit een samenhangend stelsel van maatregelen, die zowel preventief, detectief, correctief als repressief werkzaam zijn. Disaster Recovery is derhalve onderdeel van BCM.

[12] https://www.surf.nl/binaries/content/assets/surf/nl/kennisbank/2013/juridisch<normenkader<cloudservices<hoger<onderwijs.pdf

6.4. Financiering

De financiering van informatiebeveiliging wordt bij Avans geregeld conform hieronder beschreven.

Algemene zaken, zoals het opstellen van een informatiebeveiligingsplan of een externe audit, worden uit de algemene middelen betaald (DIF). Algemene Avans brede bewustwordingscampagnes en trainingen worden eveneens uit deze middelen betaald (DIF).

De beveiliging van informatiesystemen (inclusief baseline ICT-infrastructuur), inclusief de kosten daarvan, zijn integraal onderdeel van verantwoord beheer van het betreffende informatiesysteem en valt onder de verantwoordelijkheid het desbetreffende bedrijfsonderdeel dat eigenaar is van het systeem. Beveiligingskosten van werkplekken maken integraal onderdeel uit van de werkplekkosten. Voorlichting en training voor specifieke toepassingen of doelgroepen worden uit decentrale middelen betaald.

Reserveren van beveiligingsbudget bij het maken van jaarplannen essentieel is. Hier dient extra aandacht aan worden te geven in het kader IB/ Avg.

6.5. Controle, naleving en sancties

Bij Avans is het Team Integrale Veiligheid verantwoordelijk voor de interne audits en voor de controle op de uitvoering. Interne controles vinden jaarlijks plaats en hebben bij voorkeur een divers karakter (brainstorm, steekproeven, penetratietest, testen van policies, informatiebeveiliging/CSIRT ‘brandoefening’, Ozon oefening).

De ICT inrichting van Avans Hogeschool wordt intern (Team Integrale Veiligheid) en extern (ICT leveranciers en Loydds Register Quality Assurance (LRQA ISO 9001:2015 certificering)) geaudited. Deze audits richten zich op de classificatie van de in het informatiesysteem vastgelegde gegevens, op de inventarisatie van de risico’s, op de genomen beveiligingsmaatregelen en op de samenhang tussen deze drie onderwerpen. Indien een informatiesysteem wordt vervangen of indien zich significante wijzigingen voordoen in de implementatie van de beveiliging wordt een interne audit uitgevoerd.

Het Normenkader Informatiebeveiliging HO (zie hoofdstuk 1.3) wordt gebruikt als uitgangspunt voor interne en externe controles. Voor de audits van specifieke onderdelen of informatiesystemen kunnen aanvullende, meer gedetailleerde, normen worden vastgesteld. De bevindingen van de interne en externe controles, evenals mogelijke externe eisen t.a.v. beveiliging, zijn input voor de nieuwe jaarplannen van Avans Hogeschool.

De naleving bestaat uit concreet toezicht op de dagelijkse praktijk van het informatiebeveiligings-managementproces. Van belang hierbij is dat leidinggevenden (inclusief onderwijsverantwoordelijken) de medewerkers en studenten aanspreken in geval van tekortkomingen. Voor de bevordering van de naleving van de Avg is de “Functionaris Gegevensbescherming” (FG) verantwoordelijk.

Mocht de naleving ernstig tekortschieten, dan kan Avans de betrokken verantwoordelijke medewerkers of studenten een sanctie opleggen, binnen de kaders van arbeids- en studieovereenkomsten en de wettelijke mogelijkheden. Dit is primair een verantwoordelijkheid van de verantwoordelijke leidinggevenden en het bestuur.

6.6. Bewustwording en training

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van informatiebeveiliging uit te sluiten. De mens zelf creëert de grootste risico's. Daarom wordt het bewustzijn voortdurend aangescherpt, zodat kennis van risico's wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd. Avans voert regelmatig terugkerende bewustwordingscampagnes voor medewerkers, studenten en derden. Voor privacy contactpersonen en operationele beheerders worden specifieke securitytrainingen georganiseerd.

Verhoging van het beveiligingsbewustzijn is een verantwoordelijkheid van het CvB, de leidinggevenden, het Team Integrale Veiligheid en de privacy contactpersonen. Dit alles laat onverlet dat elke beveiliging faalt als deze niet gedragen wordt door de medewerkers – elke Avans medewerker en student is medeverantwoordelijk voor beveiliging van informatie. Dit is een cruciaal onderdeel van bewustwording.

6.7. Overleg

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

Op **strategisch** niveau wordt richtinggevend gesproken over *governance* en *compliance*, alsmede over doelen, scope en ambitie op het gebied van informatiebeveiliging. Dit gebeurt door de CISO, gemandateerd door CvB.

Op **tactisch** niveau wordt de strategie vertaald naar plannen, te hanteren normen, evaluatiemethoden, e.d. Deze plannen en instrumenten zijn sturend voor de uitvoering. Dit tactisch overleg wordt uitgevoerd door het Team Integrale Veiligheid in overleg met betrokken functionarissen zoals de CSIRT-coördinator, privacy contactpersonen en proceseigenaren.

Op **operationeel** niveau worden de zaken besproken die het dagelijkse bedrijfsproces aangaan in de zin van uitvoering en implementatie.

Voor alle drie de typen overleg geldt dat het zoveel mogelijk ingepast moet worden in bestaande overlegvormen met hetzelfde karakter. Zo zal op strategisch niveau niet alleen over informatiebeveiliging gesproken worden, maar ook over andere risico's waarmee Avans te maken kan krijgen, zoals bijvoorbeeld financieel, personeel en commercieel.

DEEL 2: ARCHITECTUUR EN BEHEERSMAATREGELEN

Risicoanalyse, doel en uitgangspunten

7 Informatiebeveiligingsbeleid is van iedereen

Het informatiebeveiligingsbeleid gaat eenieder aan. Hierbij is bijzondere rol weggelegd voor onze medewerkers die het beleid vertalen naar operatie en te maken krijgen met alledaagse vraagstukken. Mede daarom is deze notitie opgebouwd uit twee delen. Dit deel heeft als doel om te komen tot beter uitvoerbaar beleid; Hier wordt meer in detail ingegaan op een aantal belangrijke thema's in termen van risico, doel en uitgangspunten om zodoende een kader te schetsen voor functioneel beheerders, ICT-contactpersonen, privacy officers en alle andere medewerkers die direct of indirect een bijdrage leveren in de verdere uitwerking in jaarplannen, het beantwoorden van alledaagse vragen en bewustwording processen.

8 Bedrijfsmiddelen

Informatie mag niet worden blootgesteld aan risico's, maar hierbij geldt dat het risico in balans moet staan tot de werkbaarheid van de genomen maatregelen en de kosten hiervan. Duidelijk moet voor alle ICT-configuratie items vastgelegd zijn wie de eigenaar/hoofdgebruiker is. Daarnaast moet duidelijk zijn wie verantwoordelijk is voor gegevensbestanden, waardoor ook iemand verantwoordelijk is voor beveiliging en voor het handhaven van de beheersmaatregelen.

Risico's:
- Bedrijfsmiddelen die verband houden met ICT-voorzieningen en informatie zijn blootgesteld aan risico's zoals diefstal, beschadiging of onoordeelkundig gebruik, waarbij niet voor alle ICT- configuratie items is vastgelegd wie de eigenaar/hoofdgebruiker is.
- Onduidelijkheid wie verantwoordelijk is voor gegevensbestanden, waardoor ook niemand verantwoordelijk is voor de beveiliging en kan optreden bij incidenten.

Doelstellingen:
- Bereiken en handhaven van een adequate bescherming van bedrijfsmiddelen die verband houden met ICT-voorzieningen van de organisatie.
- Voor alle bedrijfsmiddelen die verband houden met ICT-voorzieningen is de eigenaar vastgelegd alsook de verantwoordelijke voor het handhaven van de beheersmaatregelen.

Uitgangspunten:
- Alle bedrijfsmiddelen, die verband houden met ICT-voorzieningen worden aan een 'eigenaar' toegewezen.
- Documenteren implementeren voor aanvaardbaar gebruik van informatie en bedrijfsmiddelen die verband houden met ICT-voorzieningen.
- Medewerkers gebruiken informatie primair voor het uitvoeren van de aan hen opgedragen taken en het doel waarvoor de informatie is verstrekt.
- Privégebruik van informatie en bestanden is niet toegestaan.
- Voor het werken op afstand (plaats- en tijdonafhankelijk werken) en het gebruik van privémiddelen worden nadere beleidsregels opgesteld (beleid mobiele devices).
- De medewerker neemt passende technische en organisatorische maatregelen om informatie te beveiligen tegen verlies of tegen enige vorm van onrechtmatig gebruik.

9 Beveiligingsmaatregelen ten aanzien van personeel

Avans neemt regelmatig nieuw personeel in dienst, zowel op vaste basis als via tijdelijke inhuur. Het aannemen of inhuren van nieuw personeel en het laten verrichten van werkzaamheden door externe medewerkers verdient extra aandacht, omdat menselijk falen en bedreigingen van menselijke aard significante invloed kunnen hebben op de beschikbaarheid, integriteit en vertrouwelijkheid van informatie. De groepen medewerkers die vanuit het oogpunt informatiebeveiliging onderscheid zijn:

- Interne medewerkers. Dit zijn medewerkers die in tijdelijke of vaste dienst zijn bij Avans.
- Externe medewerkers en derden. Deze medewerkers zijn niet in dienst van de Avans.
- Werkstudenten. Studenten die in opdracht van Avans voor Avans werkzaamheden verrichten en daarvoor bijzondere rechten – lees medewerker rechten – nodig hebben.

Risico's:

- Het aannemen of inhuren van nieuw personeel en het laten verrichten van werkzaamheden door externe medewerkers of werkstudenten verdient extra aandacht, omdat menselijk falen en bedreigingen van menselijke aard significante invloed kunnen hebben op de beschikbaarheid, integriteit en vertrouwelijkheid van informatie.

Doelstellingen:

- Bewerkstelligen dat werknemers, ingehuurd personeel en externe gebruikers hun verantwoordelijkheden begrijpen, en geschikt zijn voor de rollen waarvoor zij worden ingezet en dat het risico van diefstal, fraude of misbruik van faciliteiten wordt beperkt.
- De verantwoordelijkheden ten aanzien van beveiliging is vastgelegd in passende functiebeschrijvingen en in de arbeidsvoorwaarden.
- Medewerkers van Avans zijn verplicht tot geheimhouding[13]. Deze geheimhouding dient echter ook te gelden voor externe gebruikers die toegang hebben. Voor externe gebruikers, al dan niet in dienst bij derden, wordt dit contractueel geregeld.
- Werknemers, ingehuurd personeel en externe gebruikers, die ICT-voorzieningen gebruiken tekenen een overeenkomst over hun beveiligingsrollen en –verantwoordelijkheden.

Uitgangspunten:

- Bij beëindiging van het dienstverband en inhuur worden alle bedrijfsmiddelen van de organisatie geretourneerd.
- Externe medewerkers die toegang krijgen tot informatie moeten bekend zijn bij Avans. Hun gegevens worden geregistreerd zodat de controleerbaarheid van hun in- en uitstroom op onze technische infrastructuur gewaarborgd is. Zij dienen te voldoen aan de door ons gestelde beveiligingseisen.
- Verandering van verantwoordelijkheden en dienstverband binnen Avans wordt voor wat betreft autorisaties behandeld als zijnde beëindiging gevolgd door een nieuw dienstverband. Dit is geborgd in procedures en onderdeel van instroom-doorstroom-uitstroom.
- Regels die volgen uit dit beleid gelden ook voor externen
- Alle medewerkers (en voor zover van toepassing externe gebruikers van onze systemen) dienen training te krijgen in procedures die gelden voor informatiebeveiliging. Deze training dient regelmatig te worden herhaald om het beveiligingsbewustzijn op peil te houden. In werkoverleggen wordt periodiek aandacht geschonken aan informatieveiligheid. Voor zover relevant worden hierover afspraken vastgelegd. Team Integrale Veiligheid neemt dit mee in awareness training en voorlichting (zie hoofdstuk 6.4).

[13] Avans heeft via de cao art. E-2 al haar medewerkers verplicht tot geheimhouding van hetgeen hem uit hoofde van zijn functie ter kennis komt.

10 Fysieke beveiliging en beveiliging van de omgeving

Een fysieke beveiliging van voldoende niveau draagt bij aan algehele informatieveiligheid. Wanneer dit onvoldoende is geregeld kunnen onbevoegden toegang krijgen tot vertrouwelijke informatie van Avans.

Risico's:

- Onbevoegde toegang tot kritieke systemen of waardevolle informatie. Bij het ontbreken van registratie zijn incidenten bovendien niet herleidbaar tot individuen.
- Door bijvoorbeeld de inzet van externen, de toeloop van leveranciers en andere niet- medewerkers of het feit dat de medewerkers op meerdere locaties op geruime afstand van elkaar gevestigd zijn, is het betrekkelijk eenvoudig voor niet-medewerkers om toegang tot de panden te krijgen door tegelijk met een geautoriseerde medewerker naar binnen te gaan.
- Als informatie zichtbaar op bureaus ligt, is er een verhoogd risico m.b.t. de vertrouwelijkheid.
- Geen procedures voor het veilig verwijderen of hergebruiken van ICT-apparatuur.
- Bescherming van apparatuur, waaronder apparatuur die buiten de locatie wordt gebruikt en het verwijderen van bedrijfseigendommen, is noodzakelijk om het risico van toegang door onbevoegden tot informatie te verminderen en om de apparatuur en informatie te beschermen tegen verlies of schade.

Doelstellingen:

- Het voorkomen van onbevoegde fysieke toegang tot, schade aan of verstoring van informatie van de organisatie, bedrijfsmiddelen en onderbreking van de bedrijfsactiviteiten.
- ICT-voorzieningen, die kritieke of gevoelige bedrijfsactiviteiten ondersteunen, behoren fysiek te worden ondergebracht in beveiligde ruimten, beschermd door afgegrensde beveiligde gebieden, in een gecontroleerde omgeving, beveiligd met geschikte beveiligingsbarrières en toegangsbeveiliging. Ze behoren fysiek te worden beschermd tegen toegang door onbevoegden, schade en storingen.
- Het voorkomen van verlies, schade of diefstal van apparatuur en bescherming tegen fysieke bedreigingen en gevaren van buitenaf.
- Clean Desk moet als onderdeel van awareness trainingen worden meegenomen.

Uitgangspunten:

- De schade door bedreigingen van buitenaf (zoals brand, overstroming, explosies, oproer, stroomonderbreking) wordt beperkt door passende preventieve maatregelen.
- Toegang tot niet-openbare gedeelten van gebouwen of beveiligingszones is alleen mogelijk na autorisatie daartoe.
- De uitgifte van toegangsmiddelen wordt geregistreerd.
- De kwaliteit van toegangsmiddelen (deuren, sleutels, sloten, toegangspassen) is afgestemd op de zonering (en het risicoprofiel).
- De fysieke toegang tot ruimten waar zich informatie en ICT-voorzieningen bevinden is voorbehouden aan bevoegd personeel. Registratie van de verleende toegang ondersteunt de uitvoering van de toegangsregeling.
- Serverruimtes, datacenters en daaraan gekoppelde bekabelingsystemen zijn ingericht in lijn met geldende 'best practices'.
- (Data)verbindingen worden beschermd tegen interceptie of beschadiging.
- Reserveapparatuur en back-ups zijn gescheiden in twee locaties of datacenters, om de gevolgen van een calamiteit te minimaliseren. Jaarlijks wordt getest op een uitwijkscenario en back-up/restore.
- Gegevens en programmatuur worden van apparatuur verwijderd of veilig overschreven, voordat de apparatuur wordt afgevoerd. Informatie wordt bewaard en vernietigd conform de Archiefwet 1995 en de daaruit voortvloeiende archiefbesluiten.

11 Apparatuur en ICT-voorzieningen

Het (technisch) beveiligen van apparatuur/informatie is een van de meest voor de hand liggende vormen van informatiebeveiliging.

Risico's:

- Het ontbreken van documentatie kan leiden tot fouten, niet-uniforme wijze van gegevensinvoer, of in geval de beheerder/bediener uitvalt, tot problemen rondom de continuïteit.
- Onjuiste autorisaties kunnen leiden tot foutieve handelingen, fraude en verduistering.
- Het niet uitvoeren en vastleggen van technische en functionele applicatietesten en/of de resultaten hiervan, kan in bepaalde omstandigheden (tijdsdruk, vakantieperiodes, etc.) leiden tot een verhoogd risico van uitval of gegevens verlies.
- Avans gaat steeds meer samenwerken (en informatie uitwisselen) in ketens en met het werkveld en besteedt meer taken uit. Bij beheer van systemen en gegevens door een derde partij, kan ook informatie van Avans op straat komen te liggen. Avans blijft echter ook verantwoordelijk voor de informatiebeveiliging van haar gegevens in dat deel van de keten, waarbij het beheer bij een andere partij ligt.
- Programmatuur en ICT-voorzieningen zijn kwetsbaar voor virussen en malware.
- Het ontbreken van een regeling voor antivirus bescherming bij medewerkers thuis (of bij inzet van Bring-your-own-device – BYOD) leidt tot hogere beveiligingsrisico's.

Doelstellingen:

- Waarborgen van een correcte en veilige bediening van ICT-voorzieningen.
- Vastgestelde verantwoordelijkheden en procedures voor beheer en bediening van alle ICT-voorzieningen. Dit omvat tevens de ontwikkeling van geschikte bedieningsinstructies.
- Toepassing, waar nodig, van functiescheiding om het risico van nalatigheid of opzettelijk misbruik te verminderen.
- Waarborgen van veiligheidsstandaarden externe partners

Uitgangspunten:

Beheeraspecten

- In beginsel mag niemand autorisaties hebben om een gehele cyclus van handelingen in een informatiesysteem te beheersen, zodanig dat beschikbaarheid, integriteit of vertrouwelijkheid kan worden gecompromitteerd. Functiescheiding dient te worden toegepast bij het ontwerp van de autorisatie van systemen. De verantwoordelijkheid hiervoor ligt bij de informatie-eigenaar. Indien dit toch noodzakelijk is, dient een audit-trail te worden vastgelegd van alle handelingen en tijdstippen in het proces, dusdanig dat transactie kan worden herleid. De audit-trail is niet toegankelijk voor degene wiens handelingen worden vastgelegd.
- Er is een scheiding tussen beheertaken en overige gebruikstaken.
- Bij externe hosting van data en/of services (uitbesteding, cloud computing) blijft Avans eindverantwoordelijk voor de betrouwbaarheid van uitbestede diensten. Dit is gebonden aan regels en vereist goede (contractuele) afspraken en controle hierop. Externe hosting van data en/of services is in overeenstemming met Informatiebeveiligingsbeleid.
- Systemen voor test en/of acceptatie zijn logisch gescheiden van productiesystemen.
- Nieuwe systemen, upgrades en nieuwe versies worden getest op impact en gevolgen en pas geïmplementeerd na formele acceptatie en goedkeuring door de opdrachtgever. De test en de testresultaten worden gedocumenteerd.

Technische aspecten

- Het netwerk wordt gemonitord en beheerd zodat aanvallen, storingen of fouten ontdekt en hersteld kunnen worden en de betrouwbaarheid van het netwerk niet onder het afgesproken minimumniveau (servicelevels) komt.
- Op verschillende niveaus binnen de ICT-infrastructuur (netwerkcomponenten, servers, pc's) wordt antivirussoftware van verschillende leveranciers toegepast. Bij het openen of wegschrijven van bestanden worden deze geautomatiseerd gecontroleerd op virussen, trojans en andere malware. Ook inkomende en uitgaande e-mails worden hierop gecontroleerd. De update voor de detectiedefinities vindt in beginsel dagelijks plaats.
- Versleuteling vindt plaats conform 'best practices' (de stand der techniek), waarbij geldt dat de vereiste encryptie sterker is naarmate gegevens gevoeliger zijn.
- Alle apparatuur die is verbonden met het netwerk van Avans moet kunnen worden geïdentificeerd.

Softwareontwikkeling en -onderhoud

- Applicaties worden getest o.b.v. landelijke richtlijnen voor beveiliging, zoals richtlijnen voor beveiliging van webapplicaties.
- Webapplicaties worden voordat zij in productie worden genomen onder meer getest op veiligheid.
- Wanneer er persoonsgegevens of andere privacygevoelige informatie in een webapplicatie worden verwerkt moet er gebruik worden gemaakt van een veilige *https-verbinding*.
- Alleen gegevens die noodzakelijk zijn voor de gebruiker worden uitgevoerd (doelbinding), rekening houdend met beveiligingseisen (classificatie).
- Toegang tot de broncode is beperkt tot de medewerkers, die deze code onderhouden of installeren.
- Technische kwetsbaarheden worden regulier minimaal 4 keer per jaar gerepareerd door 'patchen' van software of direct bij acute dreiging conform de geldende change procedure.

Mobiele (privé-)apparatuur

- Beveiligingsmaatregelen hebben betrekking op zowel door Avans verstrekte middelen als privé-apparatuur waarmee informatie van Avans wordt verwerkt.
- Op privé-apparatuur waarmee verbinding wordt gemaakt met het Avans netwerk is Avans bevoegd om beveiligingsinstellingen af te dwingen.
- Op verzoek van Avans dienen medewerkers de installatie van software om bovenstaande beleidsregel te handhaven toe te staan. De beveiligingsinstellingen, zoals bedoeld in bovenstaande regel, zijn uitsluitend bedoeld ter bescherming van informatie en integriteit van het netwerk.
- In geval van dringende redenen kunnen noodmaatregelen worden getroffen, zoals wissen van apparatuur op afstand. Deze noodmaatregelen kunnen, voor zover dit noodzakelijk is, betrekking hebben op privémiddelen en privébestanden. Uitgangpunt hierbij is dat Avans enkel en alleen toegang heeft tot informatie van Avans en dat ook alleen die informatie gewist kan worden.

Back-up en recovery

- ICT maakt reservekopieën van alle essentiële bedrijfsgegevens en programmatuur zodat de continuïteit van de gegevensverwerking kan worden gegarandeerd.
- De omvang en frequentie van de back-ups is in overeenstemming met het belang van de data voor de continuïteit van de dienstverlening en de interne bedrijfsvoering.
- De back-up en herstelprocedures worden regelmatig (tenminste 1 x per jaar) getest om de betrouwbaarheid ervan vast te stellen.

Informatie-uitwisseling

- Er is een (spam) filter geactiveerd voor inkomende e-mail berichten.
- Er zijn procedures voor het beheer van verwijderbare media en voor het veilig verwijderen of hergebruiken van ICT-apparatuur.
- Er is innamebeleid voor mobiele apparatuur zoals laptops, telefoons en tablets.
- Bij het plaats- tijdonafhankelijk werken wordt gebruik gemaakt van een veilige verbinding en zero footprint.

Logging en controle

- Beheerders en gebruikers kunnen worden gelogd om problemen te kunnen oplossen of oneigenlijk gebruik te kunnen detecteren. In een log-regel worden alleen de voor de rapportage noodzakelijke gegevens opgeslagen. Er worden maatregelen getroffen om te verzekeren dat gegevens over logging beschikbaar blijven en niet gewijzigd kunnen worden. De bewaartermijnen zijn in overeenstemming met wettelijke eisen.

Classificatie van informatie

- Te hoge classificatie leidt tot onnodige kosten en moet worden voorkomen door . Bovendien dient informatie in beginsel voor zoveel mogelijk mensen beschikbaar te zijn (transparante overheid).
- Er wordt gestreefd naar een balans tussen het te lopen risico en de werkbaarheid en kosten van tegenmaatregelen.
- Maat daarnaast verdient een technische oplossing altijd de voorkeur boven gedragsverandering.

Dienstverlening externe partij

- Avans blijft verantwoordelijk voor de informatiebeveiliging van haar gegevens in dat deel van de keten, waarbij het beheer bij een andere partij ligt.
- In de basis-SLA voor dienstverlening is aandacht besteed aan informatiebeveiliging.
- De beveiligingsmaatregelen, definities van dienstverlening en niveaus van dienstverlening zoals vastgelegd in de (bewerkers)overeenkomst voor dienstverlening door een derde partij worden geïmplementeerd en uitgevoerd.
- De diensten, rapporten en registraties, die door de derde partij worden geleverd, worden gecontroleerd en beoordeeld en er wordt door het Team Integrale Veiligheid toegezien op juiste gebruik van de informatie.
- Indien bij samenwerking met derden sprake is van uitwisseling van informatie, waarvan Avans eigenaar of beheerder is, dient informatiebeveiliging een onderdeel te zijn de samenwerkingsovereenkomst en mag deze niet strijdig zijn met het informatiebeveiligingsbeleid.

12 Logische toegangsbeveiliging

Logische toegangsbeveiliging betekent dat de identiteit van een gebruiker die toegang krijgt tot informatie dient te worden vastgesteld. Logische toegang is gebaseerd op de classificatie van de informatie.

Risico's:

- Wanneer toegangsbeheersing niet expliciet is onderbouwd door middel van een aanvullende risicoanalyse, is niet duidelijk of het juiste niveau van beveiliging wordt gehanteerd.
- Verstoringen door onjuist gebruik van ICT-ruimtes of ICT-componenten (m.n. waar ook niet ICT-teams toegang hebben).

Doelstellingen

- Beheersen van de toegang tot informatie, ICT-voorzieningen en bedrijfsprocessen op grond van bedrijfsbehoeften en beveiligingseisen.
- Beleid ten aanzien van informatieverspreiding en autorisatie is van toepassing.

Uitgangspunten:

Authenticatie en autorisatie

- Wachtwoorden voor medewerkers worden voor een beperkte periode toegekend. Wachtwoorden dienen aan eisen te voldoen[14], deze worden afgedwongen door het systeem. Voor medewerkers met speciale bevoegdheden (systeem en functioneel beheerders) gelden strengere eisen.
- De gebruiker is verantwoordelijk voor het geheim blijven van zijn wachtwoord.
- Authenticatiemiddelen zoals wachtwoorden worden beschermd tegen inzage en wijziging door onbevoegden tijdens transport en opslag (door middel van encryptie).
- Autorisatie is rol-gebaseerd. Autorisaties worden toegekend aan de hand van functie(s) en organisatieonderdelen.
- Toegang tot informatie met classificaties 'midden' of 'hoog' vereist in de regel multifactor authenticatie (bijv. naam/wachtwoord (1) + token (2)). Hierbij hanteren we als uitgangspunt dat wij de balans zoeken tussen veiligheid, werkbaarheid en betaalbaarheid.
- Beheerders hebben naast een regulier account zonder administrator rechten ook een persoonlijk administrator account voor beheertaken. In de operatie worden beheerwerkzaamheden en werkzaamheden als gewone gebruiker onder twee verschillende gebruikersnamen uitgevoerd.
- Het gebruik van algemene beheeraccounts (root, administrator) is uitgeschakeld. Als gebruik onvermijdelijk is moet herleidbaarheid, doelbinding en onweerlegbare logging gecombineerd toegepast worden.
- Identiteitsinformatie is actueel en wordt periodiek gecontroleerd. De frequentie is afhankelijk van de classificatie.

Externe toegang derden

- Avans kan een externe partij toegang verlenen tot het netwerk en daarmee tot informatie. Hiervoor dient een procedure gemaakt en gevolgd te worden. Externe partijen kunnen niet op eigen initiatief verbinding maken met het netwerk van Avans, tenzij uitdrukkelijk overeengekomen.

Plaats- en tijdonafhankelijk werken

Voor plaats- en tijdonafhankelijk werken gelden de volgende uitgangspunten:

- Toegang tot de werkomgeving, wanneer er van buiten het Avans netwerk wordt ingelogd, wordt verleend op basis van multifactor authenticatie.
- Mobiele bedrijfsapplicaties worden bij voorkeur zo aangeboden dat er geen informatie wordt opgeslagen op het mobiele apparaat ('zero footprint'). Informatie dient te worden versleuteld bij transport en opslag conform classificatie eisen.

[14] Het wachtwoordbeleid is uitgewerkt in het wachtwoord beleidsdocument van Avans.

Encryptie (versleuteling)

- Intern dataverkeer (‘machine to machine’) wordt indien noodzakelijk conform classificatie beveiligd met certificaten.
- Beveiligingscertificaten worden door ICT centraal beheerd.

Organisatorische aspecten

- Project en inkoop worden voorzien van een advies op informatiebeveiliging en voorzien van een (D)PIA (Zie hoofdstuk Avg). Dit advies kan door het Team Integrale Veiligheid op aanvraag worden afgegeven.

Overige maatregelen

- Het fysieke (bekabelde) netwerk is niet toegankelijk voor ongeautoriseerde apparatuur.
- De netwerkschijven zijn gesegmenteerd en alleen toegankelijk voor geautoriseerde gebruikers.

13 Informatiebeveiligingsincidenten

Het is van belang om te leren van incidenten. Incidentregistratie en periodieke rapportage over opgetreden incidenten horen thuis in een volwassen informatiebeveiligingsomgeving. Elke medewerker, student en derde is zelf verantwoordelijk voor het signaleren en melden van incidenten en inbreuken op informatiebeveiliging. Incidenten en inbreuken dienen direct gemeld te worden bij de Servicelijn van Avans Hogeschool, welke dit direct doorgeeft aan het Computer Security Incident Response Team (CSIRT).

Risico's:

- Als incidenten niet geregistreerd worden, is niet duidelijk waar en wanneer er zich incidenten voor doen of voor hebben gedaan. Op deze wijze kan er geen lering worden getrokken uit deze incidenten om deze in de toekomst te voorkomen of om preventief betere maatregelen te implementeren.

Doelstellingen:

- Bewerkstelligen dat informatiebeveiligingsgebeurtenissen en zwakheden, die verband houden met informatiesystemen zodanig kenbaar worden gemaakt dat tijdig corrigerende maatregelen kunnen worden genomen.
- Formele procedures voor rapportage van gebeurtenissen en escalatie. Alle werknemers, ingehuurd personeel en externe gebruikers zijn op de hoogte van deze procedures voor het rapporteren van de verschillende soorten gebeurtenissen en zwakke plekken die invloed kunnen hebben op de beveiliging van de bedrijfsmiddelen.
- Er is een verplichte meldingssystematiek in werking om alle informatiebeveiligingsgebeurtenissen en zwakke plekken zo snel mogelijk te rapporteren aan de aangewezen privacy contactpersoon en ICT Servicelijn tel nr. 8888.

Uitgangspunten:

- De medewerker dient geconstateerde of vermoede beveiligingslekken en beveiligingsincidenten direct te melden bij ICT-servicelijn. Deze afdeling registreert het incident in stelt indien nodig het Team Integrale Veiligheid op de hoogte van het incident.
- Melding, registratie en monitoring van het incident vindt plaats via het door de afdeling ICT gebruikte applicatiesoftwarepakket.
- De eerste beoordeling van het incident vindt plaatst door CSIRT (damage control). Na deze eerste beoordeling brengt CSIRT het Team Integrale Veiligheid op de hoogte van het incident. Voor afhandeling geldt de reguliere rapportage en escalatielijn (o.a. richting FG in geval van mogelijke overtreding Agv).
- Afhankelijk van de aard en ernst van een incident kan er sprake zijn van een meldplicht bij de Autoriteit Persoonsgegevens. Het Team Integrale Veiligheid meldt dit bij de FG.
- Beschrijvingen en evaluaties van beveiligingsincidenten worden opgenomen in de jaarrapportage van het Team Integrale Veiligheid.
- Bij grote incidenten wordt gehandeld en opgeschaald conform Business Continuity Management proces.

BIJLAGEN

Bijlage 1 Wet- en regelgeving

Bij Avans wordt op de volgende wijze omgegaan met relevante wet- en regelgeving op het gebied van Informatiebeveiliging:

Wet Bescherming Persoonsgegevens (Wbp) (Hierin is opgenomen meldplicht datalekken) en haar opvolger **Algemene Verordening Gegevensverwerking (Avg).** Avans heeft de wettelijke vereisten met betrekking tot beveiliging van persoonsgegevens ingebed in dit beleid. Handelen conform dit beleid leidt in beginsel tot voldoen aan de beveiligingsvereisten uit de wet.

Archiefwet
Avans Hogeschool houdt zich aan de voorschriften uit de Archiefwet, het Archiefbesluit en de Selectielijst van de Vereniging Hogescholen (uitgewerkt in de Selectielijst Avans Hogeschool) over de wijze waarop omgegaan moet worden met informatie vastgelegd in (gedigitaliseerde) documenten, informatiesystemen, websites, e.d.

Avans houdt zich aan de wettelijke voorschriften ten aanzien van bewaartermijnen. Dit betreft alle informatie zoals die bijvoorbeeld is vastgelegd in (gedigitaliseerde) documenten, informatiesystemen, websites, e-mail enzovoorts. Dit is onderdeel van de jaarlijkse externe accountantsrapportages.

Auteurswet
Avans respecteert auteursrechten en handelt daarnaar.

Telecommunicatiewet
Omdat de doelgroep van Avans voldoende afgebakend is worden de netwerkvoorzieningen van Avans niet aangemerkt als een openbaar netwerk in de zin van de Telecommunicatiewet.

Wet Computercriminaliteit / Wetboek van strafrecht
De Wet Computercriminaliteit richt zich op de strafrechtelijke probleemgebieden in relatie tot het computergebruik. De wet bestaat uit artikelen die op diverse plekken zijn toegevoegd aan het WvS. De extra artikelen houden zich bezig met:

- Vernieling en onbruikbaar maken
- Aftappen van gegevens
- *Denial of service,* verstikkingsaanval
- Computervredebreuk
- Wat is computercriminaliteit
- Diensten afnemen zonder betalen
- Malware, kwaadaardige software

Evenwel zorgen het naleven van dit informatiebeveiligingsbeleid en het implementeren van basismaatregelen ervoor dat Avans een basisniveau van beveiliging heeft. Indien er aanvallen op Avans plaatsvinden die die beveiliging significant doorbreken en die vallen onder de Wet Computercriminaliteit, zal Avans in beginsel aangifte doen. De CSIRT-coördinator en het Team Integrale Veiligheid adviseren hierover aan de CISO – alleen CISO kan het besluit tot aangifte nemen.

Governance: Omvat algemene privacy awareness binnen organisatie, intern beleid, beleggen van verantwoordelijkheden, transparantie naar betrokkenen, samenwerking met derde partijen en bewerkers (incl. contracten, bewerkersovereenkomsten)								
Onderdeel **Invulling**	**Anonimiseren** 	**1. Dataminimalisatie** (art. 5 lid 1 sub c) 	**2. Pseudonimiseren** (art. 4 lid 5)	**3. Encryptie** (art. 6 lid 4 sub e, art. 32 lid 1 sub a)	**4. Access control** (art. 32 lid 1, art. 5 lid 1 sub f)	**5. Data protection by default** (art. 25 lid 2)	**6. Verwijderen / bewaartermijnen** (art. 5 lid 1 sub e)	**7. Faciliteren rechten van betrokkenen** (artt. 12 t/m 22)
Techniek	Anonimiseren en aggregeren (bijv. differential privacy)	Alleen strikt noodzakelijke gegevens verzamelen of overbodig direct verwijderen, (web) invulformulieren aanpassen	Ontdoen van direct identificerende kenmerken, hashing, polymorfe pseudo-id	Bijvoorbeeld public key encryptie, disk encryptie	Digitale gegevenskluis, fysieke toegangscontrole, logische toegangscontrole, authenticatie en autorisatie	Privacyvriendelijke settings als uitgangspunt, transparante user-interface, permission management	Automatisch vernietigen, 'flaggen' data na verstrijken bewaartermijn, sticky policies, data fading	Privacy dashboard, communicatie / support (art. 5 lid 1 sub a)
Onderliggende documentatie	Geen extra maatregelen nodig, want geen persoons-gegevens	Doelomschrijving met opsomming noodzakelijke gegevens	Beleid voor gescheiden houden van identificerende gegevens en overige gegevens, contracten	Informatie-beveiliging standaarden (art. 32 lid 1)	Bijhouden autorisatiematrix en logging, op basis van *need to know* en *need to access*	Registraties opt-in en opt-out en van permissies	Beleid en overzicht bewaartermijnen, omgang met e-waste (oude documenten en devices)	Privacy statement, beleid bij verzoeken tot inzage/correctie/ verwijderen gegevens
Alternatief	Als je niet anonimiseert: het schema volgen	Waar mogelijk deel gegevensset anonimiseren/ aggregeren, data fading	Andere beveiligings-maatregelen	Andere beveiligings-maatregelen (bijv. stand-alone server)	Access logs met controle achteraf	Geen alternatief, gewoon doen, is verplicht	Anonimiseren en aggregeren, (archiveren indien wettelijk toegestaan)	Geen alternatief, wettelijke plicht
Privacy Audit								
Een privacy impact assessment kan de onderdelen toetsen en helpt inzichtelijk maken wat nodig is								

Bijlage 3 Beschermingsniveaus

Vertrouwelijkheid

In onderstaande tabel staan de belangrijkste, meer technische, maatregelen voor vertrouwelijkheid. De kolommen (niveaus) zijn cumulatief.

KENNISGEBIED	BEVEILIGINGSNIVEAU		
	LAAG	MIDDEN	HOOG
		Laag +	*Laag en midden +*
Identificatie	• Gebruikers zijn uniek herleidbaar • Gescheiden beheer- en gebruikersaccounts • Identiteitsinformatie is actueel en wordt jaarlijks geverifieerd	• Geen 'gedeelde functionele identiteiten' • Identiteiten worden 2 x per jaar geverifieerd	• Identiteiten worden 3 x per jaar geverifieerd
Authenticatie	• Op basis van informatie: naam/wachtwoord • Wachtwoorden versleuteld	• Authenticatie op basis van informatie en 'eigenaarschap' (2factor) vanuit onvertrouwde zone • Sessie time-out bij inactieve sessie	• Authenticatie op basis van 'eigenaarschap' (biometrie) optioneel • Geen SSO toegestaan • Absolute sessie time-out
Autorisatie	• Autorisatie op basis van lid van organisatie • Autorisatie wordt jaarlijks geverifieerd • Aanvragen door bevoegde aanvrager •	• Autorisatie op basis van vooraf gedefinieerde functionele rol (doelbinding, noodzakelijkheid) • Autorisaties worden vooraf geaccordeerd door eigenaar van de informatie	
Versleuteling	• Versleuteling tijdens transport buiten netwerk via transportbeveiliging of berichtbeveiliging • Lifecycle mngt van cryptosleutels is geborgd • Cryptosleutels worden beschermd	• Versleuteling webverkeer (in- en extern)	• Versleuteling bij opslag • Bescherming sleutels met gecertificeerde crypto hardware
Zonering	• Aparte zone voor niveau 'laag'	• Aparte zone voor niveau 'midden' • Geen lokale opslag van data	• Aparte zone voor niveau 'hoog' • Transport van gegevens minimaliseren
Filtering	• Filtering op verkeersstromen en content (malware, spyware, virus, etc.) m.b.t. inkomend verkeer vanuit externe/onvertrouwde zone	• Filtering op verkeerstromen van en naar andere zones	
Logging & Monitoring	• Logging tbv fouten, niet toegestane acties en werking van maatregelen • Actieve monitoring op 'reguliere' dreigingen	• Aanvullende logging traceerbaarheid op natuurlijk persoon • Actieve monitoring en alerting bij inbreuk op beveiliging • Bewaren conform wettelijke eisen en/of contractuele afspraken	

Integriteit

In onderstaande tabel staan de belangrijkste, meer technische, maatregelen voor integriteit. De maatregelen zijn in deel 2 verder uitgewerkt. De kolommen (niveaus) zijn cumulatief.

KENNISGEBIED	BEVEILIGINGSNIVEAU		
	LAAG	MIDDEN	HOOG
		Laag +	*Laag en midden +*
Autorisatie	• Zie tabel vertrouwelijkheid	• Geeft invulling aan de eisen van functiescheiding	• Geeft invulling aan de eisen van functiescheiding
Functiescheiding	• Procestaken zijn gescheiden • Beheer en gebruik zijn gescheiden	• Aparte goedkeuring taak bij verwerking • Procesontwerp aanwezig	•
Invoercontrole	• Invoercontrole op volledigheid en consistentie • Pre-fill van bekende gegevens	• Inzage en recht op wijzigen van gegevens door betrokkene • Ingevoerde gegevens worden bevestigd aan betrokkene • Kritische gegevenselementen worden verplicht ingevuld	
Uitvoercontrole	• Controle op overbodige informatie	• Uitvoer beperkt tot voor de functie noodzakelijke informatie • Afdrukken van gegevens via applicatietaak • Uitvoer voldoet aan wettelijke voorschriften	• Controle van de juistheid van de uitvoer
Systeemintegriteit	• Hardening vereist • Uitvoeren van toegestane 'mobile code' in geïsoleerde omgeving	• Persistant messaging vereist • Noodstop mechanisme • Generatievalidatie en herstelmechanisme	•
Onweerlegbaarheid	• Geen	• Elektronische handtekening vereist bij formele communicatie • Wederzijdse authenticatie vereist	• Gekwalificeerde elektronische handtekening vereist bij formele communicatie • Audittrail is onweerlegbaar
Logging & Monitoring	• Logging t.b.v. fouten, niet toegestane acties en werking van maatregelen • Actieve monitoring op 'reguliere' dreigingen	• Vastlegging relevante input en output validatie	• Vastleggen oude staat van te wijzigen gegevens

Beschikbaarheid

In onderstaande tabel staan de belangrijkste, meer technische, maatregelen voor beschikbaarheid. De maatregelen in deel 2 verder uitgewerkt. De kolommen (niveaus) zijn cumulatief.

KENNISGEBIED	BEVEILIGINGSNIVEAU		
	LAAG	MIDDEN	HOOG
		Laag +	*Laag en midden +*
Herstel van verwerking	• Back & restore • Handmatige failover (standby tweede datacenter) • Disaster recovery plan • Herstel tijdens werkdagen tijdens kantooruren	• Buffering van tussenbestanden bij langere ketens • Automatische failover en loadbalancing • Business continuity plan • Beperkt herstel tijdens kantoortijden	• Realtime fail-over en via load balancing op beide datacenters actief • Jaarlijks getest calamiteiten en business continuity plan • Herstel 24*7
Redundantie	• Geen	• Dubbele uitvoeringen voorzieningen • Zo mogelijk gescheiden locaties	• Applicaties zijn geschikt voor automatische failover • Geen Spof
Voorkomen van discontinuïteit	• Invoercontrole op volledigheid en consistentie • Pre-fill van bekende gegevens	• Controle op weerbaarheid via technisch onderzoek op het niveau van netwerken, protocollen en applicaties	
Systeemintegriteit	• Hardening vereist • Uitvoeren van toegestane 'mobile code' in geïsoleerde omgeving	• Persistant messaging	• Remote beheer niet toegestaan
Logging & Monitoring	• Logging t.b.v. fouten, niet toegestane acties en werking van maatregelen • Actieve monitoring op 'reguliere' dreigingen	• Loggen performance en resource gebruik • Trending uitvoeren op logging	• Verantwoording voor alle error logs