Informatiebeveiligingsbeleid

Vastgesteld bij besluit nr. 2025-113335 van het College van Bestuur van 10-06-2025.

Inhoudsopgave

Referenties *3*
Definities *4*

1 Inleiding 5

2 Doelgroep 5

3 Reikwijdte 5

4 Doelstellingen 6

5 Uitgangspunten 7

6 Organisatie van informatiebeveiliging 9

6.1 Beleidsverklaring 9
6.2 Strategie 9
6.3 Beleid 9
6.4 Informatiebeveiliging-verbeterplan 10
6.5 Architectuur 10
6.6 Naleving 10
6.7 Communicatie 12
6.8 Rollen en verantwoordelijkheden 13

Bijlage A Relevante wet- en regelgeving 16

Bijlage B Beheersmaatregelen onder verantwoordelijkheid van het CvB 18

Versiebeheer

Versie	Datum	Auteur	Mutaties
1.2	28-07-2018	n.b.	Informatiebeveiligingsbeleid goedgekeurd door CvB.
2.0	10-06-2025	R. Reijers (CISO)	Informatiebeveiligingsbeleid goedgekeurd door CvB.

Referenties

[CERT]	CERT-charter *
[PvI]	Principes voor Informatiebeveiliging *
[SATK]	Surfaudit Toetsingskader: https://www.surf.nl/diensten/surfaudit
[VGF]	Regels voor verantwoord gebruik van ICT-faciliteiten voor medewerkers en studenten *

*) Gepubliceerd Informatiebeveiligingsbeleid is te vinden op: https://medewerker.uva.nl/content-secured/az/security/beleid-informatiebeveiliging/beleid-informatiebeveiliging.html

Definities

Beheersmaatregelen	Een actie gericht op het voorkomen van het optreden van een onzekere gebeurtenis of het beperken van de consequenties van een onzekere gebeurtenis.
Beveiligingsorganisatie	Personen uit de instelling met een beschreven rol in het IB-beleid of in de separaat beschreven governance.
CISO	Chief Information Security Officer (Beveiligingsorganisatie)
FISO	Facultaire Information Security Officer (Beveiligingsorganisatie)
FIM	Facultaire Informatie Manager
FG	Functionaris Gegevensbescherming
IB-beleid	Informatiebeveiligingsbeleid van de UvA
Informatie-eigenaar	Aangewezen eigenaar van informatie of lijnmanager met een rol als eigenaar van informatie.
ISO	Information Security Officer (Beveiligingsorganisatie)
Proceseigenaar	Inhoudelijk procesverantwoordelijke, aangewezen eigenaar van een proces.
Systeemeigenaar	Aangewezen eigenaar van een systeem of lijnmanager met een rol als eigenaar van het systeem.

1 Inleiding

Voor het goed functioneren van de Universiteit van Amsterdam (hierna: UvA) is het zorgvuldig omgaan met en goed beveiligen van informatie essentieel. Informatiebeveiliging is het treffen en onderhouden van een samenhangend pakket aan beheersmaatregelen om de kwaliteitsaspecten Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV) van de informatievoorziening te garanderen. Deze drie aspecten moeten aantoonbaar goed geregeld zijn.

- **Beschikbaarheid**: de mate waarin informatie of informatie-verwerkende voorzieningen op de juiste momenten tijdig beschikbaar zijn voor gebruikers.
- **Integriteit**: de mate waarin informatie of informatie-verwerkende voorzieningen correct en volledig zijn.
- **Vertrouwelijkheid**: de mate waarin de toegang tot informatie of informatie-verwerkende voorzieningen beperkt is tot degenen die daartoe bevoegd zijn.

In dit document, het informatiebeveiligingsbeleid (IB-beleid), is verwoord op welke manier de UvA voorziet in adequate informatiebeveiliging en daarmee voldoet aan haar verantwoordingsplicht jegens de relevante wet- en regelgeving. Het document legt de beleidsprincipes vast, de verantwoordelijke organisatie van de beveiligingsfunctie alsook het geldende normenkader dat de *beheersmaatregelen* specificeert. Met het IB-beleid wil de UvA ook bijdragen aan een betere kwaliteit van de informatievoorziening en zorgen voor een juiste balans tussen functionaliteit en veiligheid. De UvA heeft de ambitie om de informatiebeveiliging verder te borgen en te verbeteren.

2 Doelgroep

Het is van essentieel belang dat iedereen binnen de organisatie – van bestuurders en leidinggevenden tot en met medewerkers, studenten, gasten, bezoekers, leveranciers en externe relaties – zijn/haar verantwoordelijkheden kent en neemt. Dit IB-beleid heeft als doelgroep iedereen die, intern dan wel extern, op enige manier te maken heeft met (aspecten van) de processen in onderwijs, onderzoek en bedrijfsvoering bij de UvA.

Dit IB-beleid is niet van toepassing op ACTA en de Faculteit Geneeskunde.

- 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 IB-beleid van de VU.
- De Faculteit Geneeskunde maakt gebruik van de ICT-voorzieningen van het AUMC en valt voor de verwerking van gegevens in die systemen onder het IB-beleid van het AUMC.

Voor zover ACTA en de Faculteit Geneeskunde gebruikmaken van informatiesystemen die vallen onder de verantwoordelijkheid van de UvA, valt dat gebruik onder het IB-beleid van de UvA.

3 Reikwijdte

Het IB-beleid heeft betrekking op alle informatie die valt onder de verantwoordelijkheid van de UvA voor alle organisatieonderdelen en op alle (derde) partijen, mensen en apparatuur die deze informatie verwerken en op alle locaties waar deze informatie verwerkt wordt.

Aanpalende beleidsterreinen

Het IB-beleid heeft veel raakvlakken en ook overlap met de volgende beleidsterreinen van de UvA:

- **Financiën, planning & control:** Het borgen van de betrouwbaarheid van de financiële informatie en rechtmatigheid van bestedingen. Daarnaast is de coördinatie van het UvA brede risicomanagement belegd bij de afdeling Financiën, Planning & Control. Het informatiebeveiligingsbeleid hanteert het Kader Risicomanagement van de UvA als uitgangspunt voor het risicomanagementproces.
- **Privacy**: De belangrijkste regels voor de omgang met persoonsgegevens in Nederland zijn vastgesteld in de AVG, die onder andere toeziet op de beveiliging van de verwerking van persoonsgegevens (artikel 32, AVG). Daarin wordt aangegeven dat de verwerkingsverantwoordelijke (UvA) maatregelen dient te treffen die passen bij het risico die een verwerking van persoonsgegevens met zich meebrengt. Informatiebeveiligingsmaatregelen worden ingezet om risico's te beheersen.
- **Fysieke beveiliging**: De mate van bescherming van informatie wordt mede bepaald door het toegangsbeheer van locaties, gebouwen en ruimten dat onder fysieke beveiliging valt.
- **Personeelsbeleid**: Bij informatiebeveiliging speelt de mens een cruciale rol waardoor ook in het personeelsbeleid aandacht moet zijn voor informatiebeveiligingsmaatregelen.
- **Digitale strategie en informatiemanagement**: Het succes van een organisatie wordt mede bepaald door de inzet van digitale technologieën. De security-architectuur heeft daarom een sterke afhankelijkheid met de enterprise-architectuur en de informatie-architectuur.
- **Kennisveiligheid**: Kennisveiligheid is een opkomend beleidsterrein waar informatiebeveiligingsmaatregelen ingezet worden om risico's te beperken.
- **Sociale veiligheid**: Sociale (on)veiligheid breidt zich uit naar het digitale domein waar informatiebeveiligingsmaatregelen ingezet worden om risico's te beperken.

De adviesteams van Integrale Veiligheid binnen de Bestuursstaf zorgen voor de planmatige en inhoudelijke afstemming tussen de verschillende beleidsterreinen.

4 Doelstellingen

Het UvA IB-beleid heeft de volgende doelen:

- Het waarborgen van de Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV) van de informatie in de onderwijs-, onderzoek- en bedrijfsvoeringsprocessen.
- Het voorkomen van incidenten en het minimaliseren van eventuele gevolgen wanneer een incident plaatsvindt.

De afgeleide doelstellingen voor het IB-beleid zijn:

- **Het bieden van een kader**: het beleid biedt een kader om maatregelen in de informatiebeveiliging te toetsen aan een vastgestelde normering en om de taken, bevoegdheden en verantwoordelijk-heden in de organisatie te beleggen.

- **Het stellen van normen**: de basis voor de inrichting van informatiebeveiliging is het SURFaudit Toetsingskader [SATK] dat gebaseerd is op de standaard ISO 27001[1]. Beheersmaatregelen worden op basis van dit toetsingskader en op basis van aanvullende nationale- en internationale *best practices* genomen. Het SURFaudit Toetsingskader beschrijft wat de vereisten zijn om aan het gewenste volwassenheidsniveau voor informatiebeveiliging te voldoen. Het gewenste volwassenheidsniveau voor informatiebeveiliging wordt bepaald door de koepel van Universiteiten van Nederland (UNL).
- **Het nemen van de verantwoordelijkheid**: het College van Bestuur neemt zijn verantwoordelijkheid door het IB-beleid en de governance vast te leggen voor de UvA.
- **Compliance**: het beleid biedt de basis om te voldoen aan de wettelijke voorschriften en interne regelgeving voor het inrichten van de informatiebeveiliging. De relevante wet- en regelgeving staat benoemd in Bijlage A.

Het IB-beleid beschrijft het kader en de uitgangspunten van de Informatiebeveiliging. De nadere uitwerking van onderwerp specifieke beleidsregels vindt plaats in separate thematische documenten, zoals benoemd in hoofdstuk 6.3.

5 Uitgangspunten

Algemene uitgangspunten

De UvA is een instelling met een open karakter die **open onderzoek en onderwijs** hoog in het vaandel heeft staan. Het adagium is "Open uitwisseling van kennis voor onderzoek en onderwijs, tenzij er zwaarwegende redenen zijn om niet open te werken". Bijvoorbeeld als dit kan leiden tot het schenden van de privacy of het gebruiken van kennis voor niet ethische doeleinden.

Het onderzoek en onderwijs kenmerkt zich door veel **samenwerking** met externe partijen zoals kennisinstellingen en bedrijven. De campussen zijn ontmoetingsplaatsen voor medewerkers, studenten en hun gasten.

Ook in een instelling met een open karakter zijn beveiligingsmaatregelen noodzakelijk. Deze maatregelen moeten in verhouding staan tot de eventuele risico's; **proportionaliteit** is hierbij gewenst. Er moet steeds een goede afweging gemaakt worden tussen de gevolgen van een maatregel voor het werk van medewerkers en studenten *en* het risico dat de instelling loopt als de maatregel niet wordt getroffen.

Het IB-beleid en de uitvoering daarvan is in **overeenstemming met relevante wet- en regelgeving** op basis van het principe 'Pas toe of leg uit'.

De UvA verwacht van medewerkers en studenten dat ze zich qua houding en qua omgang met techniek 'fatsoenlijk' gedragen; dat is hun **eigen verantwoordelijkheid** nemen met betrekking tot de beveiliging van de informatie van de instelling. De "Regels voor verantwoord gebruik van ICT-faciliteiten" [VGF] maken het verwacht gedrag duidelijk.

[1] Voluit: NEN-ISO/IEC 27001: Eisen aan Managementsystemen voor informatiebeveiliging.

Beveiliging kan alleen succesvol zijn als medewerkers en studenten zich bewust zijn van het belang en de noodzaak, hun rol en verantwoordelijkheid kennen, en hiernaar handelen. Goede **communicatie** wordt daarom actief bevorderd, op en tussen alle niveaus in de instelling.

Beleidsuitgangspunten

De volgende beleidsuitgangspunten worden gehanteerd:

Eigendom van informatie.
De instelling is als rechtspersoon eigenaar van de (fysieke en digitale) informatie die onder haar verantwoordelijkheid wordt verwerkt, tenzij dit anders is overeengekomen voor bijvoorbeeld onderzoek. De instelling borgt het eigenaarschap verder in de organisatie.
Daarnaast beheert de instelling informatie van derden. Medewerkers en studenten dienen goed geïnformeerd te zijn over de regelgeving voor het (her)gebruik van deze informatie.

Waardering van informatie.
Iedereen behoort de waarde van informatie te kennen en daarnaar te handelen. Deze waarde wordt bepaald door de mogelijke schade als gevolg van verlies van beschikbaarheid, integriteit of vertrouwelijkheid. De waarde van de informatie wordt door de eigenaar van de informatie bepaald. De eigenaar van de informatie moet alle informatie waarop het IB-beleid van toepassing is (laten) classificeren. Aan de hand van deze classificatie wordt vastgesteld welk niveau van beveiliging proportioneel is en welke maatregelen nodig zijn.

Security by design
Bij projecten, zoals het aanschaffen van nieuwe informatiesystemen of software(tools), moet de opdrachtgever vanaf de start rekening houden met informatiebeveiliging. Bij (onderzoeks)projecten, infrastructurele wijzigingen of het aanschaffen van nieuwe (informatie)systemen moet vanaf de start rekening worden gehouden met de inrichting van gegevensbescherming (‘security by design’). Dit houdt onder andere in dat de UvA handelt conform haar beleidsuitgangspunten en -principes, haar systemen beveiligt, en in overeenkomsten met dienstverleners afspraken vastlegt over informatiebeveiliging.

Informatiebeveiliging is ieders verantwoordelijkheid.
Alle medewerkers van de UvA hebben een verantwoordelijkheid in de informatiebeveiliging van de UvA. Het bestuur en hoger management, leidinggevenden en de beveiligingsorganisatie dragen de primaire verantwoordelijkheid voor de informatiebeveiliging. Zij zien er vanuit hun lijnverantwoordelijkheid op toe dat iedereen het beleid naleeft en dragen het beleid uit. Dat betekent dat die leidinggevenden de verantwoordelijkheid dragen voor een goede informatiebeveiliging in hun groep, afdeling, faculteit, divisie, enzovoorts. Dit omvat ook de keuze van maatregelen, de uitvoering, handhaving en rapportage ervan binnen de gestelde kaders.

Informatiebeveiliging is een continu proces.
Het beveiligen van informatie is een continu proces dat wordt afgestemd op de jaarlijkse planning- en control cyclus: er wordt een Jaarplan Informatiebeveiliging opgesteld. De resultaten van het plan worden geëvalueerd en samengevat in een jaarverslag. Op basis van de evaluatie wordt een nieuw jaarplan opgesteld. Organisatorische en technologische ontwikkelingen binnen en buiten de instelling en veranderingen in wetgeving worden op de voet gevolgd. Het IB-beleid wordt daarmee in lijn gebracht. Door het (laten) uitvoeren van audits controleert de instelling of het beleid en de vereiste maatregelen worden opgevolgd en of deze voldoende effectief en efficiënt zijn.

6 Organisatie van informatiebeveiliging

6.1 Beleidsverklaring

Het College van Bestuur ziet toe op de doeltreffende naleving van het IB-beleid. Zij zorgt voor:

- de middelen en maatregelen om informatie op het gewenste niveau te beschermen,
- voor de continue verbetering van informatiebeveiliging, en
- het borgen van informatiebeveiliging door middel van verbeterplannen en het (laten) uitvoeren van audits volgens het Surfaudit Toetsingskader [SATK].

6.2 Strategie

Het Instellingsplan van de UvA bepaalt de strategie voor de instelling. De CISO ziet toe op het opstellen en onderhouden van een hiervan afgeleide informatiebeveiligingsstrategie en -visie, stemt die af met de stakeholders[2] in de instelling en laat deze vaststellen door het CvB. De geldigheid en uitvoerbaarheid wordt jaarlijks geverifieerd door de CISO.

6.3 Beleid

Opzet en goedkeuring van beleid

Het UvA IB-beleid (dit document) wordt opgesteld onder verantwoordelijkheid van de CISO en wordt vastgesteld door het CvB.

De thematische uitwerkingen van het IB-beleid, die gebaseerd zijn op de beheersmaatregelen uit het SURFaudit Toetsingskader [SATK], ISO27001 of andere in de sector of internationaal geldende richtlijnen of best practices, worden separaat opgesteld en vastgesteld door de CISO onder de voorwaarden dat de CISO overeenstemming bereikt over de verwachte kosten, toetsbare uitgangspunten en de impact op andere afdelingen met relevante stakeholders.
Relevante stakeholders kunnen zijn: decanen, faculteitsdirecteuren, directeuren bedrijfsvoering en dienstdirecteuren, controllers, Functionaris Gegevensbescherming, Centrale Privacy Officer, Juridische Zaken, Informatiemanagement, coördinator UvA breed risicomanagement en hoofden van de relevante stafafdelingen afhankelijk van het onderwerp. Deze stakeholders laten zich inhoudelijk adviseren door onder andere: (decentrale) Information Security Officers, Informatiemanagers, Privacy Officers en relevante inhoudsdeskundigen.
In het geval dat de CISO *geen* overeenstemming bereikt met de stakeholders legt de CISO het thema IB-beleid voor aan de portefeuillehouder Informatiebeveiliging van het CvB.

Thematische uitwerkingen die een directe impact hebben op medewerkers en/of studenten worden alsnog door het College van Bestuur expliciet vastgesteld. Bijlage B bevat de lijst met thema's.

Het UvA IB-beleid en de thematische uitwerkingen van het beleid kunnen (optioneel) verder worden uitgewerkt in lokaal beleid, toegespitst op de lokale context binnen de bestuursstaf, faculteit of dienst.

[2] BVO en stakeholders van "Aanpalende beleidsterreinen" (H3).

Dergelijk beleid wordt vastgesteld door de verantwoordelijke secretaris, decaan of directeur. De verantwoordelijke laat zich bij het vaststellen adviseren door de CISO.

Implementatie van IB-beleid

In de instelling wordt op centraal- en decentraal niveau uitvoering gegeven aan het implementeren van het IB-beleid. Op centraal niveau valt dit onder de verantwoordelijkheid van de Secretaris. Op decentraal niveau valt dit onder de eindverantwoordelijkheid van decanen, faculteitsdirecteuren of directeuren van diensten. De CISO adviseert en monitort de algehele planvorming en op de uitvoering van de implementatie.

De CISO:

- informeert de stakeholders over nieuw beleid en eventuele wijzigingen in bestaand beleid, en
- publiceert het IB-beleid zodat het vindbaar en toegankelijk is voor de hele organisatie.

Evaluatie van beleid

Beleid en richtlijnen worden tenminste één keer per vier jaar geëvalueerd en opnieuw vastgesteld en daar waar nodig tussentijds geactualiseerd. Beleidsonderwerpen die voor wijziging in aanmerking komen, worden opgenomen in de informatiebeveiliging-verbeterplannen van de CISO, de faculteit en/of de dienst.

6.4 Informatiebeveiliging-verbeterplan

De CISO vertaalt de informatiebeveiligingsvisie en -strategie door in het (centrale) verbeterplan voor informatiebeveiliging en voorziet dit van een activiteitenplanning en een (globale) tijdsplanning. Het informatiebeveiliging-verbeterplan wordt *jaarlijks* vastgesteld door het CvB en bepaalt de budgettering, prioritering en high-level planning van de implementatie en de uitvoering van activiteiten en beheersmaatregelen voor informatiebeveiliging.

De Information Security Officer(s) van faculteiten en diensten maken een doorvertaling van het centrale verbeterplan naar het eigen (decentrale) informatiebeveiliging-verbeterplan. De decaan of de directeur van faculteit of dienst stelt *jaarlijks* het eigen verbeterplan vast en stemt dit af met het CVB.

6.5 Architectuur

Ter ondersteuning van de implementatie van het IB-beleid wordt onder de verantwoordelijkheid van de CISO een security-architectuur opgesteld. Deze wordt afgeleid van de enterprise-architectuur en sluit aan bij de informatie-architectuur van de instelling. De security-architectuur ondersteunt bij het maken van de veilige keuzes voor het ondersteunen van de bedrijfsprocessen.

De architectuurprincipes voor informatiebeveiliging zijn verder uitgewerkt in: Principes voor Informatiebeveiliging [PvI].

6.6 Naleving

Een belangrijk onderdeel van het IB-beleid is het controleren op de correcte naleving van het beleid. Deze controle bestaat uit de interne toetsing, de onafhankelijke toetsing en de rapportage en managementbeoordeling van de implementatie en effectiviteit van het beleid.

Interne toetsing

Interne controles vinden plaats op verschillende manieren:

Interne audits
Het SURFaudit Toetsingskader [SATK] wordt gebruikt als uitgangspunt voor een *jaarlijkse* interne audit op processen en informatiesystemen van faculteiten en diensten, gepland en uitgevoerd door de Interne Auditafdeling van de instelling. Alle onderwerpen uit het SURFaudit Toetsingskader worden in een driejaarlijkse cyclus getoetst, verspreid over de faculteiten en diensten[3]. De interne audit richt zich specifiek op (1) de correcte classificatie van vastgelegde gegevens in informatiesystemen, (2) de juiste mitigatie van de risico's uit het SURFaudit Toetsingskader, (3) de effectiviteit van de (bijbehorende) beveiligingsmaatregelen en (4) de samenhang tussen deze onderwerpen.

Periodieke controles
De van toepassing zijnde beheersmaatregelen[4] kunnen periodieke controles voorschrijven die uitgevoerd moeten worden door de verantwoordelijke eigenaar van de beheersmaatregel[5] en kunnen een controle vereisen door een 2e lijn. Dit staat uitgewerkt in het thematisch IB-beleid van de respectievelijke beheersmaatregelen.

Incidentele activiteiten
De interne controles worden in opdracht van de CISO aangevuld met diverse incidentele activiteiten, zoals het nemen van steekproeven, het uitvoeren van (penetratie)testen, het controleren van de feitelijke werking van de vastgestelde beveiligingsmaatregelen, en het monitoren van de uitvoering van de informatiebeveiligingsjaarplannen.

Oefeningen
Crisisbeheersingsvaardigheden en operationele procedures worden *jaarlijks* geoefend in een brainstormsessie, tabletop oefening of een simulatie-oefening, zo mogelijk in samenwerking met andere instellingen[6] in opdracht van het CvB.

Onafhankelijke toetsing

Het SURFaudit Toetsingskader [SATK] wordt gebruikt als uitgangspunt wanneer een onafhankelijke partij een audit uitvoert op de processen en informatiesystemen van faculteiten en diensten.

De koepel van Universiteiten van Nederland (UNL) vereist een *jaarlijkse* auditfrequentie en de Vereniging Hogescholen (VH) vereist een *tweejaarlijkse* audit frequentie. De gezamenlijke diensten van de universiteit en de hogeschool worden om die reden (mogelijk) geauditeerd op de hoogste frequentie van die twee: *jaarlijks*.

[3] Alle onderwerpen moeten tenminste 1x in de drie jaar aan bod komen. De onderwerpen worden verdeeld over de faculteiten en diensten betekent dat niet alle onderwerpen apart per faculteit of dienst getoetst worden.
[4] Zoals beschreven in de thematische informatiebeveiligingsbeleid documenten.
[5] Dit wordt verder uitgewerkt in §6.8.
[6] Zoals de (N)OZON oefening die jaarlijks door SURF wordt gecoördineerd.

Managementbeoordeling en rapportage

Als onderdeel van de P&C cyclus van de instelling (waar ook het UA brede risicomanagementproces in verankerd is) beoordeelt **het management** (zie toelichting hieronder) de status van de informatiebeveiliging op de volgende aspecten:

- de voortgang van het opvolgen van de bevindingen van de interne en onafhankelijke toetsing van de informatiebeveiligingsrisico's
- de informatiebeveiligingsincidenten
- de voortgang van de implementatie van beheersmaatregelen
- de effectiviteit van beheersmaatregelen uit het [SATK].

Van de managementbeoordeling wordt een rapportage gemaakt en besproken, als volgt:

- De **Information Security Officer (ISO)** van de bestuursstaf/faculteit/dienst stelt de concept managementbeoordeling op.
- De **secretaris/decaan/directeur** bespreekt de managementbeoordeling met de ISO van de bestuursstaf/faculteit/dienst en stelt deze vast.
- De **CISO** bespreekt de managementbeoordeling met de ISO van de bestuursstaf/faculteit/dienst.
- De **Portefeuillehouder Informatiebeveiliging in het CvB** bespreekt de managementbeoordeling met de secretaris/decaan/directeur van de bestuursstaf/faculteit/dienst en vraagt de CISO om een duiding van de managementbeoordeling.

De uitkomst van de managementbeoordeling is input voor het informatiebeveiliging-verbeterplan van de faculteit, dienst en/of instelling.

Ter ondersteuning van de managementbeoordeling wordt een tussentijdse rapportage/beoordeling ontwikkeld op de voornoemde aspecten van de managementbeoordeling:

- De **ISO** rapporteert *per halfjaar* aan de secretaris/decaan/directeur met een cc aan de CISO.
- De **CISO** rapporteert *per halfjaar* aan het CvB.
- De **secretaris/decaan/directeur** rapporteert aan het CvB conform de geldende PDCA-cyclus.

Het **CvB** ontvangt een jaarverslag van de CISO in het eerste kwartaal van ieder kalenderjaar.

6.7 Communicatie

De informatiebeveiligingsstrategie, het IB-beleid en het centrale informatiebeveiliging-verbeterplan worden door de CISO actief gecommuniceerd door:

- deze te publiceren op intranet,
- deze te delen met en te presenteren aan de secretaris, decanen, directeuren bedrijfsvoering en aan de interne *beveiligingsorganisatie*.

Leveranciers worden geïnformeerd over de eisen uit het IB-beleid via de afdeling inkoop (inkoopeisen) en de betrokken interne *beveiligingsorganisatie*.

Medewerkers en studenten worden doelgericht geïnformeerd via de regels-voor-verantwoord-gebruik-ict-faciliteiten[7] [VGF] en via de geëigende communicatiekanalen van de instelling.

[7] Ook wel "acceptable use policy" genoemd.

6.8 Rollen en verantwoordelijkheden

Helderheid over rollen en verantwoordelijkheden is cruciaal om de uitvoering van het IB-beleid te kunnen waarborgen. Dit hoofdstuk beschrijft de strategische rollen waaruit de *beveiligingsorganisatie* is opgebouwd. De *beveiligingsorganisatie* wordt gedetailleerder beschreven in een apart governance document.

Inbedding van informatiebeveiliging op strategisch niveau

College van Bestuur

Het College van Bestuur (CvB) is eindverantwoordelijk voor de informatiebeveiliging binnen de UvA en stelt het IB-beleid en de daaruit voortvloeiende maatregelen vast. Zij zorgt ervoor dat de organisatie over voldoende middelen beschikt om doelen te halen en risico's te mitigeren en stimuleert een cultuur van verantwoord gedrag.

CvB-portefeuillehouder Informatiebeveiliging

De CvB-portefeuillehouder informatiebeveiliging is de eerstverantwoordelijke voor informatiebeveiliging binnen de UvA.

Secretaris

De secretaris van de instelling adviseert het College van Bestuur op het gebied van de integrale veiligheid. Informatiebeveiliging is een onderdeel van integrale veiligheid.

De secretaris is verantwoordelijk voor de informatiebeveiliging op centraal niveau en zorgt ervoor dat er voldoende middelen zijn om te kunnen voldoen aan de eisen van het IB-beleid, ziet toe op de naleving ervan en rapporteert binnen de PDCA cyclus over informatiebeveiliging.

Decaan, Directeur, Directeur bedrijfsvoering

De Decanen van de faculteiten en de directeuren van de diensten zijn verantwoordelijk voor de informatiebeveiliging binnen de faculteit of dienst. Zij zorgen ervoor dat er voldoende middelen zijn om te kunnen voldoen aan de eisen van het IB-beleid, zien toe op de naleving ervan en rapporteren binnen de PDCA cyclus over informatiebeveiliging.

De inrichting van informatiebeveiliging binnen de faculteit is belegd bij de directeur bedrijfsvoering. Deze is verantwoordelijk voor het implementeren van het IB-beleid.

Centrale rollen bij de Bestuursstaf

Chief Information Security Officer

De (inhoudelijke) verantwoordelijkheid voor informatiebeveiliging is door het CvB gemandateerd aan de Chief Information Security Officer (CISO). Deze heeft de opdracht om zorg te dragen voor de informatiebeveiliging voor de gehele instelling.

De CISO is een rol op strategisch en tactisch niveau en is belegd binnen de Bestuursstaf. De CISO formuleert het IB-beleid, de kaders en de richtlijnen en ondersteunt bij een juiste vertaling daarvan

naar de instellingsonderdelen. De CISO bewaakt de uniformiteit van de informatiebeveiliging binnen de instelling en adviseert het management.

De CISO houdt binnen de UvA toezicht op de toepassing en naleving van het IB-beleid, en werkt hierbij nauw samen met de Functionaris Gegevensbescherming (FG), de Centrale Privacy Officer (CPO) en de interne Auditafdeling.

De CISO rapporteert per halfjaar via de secretaris aan het CvB.

Per kalenderjaar stelt de CISO een informatiebeveiliging-verbeterplan op. Dit plan is mede gebaseerd op de verbeteracties die zijn geïdentificeerd bij de periodieke controles, audits, incidenten, resultaten van risicoanalyses en andere initiatieven die het afgelopen jaar hebben plaatsgevonden.

De CISO is functioneel verantwoordelijk voor het Computer Emergency Response Team (CERT). Zie het CERT-charter [CERT].

Decentrale rollen bij faculteiten of diensten

Information Security Officer

De Information Security Officer (ISO)[8] bij een faculteit of dienst vervult een rol op tactisch niveau. De ISO adviseert het organisatieonderdeel en vervult een rol bij het vertalen van het IB-beleid naar tactische en operationele plannen en bij de implementatie, rapportage en evaluatie ervan. Dit doet de ISO samen met de CISO, de functionele lijnmanager en de lijnmanagers met een rol als de proces-, systeem-, of diensteigenaar.

Eigenaar van proces en systeem

De voor een proces binnen onderwijs, onderzoek en/of bedrijfsvoering verantwoordelijke persoon, hierna ‘proceseigenaar' genoemd, is verantwoordelijk voor de juiste bescherming van gegevens in het proces en in de informatiesystemen die het proces ondersteunen. De proceseigenaar heeft in overeenstemming met het IB-beleid de verantwoordelijkheid om o.a. via risicoanalyse te bepalen welke beheersmaatregelen van toepassing zijn en te evalueren of de beheersmaatregelen effectief zijn, in aansluiting met de werkwijze AO UvA en het Kader risicomanagement van de UvA. De proceseigenaar wordt bij die verantwoordelijkheid ondersteund door de Information Security Officer en systeemeigena(a)r(en) van betrokken informatiesyste(e)m(en).

De verantwoordelijke persoon voor een informatiesysteem, hierna ’systeemeigenaar' genoemd, is verantwoordelijk voor de juiste bescherming van gegevens in het informatiesysteem. De systeemeigenaar heeft in overeenstemming met dit beleid de verantwoordelijkheid voor:

- het toepassen van de eisen van het IB-beleid op dat systeem, en
- om o.a. via risicoanalyse te bepalen welke beheersmaatregelen van toepassing zijn en te evalueren of de beheersmaatregelen effectief zijn, in overeenstemming met het UvA brede Kader Risicomanagement.

De systeemeigenaar wordt bij die verantwoordelijkheid ondersteund door de Information Security Officer.

[8] De lokale governance van een faculteit of dienst kan deze rol verder onderverdelen in één of meerdere functies. Bij faculteiten ook wel de Facultaire Information Security Officer (FISO) genoemd.

Bij het ontbreken van expliciet aangewezen eigenaarschap wordt het proceseigenaarschap en/of het systeemeigenaarschap belegd in de lijn op het niveau van afdelingshoofd, directeur, decaan of secretaris.

Leidinggevende

Erop toezien dat medewerkers het IB-beleid naleven is een onderdeel van de integrale bedrijfsvoering. Iedere leidinggevende heeft de verantwoordelijkheid om:

- Ervoor te zorgen dat medewerkers op de hoogte zijn van (de voor hen relevante aspecten van) het IB-beleid.
- Erop toe te zien dat medewerkers het IB-beleid naleven.
- Het onderwerp informatiebeveiliging (op een inspirerende manier) regelmatig onder de aandacht te brengen in werkoverleggen.
- Als aanspreekpunt beschikbaar te zijn voor alle personeel-gerelateerde informatiebeveiligings-zaken.

De leidinggevende kan hierbij ondersteund worden door de Information Security Officer van de faculteit of dienst.

Medewerkers

Om een informatieveilige en digitaal weerbare organisatie te zijn, is het niet voldoende om alleen technische en organisatorische maatregelen te nemen. Het is nodig dat alle medewerkers veilig werken met de UvA-informatie(systemen). Van medewerkers wordt verwacht en gevraagd dat zij zich hiervoor inzetten. Dit is niet vrijblijvend, onveilig gedrag kan leiden tot disciplinaire maatregelen volgens de bestaande cao afspraken. Om medewerkers optimaal te faciliteren, biedt de instelling voorlichtings- en trainingsactiviteiten aan en zijn er gedragscodes geformuleerd; zie de “Regels voor verantwoord gebruik van ICT-faciliteiten” [VGF].

Bijlage A Relevante wet- en regelgeving

Deze bijlage geeft een overzicht van de belangrijkste aan informatiebeveiliging gerelateerde wet- en regelgeving met specifieke aandachtspunten voor de UvA.

1. **Wet op het Hoger onderwijs en Wetenschappelijk onderzoek (WHW)**

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)[9]. 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[10].

2. **Algemene Verordening Gegevensbescherming (AVG)**

De AVG ziet specifiek toe op de beveiliging van de verwerking van persoonsgegevens (artikel 32, AVG). Daaruit volgt dat de UvA als de verwerkingsverantwoordelijke maatregelen dient te treffen die passen bij het risico die een verwerking van persoonsgegevens met zich meebrengt. Informatiebeveiliging heeft dan ook concrete raakvlakken met de bescherming van persoonsgegevens. De aspecten beschikbaarheid, integriteit en vertrouwelijkheid van informatie zijn kernelementen van de AVG en de bescherming van persoonsgegevens die in het IB-beleid worden uitgewerkt.

3. **Wettelijke Bewaartermijnen/Archiefwet**

De UvA hanteert de bewaartermijnen die de wet voorschrijft zoals deze zijn vastgelegd in specifieke wetgeving - zoals de Belastingwet en in het arbeidsrecht - en in de Archiefwet en het Archiefbesluit. De UvA hanteert daarbij het Basisselectie document Wetenschappelijk Onderwijs van de hoger onderwijssector. Dit selectiedocument betreft alle informatie, zoals die bijvoorbeeld is vastgelegd in (gedigitaliseerde) documenten, informatiesystemen, websites en e-mail. Dit is onderdeel van de jaarlijkse externe accountantsrapportages.

4. **Intellectueel eigendom**

Dit omvat o.m. de Auteurswet en de Rijksoctrooiwet 1995. De instelling respecteert de rechten op intellectueel eigendom en handelt daarnaar.

5. **Telecommunicatiewet, Wet Netneutraliteit, cookiewet**

Omdat de doelgroep van de instelling voldoende afgebakend is, worden de netwerkvoorzieningen van de UvA *niet* aangemerkt als een openbaar netwerk in de zin van de Telecommunicatiewet. Uitzondering hierop zijn enkele voorzieningen ten behoeve van studentenhuisvesting. Hiervoor zijn procedures conform de Wet Netneutraliteit ingericht.

6. **Wet Computercriminaliteit III**

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 Wetboek van Strafrecht.

[9] Code goed bestuur (2019): https://www.universiteitenvannederland.nl/code-goed-bestuur-universiteiten
[10] Gedragscode wetenschapsbeoefening (2016): https://www.universiteitenvannederland.nl/onderwerpen/onderzoek/wetenschappelijke-integriteit

De extra artikelen houden zich bezig met:

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

Naleving van het UvA IB-beleid, met name van de beveiligingsmaatregelen en het te verwachten gedrag zorgen ervoor dat de instelling een adequaat basisniveau van beveiliging heeft tegen deze dreigingen. Indien er aanvallen op de UvA plaatsvinden die de beveiliging significant doorbreken en die vallen onder de Wet Computercriminaliteit, zal het bestuur van de instelling aangifte doen.

7. eIdas verordening

Europese verordening betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt.

8. Overige codes en landelijke afspraken

Het IB-beleid bij de UvA is gebaseerd op het SURFaudit Toetsingskader [SATK] en de instelling is deelnemer in de koepel Universiteiten van Nederland (UNL).

De instelling is in dit kader gehouden aan de volgende codes en landelijke afspraken:

- Code goed bestuur universiteiten
- Juridisch Normenkader Hoger Onderwijs
- Nederlandse gedragscode wetenschappelijke integriteit

Bijlage B Beheersmaatregelen onder verantwoordelijkheid van het CvB

De volgende informatiebeveiligingsonderwerpen hebben een impact op medewerkers en/of studenten. Om die reden valt het vaststellen ervan onder de directe verantwoordelijkheid van het College van Bestuur:

- Principes voor Informatiebeveiliging
- Autorisatiebeleid
- Werkplekbeleid
- Regels voor verantwoord gebruik van ICT-faciliteiten voor studenten
- Regels voor verantwoord gebruik van ICT-faciliteiten voor medewerkers
- Governance informatiebeveiliging

Opmerking: De volgende documenten worden *niet* meer benoemd, maar zijn bij de vorige versie van het beleid wel vastgesteld door CvB:

- Classificatierichtlijn Informatie en Informatiesystemen
- Verantwoorde openbaarmaking (responsible disclosure)

Bij een volgende update zullen deze documenten niet meer vastgesteld worden door het CvB maar door de CISO.