UNIVERSITEIT VAN AMSTERDAM

INFORMATIEBEVEILIGINGSBELEID

Vastgesteld bij besluit nr. 2018-068316 van het College van Bestuur van 25 september 2018

Inhoudsopgave

1. Inleiding

De digitale verwerking van informatie is niet meer weg te denken anno nu. Bijna alle processen zijn afhankelijk van een goede en ongestoorde werking van IT. Dat geldt net zo zeer voor het primaire proces, alsook voor secundaire processen, en ondersteunende processen als financieel management of personeelszaken. Zonder werkende ICT geen onderzoek, geen onderwijs, geen facturering, geen uitbetaalde salarissen, geen werkende toegangscontrole, enzovoorts.

Informatiebeveiliging is een beleidsverantwoordelijkheid van het bestuur van de Universiteit van Amsterdam (hierna: de UvA). De toenemende afhankelijkheid van informatie en computersystemen brengt de kans op nieuwe kwetsbaarheden en risico's met zich mee. Het is daarom van belang adequate maatregelen te nemen. Immers, onvoldoende informatiebeveiliging kan leiden tot onacceptabele risico's bij de uitvoering van onderwijs en onderzoek en bij de bedrijfsvoering van de instelling. Incidenten en inbreuken in deze processen kunnen leiden tot financiële schades en imagoverlies.
Onder informatiebeveiliging wordt verstaan het treffen en onderhouden van een samenhangend pakket aan *maatregelen om de kwaliteitsaspecten beschikbaarheid, integriteit en vertrouwelijkheid*[1] *van de informatievoorziening*[2] te garanderen.

De kwaliteitsaspecten zijn:
- Beschikbaarheid: de mate waarin informatie of functionaliteit op de juiste plaats en tijd beschikbaar zijn voor gebruikers, kortom werken de middelen/processen, zijn ze "in de lucht"?
- Integriteit: de mate waarin informatie betrouwbaar is ofwel is de inhoud van de informatiestromen beveiligd, dat wil zeggen is het zeker dat er niet mee geknoeid is of kan worden?
- Vertrouwelijkheid: de mate waarin de toegang tot informatie of functionaliteit beperkt is tot degenen die daartoe bevoegd zijn.[3] Anders gezegd: Hebben alleen die mensen toegang tot bepaalde informatie die daartoe gemachtigd zijn, en is het voor anderen ontoegankelijk c.q. onleesbaar?

Een aanvullend aspect dat voor alle kwaliteitsaspecten van belang is, is controleerbaarheid: niet alleen "weten" of iets in orde is, maar dat ook achteraf kunnen "verifiëren".

De UvA heeft de ambitie om de informatiebeveiliging structureel naar een hoger niveau te brengen. Dit beleidsdocument legt hiervoor de basis door het vastleggen van de beleidsprincipes en de organisatie van de beveiligingsfunctie. Met de gelegde basis kan de organisatie permanent werken aan het verbeteren van de informatiebeveiliging.

2. Doelgroep

Het informatiebeveiligingsbeleid bij de UvA richt zich primair op bestuur en hoger management, de beveiligingsorganisatie en leidinggevenden. Het is van toepassing op alle medewerkers, docenten, studenten, bestuurders, gasten, bezoekers en externe relaties. Kortom, op iedereen die, intern dan wel extern, op enige manier te maken heeft met (aspecten van) het bedrijfsproces bij de UvA. ACTA maakt gebruik van de IT-voorzieningen van de VU en valt voor de verwerking van gegevens in het kader van de zorgfunctie onder het informatiebeveiligingsbeleid van de VU. De Faculteit Geneeskunde maakt gebruik van de ICT-voorzieningen van het AMC en valt daarvoor onder het informatiebeveiligingsbeleid van het AMC. Voor zover de faculteit gebruik maakt van UvA-

[1] Ook bekend als de BIV aspecten van informatie.
[2] De informatievoorziening van een organisatie is het geheel van mensen, middelen en maatregelen, gericht op de informatiebehoefte van die organisatie. Het informatiebeveiligingsbeleid is een samenspel van niet-digitale aspecten (fysieke beveiliging en personeelsbeleid) en digitale aspecten. Zie verder ook Reikwijdte.
[3] Uit: Overbeek, Roos Lindgreen, Spruit: Informatiebeveiliging onder controle, ISBN 90-430-0289-5

informatiesystemen, zoals Canvas en SIS, valt dat gebruik onder het informatiebeveiligingsbeleid van de UvA.

3. Reikwijdte

Bij de UvA wordt informatiebeveiliging breed geïnterpreteerd. Er is een belangrijke relatie en een gedeeltelijke overlap met aanpalende beleidsterreinen:

- **Privacy.** Informatiebeveiliging en privacy zijn nauw met elkaar verbonden. De UvA kent een apart privacy-beleid[4];
- **Safety.** ARBO- en milieuwetgeving;
- **Security (fysieke beveiliging).** Het betreft hier b.v. toegangsbeheer van ruimten;
- **Personeelsbeleid.** Bij informatiebeveiliging speelt de mens een cruciale rol. Er is dan ook een relatie met personeelsbeleid.

Op strategisch niveau wordt aandacht geschonken aan deze raakvlakken en wordt zowel planmatig als inhoudelijk afstemming gezocht. Samenwerking tussen de verschillende disciplines is een noodzakelijke voorwaarde om het niveau van informatiebeveiliging structureel te verhogen.

Het informatiebeveiligingsbeleid binnen de UvA heeft betrekking op alle medewerkers, studenten, gasten, bezoekers en externe relaties (inhuur / outsourcing), alsmede op alle organisatieonderdelen. Tevens vallen onder het informatiebeveiligingsbeleid alle apparaten waarmee geautoriseerde toegang tot het instellingsnetwerk verkregen kan worden.

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

4. Doel informatiebeveiligingsbeleid

Het informatiebeveiligingsbeleid bij de UvA heeft als doel het waarborgen van de continuïteit van de bedrijfsvoering[5] en het minimaliseren van de schade door het voorkomen van incidenten en het minimaliseren van eventuele gevolgen.

De afgeleide doelstellingen voor het informatiebeveiligingsbeleid voor de UvA zijn:

- **Het bieden van een kader:** het beleid biedt een kader om (toekomstige) maatregelen in de informatiebeveiliging te toetsen aan een vastgestelde best practice of norm en om de taken, bevoegdheden en verantwoordelijkheden in de organisatie te beleggen;
- **Het stellen van normen:** de basis voor de inrichting van informatiebeveiliging is ISO 27001. [6] Maatregelen worden op basis van best practices in het hoger onderwijs, het Normenkader Surfaudit[7] en ISO 27002 genomen[8];
- **Het nemen van de verantwoordelijkheid:** het College van Bestuur neemt haar verantwoordelijkheid door de uitgangspunten en de organisatie van het informatiebeveiligingsbeleid vast te leggen voor alle betrokkenen binnen de UvA;
- **Compliance:** het beleid biedt de basis om te voldoen aan wettelijke voorschriften. In Bijlage A wordt de relevante wet- en regelgeving benoemd.

---

[4] Privacybeleid en beleid verwerking persoonsgevens Universiteit van Amsterdam.
[5] Onderwijs en onderzoek zijn hier nadrukkelijk onderdeel van.
[6] Voluit: NEN-ISO/IEC 27001: Eisen aan Managementsystemen voor informatiebeveiliging.
[7] https://www.surf.nl/diensten-en-producten/surfaudit/normenkader-surfaudit/index.html.
[8] Voluit: NEN-ISO/IEC 27002: Code voor Informatiebeveiliging.

Het Informatiebeveiligingsbeleid schetst het kader en de uitgangspunten van de Informatiebeveiliging. De nadere uitwerking en operationalisering van dit beleid vindt plaats in separate documenten. Een overzicht van de documenten gerelateerd aan het informatiebeveiligingsbeleid is opgenomen in Bijlage B. Alle documenten worden na vaststelling gepubliceerd op de website van de UvA.

5. Beleidsprincipes

5.1 Algemene uitgangspunten

Algemeen uitgangspunt is dat het informatiebeveiligingsbeleid in overeenstemming is met **relevante wet- en regelgeving**, zoals b.v. de AVG (2018). In Bijlage A wordt een overzicht gegeven van de relevante wetgeving.

De UvA is een open instelling waar veel mogelijk is. Het onderzoek en onderwijs kenmerkt zich door veel samenwerking met externe groepen. De campussen zijn ontmoetingsplaatsen voor medewerkers, studenten en hun gasten. Er wordt van medewerkers en studenten verwacht dat ze zich qua techniek en qua houding 'fatsoenlijk' gedragen **(eigen verantwoordelijkheid)**. Ook binnen een open omgeving moeten er noodzakelijke beveiligingsmaatregelen worden getroffen, waarbij individuen deze maatregelen wellicht minder waarderen. **Proportionaliteit** is hierbij gewenst, waarbij steeds een afweging plaats vindt tussen de impact van een maatregel op het werk van medewerkers en studenten en het risico dat de instelling loopt als de maatregel niet wordt getroffen.

Het succes van beveiliging staat of valt met goede **communicatie** en het bewustzijn van het belang en de noodzaak van informatiebeveiliging bij medewerkers en studenten. Goede communicatie wordt daarom actief bevorderd, op en tussen alle niveaus in de instelling.

5.2 Beleidsuitgangspunten

De volgende beleidsuitgangspunten worden gehanteerd:
Informatiebeveiliging wordt als proces ingericht. Dat houdt in dat de jaarlijkse planning- en controlecyclus, gebaseerd is op ISO 27001[9] (Plan, Do, Check, Act). Er wordt een jaarplan informatiebeveiliging opgesteld en uitgevoerd. De resultaten ervan worden geëvalueerd in een jaarverslag en vertaald naar een nieuw jaarplan. Het jaarplan en jaarverslag worden geconsolideerd in de bestuurlijke Planning- en Controlcyclus.
De beveiliging dient de volgende aspecten van de informatievoorziening te waarborgen:

- Beschikbaarheid: de mate waarin informatie of functionaliteit op de juiste momenten en locaties beschikbaar zijn voor gebruikers;
- Integriteit: de mate waarin informatie betrouwbaar is;
- Vertrouwelijkheid: de mate waarin de toegang tot informatie of functionaliteit beperkt is tot degenen die daartoe bevoegd zijn.

Informatiebeveiliging is ieders verantwoordelijkheid. Medewerkers, studenten, docenten en derden dragen actief bij aan de veiligheid van geautomatiseerde systemen en de daarin opgeslagen informatie. Iedereen behoort de waarde van de digitale informatie te kennen en daarnaar te handelen. Lijnmanagers (leidinggevenden, afdelingshoofden) dragen de primaire verantwoordelijkheid voor een goede informatiebeveiliging. Dat betekent dat de leidinggevenden de verantwoordelijkheid dragen voor een goede informatiebeveiliging in hun groep, afdeling, faculteit, divisie, enzovoorts. Dit omvat ook de keuze van maatregelen en de uitvoering en handhaving ervan binnen de gestelde kaders.

[9] Dit wordt vormgegeven door het inrichten van een Information Security Management System (ISMS). ISMS is een managementsysteem voor informatiebeveiliging.

Eigendom van digitale informatie. De instelling is als rechtspersoon eigenaar van de digitale informatie die onder haar verantwoordelijkheid wordt geproduceerd, tenzij dit anders is overeengekomen voor bijvoorbeeld onderzoek. Daarnaast beheert de instelling informatie, waarvan het eigendom toebehoort aan derden. Medewerkers en studenten dienen goed geïnformeerd te zijn over de regelgeving voor het (her)gebruik van deze informatie.

Waardering van digitale informatie. De waarde wordt door de eigenaar van de informatie bepaald door alle digitale informatie waarop dit beleid van toepassing is, te (laten) classificeren. Met behulp van deze classificatie wordt vastgesteld welk niveau van beveiligingsmaatregelen noodzakelijk is.

Security by design. Bij projecten, zoals de aanschaf van nieuwe systemen, wordt vanaf de start door de opdrachtgever rekening gehouden met informatieveiligheid. Bij (onderzoeks)projecten, infrastructurele wijzigingen of de aanschaf van nieuwe systemen, wordt vanaf de start rekening gehouden met de inrichting van privacy en gegevensbescherming ('Privacy en security by design'). Dit houdt onder andere in dat de UvA handelt conform haar beleidsuitgangspunten en -principes (Hoofdstuk 2), betrokkenen informeert over de functies en de verwerking van persoonsgegevens (conform het Privacybeleid), haar systemen beveiligt en zij haar betrokkenen in staat stelt om hun rechten uit te oefenen conform het Privacybeleid. In alle overeenkomsten met dienstverleners is een paragraaf over informatiebeveiliging opgenomen en wordt (indien persoonsgegevens worden verwerkt) een verwerkersovereenkomst opgesteld.
Bij nieuwe systemen die een hoog risico voor de privacy rechten en - vrijheden van betrokkenen opleveren, wordt er standaard een Privacy Impact Assessment (PIA) uitgevoerd. In een PIA worden de effecten van een voorgenomen verwerkingsactiviteiten beoordeeld en worden deze gestandaardiseerd in kaart gebracht. Op basis hiervan worden maatregelen getroffen om de geconstateerde effecten te voorkomen of te verkleinen. De PIA wordt uitgevoerd door of namens het College van Bestuur als verwerkingsverantwoordelijke.

Informatieveiligheid is een continu proces. Technologische en organisatorische ontwikkelingen binnen en buiten de instelling maken het noodzakelijk om periodiek te bezien of de UvA nog voldoende op koers zit met het beleid. Audits maken het mogelijk het beleid en de genomen maatregelen te controleren op opvolging, effectiviteit en efficiency.

5.3 Classificatie

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

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

Bij de UvA worden alle gegevens, waarop dit informatiebeveiligingsbeleid van toepassing is, geclassificeerd op de kwaliteitsaspecten *Beschikbaarheid, Integriteit* en *Vertrouwelijkheid* (zie Hoofdstuk 1).

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

De classificatie dient door of namens de eigenaar van de betreffende informatie of van het betreffende informatiesysteem te worden bepaald. Voor de concernsystemen van de UvA zijn

functionarissen aangewezen die de rol van systeemeigenaar vervullen[10]. Voor de beschrijving en uitwerking van de beveiligingsniveaus wordt verwezen naar de Classificatierichtlijn Informatie en Informatiesystemen UvA, waarin tevens de classificatiemethodiek is geformuleerd.

6. Rollen en verantwoordelijkheden met betrekking tot het informatiebeveiligingsbeleid

Om het informatiebeveiligingsbeleid gestructureerd en gecoördineerd uit te voeren is bij de UvA een aantal rollen onderkend die aan verschillende functionarissen binnen de organisatie zijn toegewezen.

Inbedding van informatiebeveiliging op strategisch niveau

6.1 Het College van Bestuur

Het College van Bestuur is eindverantwoordelijk voor de informatiebeveiliging binnen de UvA en stelt het beleid en de maatregelen op het gebied van informatiebeveiliging vast. De inhoudelijke verantwoordelijkheid voor informatiebeveiliging is gemandateerd aan de CISO. Deze heeft de opdracht om zorg te dragen voor de informatiebeveiliging voor de gehele instelling.

6.2 Portefeuillehouder informatiebeveiliging

De portefeuillehouder informatiebeveiliging is het Collegelid dat bedrijfsvoering in portefeuille heeft. Het onderwerp informatiebeveiliging en privacy vormt een integraal onderdeel van deze verantwoordelijkheid. Hij/zij is eerstverantwoordelijke voor informatiebeveiliging binnen de UvA.

6.3 Chief Security Officer (CSO)

De Chief Security Officer (CSO) is een rol op strategisch niveau en is belegd bij de Secretaris van de instelling. De CSO adviseert het College van Bestuur op het gebied van de integrale veiligheid. Informatiebeveiliging is een onderdeel van integrale veiligheid.

6.4 Decaan

De Decaan van een faculteit is gemandateerd eindverantwoordelijk voor de informatiebeveiliging binnen de faculteit, als beheerseenheid. Dit betekent dat de decaan binnen de faculteit passende maatregelen moet nemen om te voldoen aan het vigerende informatiebeveiligingsbeleid.

Centrale rollen bij de Bestuursstaf

6.5 Chief Information Security Officer (CISO)

De Chief Information Security Officer (CISO) is een rol op strategisch en tactisch niveau en is belegd bij de bestuursstaf. De CISO formuleert het informatiebeveiligingsbeleid en helpt bij een juiste vertaling daarvan naar instellingsonderdelen. Hij/zij bewaakt de uniformiteit ten aanzien van informatiebeveiliging binnen de organisatie en adviseert het CvB, de decanen en de directie van de centrale ondersteunende diensten. De CISO houdt binnen de UvA toezicht op de toepassing en naleving van het informatiebeveiligingsbeleid. De CISO werkt nauw samen met de functionaris gegevensbescherming (FG)[11]. Elk jaar stelt de CISO een jaarverslag over het afgelopen jaar en een jaarplan voor het volgende jaar op. Het jaarplan 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. Dergelijke verslagen worden geconsolideerd in de Planning- en Controlcyclus. De CISO is functioneel verantwoordelijk voor het Computer Emergency Response Team (CERT).

[10] Zie: https://medewerker.uva.nl/content-secured/az/systeemeigenaarschap/systeemeigenaarschap.html

[11] De functionaris voor de gegevensbescherming (FG) heeft een informerende en adviserende rol binnen de UvA. De FG bevordert het privacy bewustzijn van betrokkenen, bijvoorbeeld door informatie via de UvA-website te verstrekken over privacy en de daaruit voortvloeiende rechten. De FG vervult een onafhankelijke positie binnen de UvA. De verantwoordelijkheden en taken van de FG zijn beschreven in het privacy beleid: “Privacybeleid en beleid verwerking persoonsgevens Universiteit van Amsterdam”

Informatiebeveiliging bij ICTS

6.6 Information Security Manager (ISM)

De rol van Information Security Manager (ISM) wordt ingevuld binnen de staf van ICTS. De ISM vervult een rol bij de vertaling van de strategie naar tactische (en operationele) plannen voor de instelling. Dit doet de ISM samen met de CISO (vanwege de uniformiteit), de facultaire informatie-managers en de eigenaren van de informatiesystemen en technische platforms. Tevens adviseert de ISM over specifieke informatiebeveiligingsmaatregelen in projecten en bewaakt de consistentie van de maatregelen, onder meer om toe te zien op het toepassen van het 'security by design' principe. De ISM is op dit moment tevens coördinator van CERT-UvA.

6.7 Information Security Officer (ISO)

De Information Security Officer (ISO) bij ICTS is een rol op operationeel niveau. De ISO definieert de ICT-beveiligingsrichtlijnen voor de ICT-organisatie in overeenstemming met het informatie-beveiligingsbeleid, de informatiebeveiligingsstrategie en -architectuur van de UvA en organiseert en managet de ICT-beveiliging van de organisatie binnen ICTS.

6.8 CERT

Het CERT is het ICT incident respons team. Zij houdt zich bezig met het voorkomen, detecteren en oplossen van security incidenten. De afhandeling van incidenten wordt door het CERT gecoördineerd en zij belegt acties bij de juiste personen. [12] Het CERT heeft een directe escalatielijn met de CISO en het CvB indien nodig.

Decentrale rollen bij faculteiten of ondersteunende diensten

6.9 Security Officer

De Security Officer bij een faculteit of andere beheereenheid is een rol op tactisch niveau. De Security Officer adviseert de faculteit of het organisatieonderdeel. Hij vervult een rol bij de vertaling van de strategie naar tactische en operationele plannen en bij de implementatie, borging en evaluatie van die plannen. Dit doet de Security Officer samen met de Chief Information Security Officer, de functionele lijn op dit beleidsterrein en de lijnmanagers met een rol als de proces-, systeem-, of dienst eigenaar. De rol van Security Officer kan binnen een faculteit of afdeling door meerdere personen vervuld worden. De invulling van de facultaire Security Officer rol moet zodanig worden ingevuld dat die rekening houdt met omvang van de faculteit of het organisatieonderdeel. Zo is denkbaar dat kleinere organisatieonderdelen een security Officer delen of de rol in de vorm van een security ambassadeur wat lichter invullen.

6.10 Systeemeigenaar

De systeemeigenaar[13] is ervoor verantwoordelijk dat de applicatie en bijbehorende ICT-faciliteiten een goede ondersteuning bieden aan het proces en voldoen aan het informatiebeveiligingsbeleid. Dit betekent dat de systeemeigenaar er voor zorgt dat zowel nu, als in de toekomst de applicatie en bijbehorende ICT-faciliteiten beantwoorden aan de eisen en wensen van de gebruikers, de wet- en regelgeving en het informatiebeveiligingsbeleid. De systeemeigenaar kan hierin ondersteund worden door de CISO en/of ISM.

6.11 Leidinggevende

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

- er voor te zorgen dat zijn/haar medewerkers op de hoogte zijn van (de voor hen relevante aspecten van) het beveiligingsbeleid;
- toe te zien op de naleving van het beveiligingsbeleid door zijn/haar medewerkers;

[12] Voor informatie over de werkwijze van CERT zie https://extranet.uva.nl/content/a-z/cert-uva/cert-uva.html.

[13] De systeemeigenaar is verantwoordelijk voor de beschikbaarheid en kwaliteit van de informatiediensten die door het systeem geleverd worden. Het systeemeigenaarschap wordt belegd op het niveau van afdelingshoofd, divisiemanager of directeur.

- regelmatig het onderwerp informatiebeveiliging onder de aandacht te brengen in werkoverleggen;
- als aanspreekpunt beschikbaar te zijn voor alle personeel gerelateerde informatiebeveiligingszaken.

De leidinggevende kan hierin ondersteund worden door de Security Officer, CISO en/of ISM.

6.12 Medewerkers

Informatiebeveiliging en het zorgvuldig omgaan met persoonsgegevens is ieders verantwoordelijkheid. Er wordt van medewerkers verwacht dat ze zich integer gedragen. Het is niet acceptabel dat door al dan niet opzettelijk gedrag onveilige situaties ontstaan die leiden tot schade en/of imagoverlies van de Universiteit van Amsterdam of van individuen. Het is om deze reden dat er gedragscodes worden geformuleerd[14]. Er zullen passende voorlichtings- en trainingsactiviteiten worden aangeboden.

6.13 Inpassing in de instellingsgovernance

Om de samenhang in de organisatie met betrekking tot informatiebeveiliging goed tot uitdrukking te laten komen en de initiatieven en activiteiten op het gebied van de informatiebeveiliging binnen de verschillende onderdelen op elkaar af te stemmen, is het belangrijk om gestructureerd overleg te voeren over het onderwerp informatiebeveiliging op verschillende niveaus.

Op **strategisch niveau** wordt richtinggevend gesproken over governance en compliance, alsmede over doelen, bereik en ambitie op het gebied van informatiebeveiliging. Het strategisch niveau wordt ingevuld in het overleg tussen het College van Bestuur en de decanen (CBO).

Op **tactisch niveau** wordt de strategie vertaald naar plannen, te hanteren normen en evaluatiemethoden. Deze plannen en instrumenten zijn sturend voor de uitvoering. Het tactisch niveau wordt ingevuld in het overleg tussen het College van Bestuur, de directeuren bedrijfsvoering van de faculteiten, de directeuren van de centrale stafdiensten en de directeuren van de centrale diensten (BVO).

Op **operationeel niveau** worden de zaken besproken die de dagelijkse bedrijfsvoering en uitvoering aangaan. Het operationeel niveau wordt ingevuld door de directeuren van de centrale diensten en de directeuren bedrijfsvoering, alsmede door (groepen van) medewerkers waar de directeuren leiding aan geven.

7. Implementatie van beleid

Het College van Bestuur van de UvA is eindverantwoordelijk voor de informatiebeveiliging binnen de UvA en stelt het beleid en de maatregelen op het gebied van informatiebeveiliging vast. De feitelijke uitvoering van het informatiebeveiligingsbeleid vindt echter plaats op allerlei lagen van de UvA. Het goed, efficiënt en verantwoord leiden van een organisatie wordt vaak aangeduid met de term governance. Het omvat vooral ook de relatie met de belangrijkste belanghebbenden van de UvA, zoals medewerkers, studenten, subsidieverstrekkers en partners, alsmede de samenleving als geheel. De UvA streeft een goed corporate governance-beleid na en heeft in dit verband aandacht voor de rechten van alle betrokkenen, zoals geformuleerd in de Code goed bestuur universiteiten van de VSNU.[15]

7.1 Informatie voor medewerkers en studenten

Iedere medewerker heeft overeenkomstig zijn rol een eigen verantwoordelijkheid. Er wordt van medewerkers en studenten verwacht dat ze zich qua techniek en ook qua houding ‘fatsoenlijk’ gedragen. Niet acceptabel is dat door al dan niet opzettelijk doen of nalaten onveilige situaties ontstaan die leiden tot schade en/of imagoverlies voor de UvA of van individuen. De UvA informeert haar studenten en medewerkers over wat er van hen verwacht wordt door middel van

[14] Acceptable use policies voor medewerkers en studenten.
[15] Artikel 2.1.2 van de Code goed bestuur universiteiten van de VSNU.

informatie op intranet. Daarbij worden ook instructies en tips gegeven voor het veilig werken met gegevens en ICT-middelen.

7.2 Bewustwording

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van informatiebeveiliging uit te sluiten. In de praktijk blijkt de mens meestal de belangrijkste risicofactor. Daarom worden beveiligingsrisico's en -maatregelen regelmatig onder de aandacht gebracht, zodat kennis van risico's wordt verhoogd en het (veilig en verantwoord) gedrag wordt aangemoedigd. Onderdeel van de uitvoering van het informatiebeveiligingsbeleid zijn regelmatig terugkerende bewustwordings-campagnes voor medewerkers, studenten en derden. Zulke campagnes kunnen aansluiten bij landelijke campagnes in het hoger onderwijs, zo mogelijk in afstemming met beveiligingscampagnes voor Arbo, milieu en fysiek. Deze campagnes worden onder regie van de CISO en FG geïnitieerd, waarbij in de uitvoering wordt samengewerkt met Bureau Communicatie en de leidinggevenden binnen staven, diensten en faculteiten.

7.3 Controle en naleving

Jaarplan en jaarverslag. Elk jaar stelt de CISO een jaarverslag over het afgelopen jaar en een jaarplan voor het volgende jaar op. Het jaarplan is mede gebaseerd op de resultaten van de periodieke controles / audits. Er wordt o.a. ingegaan op incidenten, resultaten van risicoanalyses (incl. genomen maatregelen), advisering op aangepaste of nieuwe informatiesystemen ('security by design') en andere initiatieven die het afgelopen jaar hebben plaatsgevonden. Dergelijke verslagen worden geconsolideerd in de Planning- en Controlcyclus. Het jaarplan en jaarverslag wordt aangeboden aan het CvB in het kader van de Planning- en Controlcyclus. Het College van Bestuur deelt de bevindingen uit de verslaglegging van de CISO met de Centrale Ondernemingsraad (COR) en de Centrale Studentenraad (CSR).

Toezicht op naleving. De CISO houdt toezicht op de naleving van het informatiebeveiligingsbeleid, inclusief de toewijzing van verantwoordelijkheden, bewustwording en opleiding van personeel en stemt dit af met de functionaris gegevensbescherming (FG) waar dit privacy-vraagstukken raakt. Aanvullend hierop maken audits het mogelijk het beleid en de genomen maatregelen te controleren op naleving en effectiviteit.

8. Melding en afhandeling van incidenten

Computer Emergency Response Team (CERT). Het CERT waakt over de computer- en netwerkveiligheid en heeft een coördinerende taak ten aanzien van de preventie, detectie en correctie van veiligheidsincidenten gericht op de digitale informatie en de systemen. Het CERT bestaat uit ICT- en security specialisten en wordt op dit moment gecoördineerd door de Information Security Manager. De dienstverlening van het CERT is gedocumenteerd (Inrichting CERT- UvA[16]) en door het College van Bestuur bekrachtigd.
Afhankelijk van het type incident rapporteert de coördinator van het CERT aan de CISO, zowel tijdens het incident als na de evaluatie ervan. Ook het hoofd Communicatie (UvA) wordt geïnformeerd. Wanneer het een incident betreft waarbij de privacy wetgeving wordt geschonden wordt direct de functionaris gegevensbescherming (FG) geïnformeerd.

Melding van incidenten. Indien er zich een informatiebeveiligingsincident of een inbreuk voordoet nemen medewerkers, studenten of derden – rechtstreeks of via de servicedesk ICTS – contact op met het CERT. Opschaling binnen ICTS vindt plaats op aanwijzing van het decentraal coördinatieteam van ICTS. Opschaling naar het decentrale crisisteam (DCT) of het centrale crisisteam (CCT) vindt plaats volgens de Crisiswijzer.[17]

[16] Inrichting CERT-UvA versie 2004.
[17] Crisiswijzer Universiteit van Amsterdam 2018

Bijlage A Wetgeving

Bij de UvA wordt op de volgende wijze omgegaan met relevante wet- en regelgeving.

Wet op het Hoger onderwijs en Wetenschappelijk onderzoek. De UvA is een publiekrechtelijke rechtspersoon op grond van artikel 1.8, tweede lid, juncto bijlage 1 onder a, van de Wet op het hoger onderwijs en wetenschappelijk onderzoek (WHW). De bestuurlijke structuur is vastgelegd in de WHW en in het daarop gebaseerde Universiteitsreglement, en is in overeenstemming met de Code goed bestuur universiteiten van de VSNU (versie 2017)[18]. De UvA heeft een kwaliteitszorgsysteem, waarin (onder meer) het zorgvuldig omgaan met gegevens in de studentenadministratie en met de studieresultaten is gewaarborgd. Daarnaast worden gedrags- en integriteitscodes voor (wetenschappelijk) onderzoek nageleefd en toegepast.[19]

Wet bescherming persoonsgegevens (Wbp). De Wet bescherming persoonsgegevens (Wbp) wordt per 25 mei 2018 vervangen door de Algemene Verordening Gegevensbescherming. Onderliggend beleid is daarom vormgegeven op basis van de bepalingen uit de AVG (zie volgende paragraaf).

Algemene Verordening Gegevensbescherming (AVG). 25 mei 2018 is de AVG rechtstreeks van toepassing in alle lidstaten van de Europese Unie. De AVG is de opvolger van de Wbp in Nederland en kent onder andere striktere eisen voor documentatie van verwerkingen en verantwoording naar betrokkenen. De UvA heeft deze striktere eisen uit de AVG geïmplementeerd door middel van het privacybeleid. De UvA verwerkt persoonsgegevens wanneer de verwerking op één (of meer) grondslagen uit de AVG kan worden gebaseerd. De UvA heeft in het kader van de AVG een aantal technische en organisatorische maatregelen geïmplementeerd, zoals de aanstelling van een Functionaris voor de gegevensbescherming (FG), ingeregelde werkwijzen voor het kunnen doen gelden van de rechten op informatie en inzage en een procedure voor het melden van datalekken. Bij het ontwikkelen en aanpassen van informatiesystemen worden de principes ‘privacy en security by design’ gehanteerd.

Archiefwet. De UvA houdt zich aan de voorschriften uit de Archiefwet en het Archiefbesluit over de wijze waarop omgegaan moet worden met informatie vastgelegd in (gedigitaliseerde) documenten, informatiesystemen, websites, e.d. Dit is onderdeel van de jaarlijkse externe accountantsrapportages.

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

Telecommunicatiewet. De Telecommunicatiewet is niet van toepassing omdat de UvA geen openbare netwerken kent. De netwerken zijn slechts beschikbaar voor een besloten groep betrokkenen (studenten en medewerkers) bij onderwijs en onderzoek en geven toegang tot daarvoor relevante diensten.

Wet Computercriminaliteit. De Wet Computercriminaliteit richt zich op de strafrechtelijke probleemgebieden in relatie tot het computergebruik. De wet schrijft voor dat ‘enige beveiliging’ vereist is alvorens er sprake kan zijn van het eventueel strafrechtelijk vervolgen van delicten jegens de onderwijsinstelling en het eventueel vrijwaren van bestuurders van de instelling. Naleving van dit informatiebeveiligingsbeleid en implementatie van de basis maatregelen bij de UvA moet leiden tot een niveau van beveiliging dat als voldoende mag worden gezien in het kader van de Wet Computercriminaliteit.

---

[18] Code goed bestuur, versie 2017. Te vinden via: www.vsnu.nl > domeinen > Governance & Accountability > Code goed bestuur. Direct link: https://www.vsnu.nl/files/documenten/Domeinen/Governance/Code%20Goed%20Bestuur%202017.pdf

[19] Dit betreft onder andere De Nederlandse Gedragscode Wetenschapsbeoefening, 2014. Te vinden via: > domeinen > Governance & Accountability > Nederlandse gedragscode Wetenschapsbeoefening. Direct link: http://www.vsnu.nl/files/documenten/Domeinen/Onderzoek/Code_wetenschapsbeoefening_2004_(2014).pdf

Bijlage B Aan het informatiebeveiligingsbeleid gerelateerde documenten

Het Informatiebeveiligingsbeleid schetst het kader en de uitgangspunten van het beleid. De nadere uitwerking van dit beleid vindt plaats in separate documenten. Deze bijlage bevat een overzicht van de documenten op het gebied van informatiebeveiliging. Alle beleidsdocumenten worden na vaststelling gepubliceerd op de website van de UvA.

Security principes. Het hoogste niveau van idealen en waarden die de organisatie leiden in haar gedrag. Voorbeelden zijn:

- Openheid - Security oplossingen zijn gebouwd op open protocollen en systemen, zijn onderhoudbaar, worden ondersteund door een breed aantal platformen, ondersteunen een breed aantal grote industrie standaarden. Geen security by obscurity.
- Security by Design - Security moet worden ontworpen als een integraal onderdeel van de systeem architectuur

De security principes worden vastgesteld door het CvB en wordt ter instemming aangeboden aan de COR/CSR.

Security organisatie. Dit document beschrijft de taken, verantwoordelijkheden en bevoegdheden van de verschillende rollen in de security organisatie en de organisatorische positionering. Tevens wordt de functionele en hiërarchische relatie van de rollen beschreven. Voor de rol van Security Officer bij faculteiten en diensten wordt een advies geformuleerd voor het type functie(s) dat deze rol kan invullen. De security organisatie worden vastgesteld door het CvB en wordt ter instemming aangeboden aan de COR/CSR.

Acceptable Use Policy (Gebruiksregels ICT-faciliteiten) voor medewerkers van de Universiteit van Amsterdam. Met deze gedragslijn stelt de UvA regels omtrent het gewenst gebruik van haar ICT-faciliteiten door medewerkers. Het streven daarbij is een goede balans aan te brengen tussen het inzetten van ICT-faciliteiten ten behoeve van onderwijs, onderzoek en bedrijfsvoering aan de ene kant en het verantwoord en veilig gebruik van de ICT-faciliteiten en de privacy van de medewerker aan de andere kant. De Acceptable Use Policy wordt vastgesteld door het CvB en wordt instemming aangeboden aan de COR.

Acceptable Use Policy (Gebruiksregels ICT-faciliteiten) voor studenten van de Universiteit van Amsterdam. Met deze gedragslijn stelt de UvA regels omtrent het gewenst gebruik van haar ICT-faciliteiten door studenten. Het streven daarbij is een goede balans aan te brengen tussen het inzetten van ICT-faciliteiten ten behoeve van onderwijs, onderzoek en bedrijfsvoering aan de ene kant en het verantwoord en veilig gebruik van de ICT-faciliteiten en de privacy van de student aan de andere kant. De Acceptable Use Policy wordt vastgesteld door het CvB en wordt ter instemming aangeboden aan de CSR.

Classificatierichtlijn Informatie en Informatiesystemen UvA. Dit document beschrijft de classificatiemethodiek die wordt toegepast om informatiesystemen te classificeren op de kwaliteitsaspecten Beschikbaarheid, Integriteit en Vertrouwelijkheid. Op basis van deze classificatie kan het niveau van beveiligingsmaatregelen worden bepaald. De richtlijn wordt samen met de HvA opgesteld. De classificatierichtlijn wordt vastgesteld door het CvB en wordt ter informatie aangeboden aan de COR en CSR.

Autorisatiebeleid. Het Autorisatiebeleid geeft algemene richtlijnen hoe bij informatiesystemen om te gaan met autorisaties. Het toekennen van rechten wie wat mag, noemen we autorisatie. De UvA gebruikt informatiesystemen om relevante gegevens te raadplegen en vast te leggen. Bij alle systemen is de integriteit van belang, we willen immers niet dat iedereen zomaar gegevens kan veranderen. Bij veel systemen speelt de vertrouwelijkheid een rol, niet iedereen mag zomaar persoonsgegevens of anderszins vertrouwelijke informatie raadplegen. Voor het naleven van de AVG is het noodzakelijk dat het autorisatiebeleid van de systemen welke de gegevens over personen

bevatten goed is geregeld. Het autorisatiebeleid wordt vastgesteld door het CvB en wordt ter instemming aangeboden aan de COR en CSR.

UvA-leidraad voor Responsible Disclosure. Responsible disclosure binnen de ICT-wereld is het op een verantwoorde wijze en in gezamenlijkheid tussen melder en organisatie openbaar maken van ICT-kwetsbaarheden op basis van een door organisaties hiervoor vastgesteld beleid voor responsible disclosure. De leidraad beschrijft verantwoordelijkheden van de organisatie en de melder en de bouwstenen voor responsible disclosure bij de UvA. De leidraad wordt opgesteld gebruik makend van voorbeelden zoals die van het Ministerie van Veiligheid en Justitie. De UvA-leidraad voor Responsible Disclose wordt vastgesteld door het CvB en wordt ter informatie aangeboden aan de COR en CSR.

Wachtwoordregeling. Wachtwoorden vormen een belangrijk aspect van de informatiebeveiliging van de instelling. Wachtwoorden zorgen ervoor dat onbevoegden minder makkelijk toegang kunnen krijgen tot informatie die onder beheer van de instelling valt (instellingsinformatie). Wachtwoorden beschermen de gebruiker tegen misbruik van zijn account en tegen onbedoelde verspreiding van zijn persoonlijke gegevens. Het doel van deze wachtwoordregeling is tweeledig:

- Het vaststellen van regels waar wachtwoorden en wachtwoord procedures aan moeten voldoen.
- Het vaststellen van de bescherming van de wachtwoorden.

De wachtwoordregeling is vastgesteld door de Stuurgroep ICT en wordt ter informatie aangeboden aan de COR en CSR.

Inrichting-CERT-UvA. Het document Inrichting CERT-UvA beschrijft het doel, taken, verantwoordelijkheden en bevoegdheden, organisatie en middelen van CERT-UvA. De Inrichting CERT-UvA is vastgesteld door het CvB.

Hulpmiddelen voor verantwoorde gegevensopslag. Er wordt een handreiking opgesteld waarmee medewerkers, aan de hand van de aard van de gegevens, kunnen bepalen op welke plaats de gegevens het beste kunnen worden opgeslagen. De handreiking wordt opgesteld door ICTS en wordt ter informatie aangeboden aan de COR.