

Informatiebeveiligingsbeleid EP- Nuffic

Datum : 15-09-2015
Versie : 3.0
Auteur : Team ICT

Opgesteld voor:
EP-Nuffic
Vastgesteld door:
DO

Inhoudsopgave

1. Inleiding	3
1.1. Algemeen.....	3
1.2 Reikwijdte van het beleid	3
1.3 Doelstelling Informatiebeveiligingsbeleid	4
1.4. Leeswijzer	4
2. Uitgangspunten informatiebeveiliging	5
2.1. Uitgangspunten	5
2.2. Classificatie van informatie	5
2.2.1 Risicoprofiel van proces	6
2.2.2 Niveau beveiliging persoonsgegevens	6
2.2.3 Wegingsfactoren.....	7
2.3 Standaard en additionele beveiligingsmaatregelen.....	7
2.4 Structuur beveiligingsmaatregelen	8
3. Wet- en regelgeving	9
4. Organisatie Informatiebeveiligingsbeleid	10
4.1 Organisatie van de informatiebeveiligingsfunctie	10
4.1.1 Financiering van informatiebeveiliging	11
4.1.2 Bescherming van persoonsgegevens en privacy	11
4.2 Bewustwording	11
5. Beleidsprincipes ten aanzien van maatregelen.....	12
5.1 Medewerkers onmisbare schakel.....	12
5.2 Passende fysieke beveiliging	12
5.3 Correcte en veilige bediening van IT voorzieningen	12
5.4 Passende toegangsbeveiliging.....	13
5.5 Verwerving, ontwikkeling en onderhoud van informatiesystemen	13
5.6 Continuïteitsmanagement.....	13
6. Melding en afhandeling van security incidenten.....	14
7. Naleving.....	15
7.1 Lijnverantwoordelijkheid	15
7.2 Kaderstellende rol.....	15
7.3 Audits.....	15
Bijlage 1 Documenten informatiebeveiliging	16

1. Inleiding

1.1. Algemeen

Informatie is een van de belangrijkste bezittingen van EP-Nuffic en bevindt zich in allerlei systemen en sites. Het mag duidelijk zijn dat verlies of beschadiging van data grote gevolgen kan hebben. Te denken valt aan reputatieschade, verlies aan kennis en financiële schade. Om de beveiliging van informatie te optimaliseren is een goed Informatiebeveiligingsbeleid noodzakelijk.

Informatiebeveiliging is het treffen en onderhouden van een samenhangend pakket aan maatregelen om de kwaliteitsaspecten beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening te garanderen.

Het Informatiebeveiligingsbeleid is opgesteld conform het document “Informatiebeveiliging in het Hoger Onderwijs”/ CIO Beraad en SURF-ibo, dat door veel instellingen als model wordt gehanteerd. Daarnaast is de internationale standaard **ISO/IEC 27002**, zijnde de code voor informatiebeveiliging, als leidraad gebruikt. In deze standaard worden alle facetten van Informatiebeveiligingsbeleid die als “good practice” van belang zijn, benoemd en beschreven.

EP-Nuffic heeft de ambitie om met het onderhavige beleidsdocument informatiebeveiliging structureel naar een hoger niveau te brengen en daar te houden door de aspecten wet- en regelgeving, de organisatie van de beveiligingsfunctie en het Informatiebeveiligingsbeleid - ook in hun onderlinge relatie duidelijk te beschrijven, vast te stellen en te borgen.

1.2 Reikwijdte van het beleid

Dit beleid heeft betrekking op:

- De beveiliging van informatie die ontleend kan worden aan gegevensverzamelingen van EP-Nuffic (digitaal en fysiek), hieronder vallen persoonsgegevens;
- De beveiliging van de (geautomatiseerde) informatiesystemen en de beveiliging van ICT-voorzieningen van EP-Nuffic,

Ook als er sprake is van het uitbesteden van (delen van) dienstverlening (outsourcing) blijft dit beleid van toepassing. Waar applicaties en gegevens in de cloud beheerd worden gelden specifieke eisen aan clouddiensten.

Het streven is om de NESO-kantoren in de toekomst te laten voldoen aan passende maatregelen gesteld in het beleid, rekening houdend met de omvang, risico's en kosten.

Voor informatiebeveiliging worden ook eisen aan de fysieke beveiliging van de omgeving gesteld en eisen aan archief en personeel gesteld. Hoewel deze buiten de scope van dit document vallen, vormt het Informatiebeveiligingsbeleid een geïntegreerd geheel met onderstaande beleidsterreinen

- De fysieke beveiliging van de omgeving
De fysieke beveiliging betreft het voorkomen van onbevoegde fysieke toegang tot EP-Nuffic en het voorkomen van schade aan of verstoring van het terrein en de informatie van EP-Nuffic. De afdeling HRM & Services is verantwoordelijk voor de fysieke beveiliging (zie ook 5.4).
Zij organiseert de toegangsbeveiliging- en beveiliging van ruimten. Met de externe bewakingsdienst worden afspraken vastgelegd omtrent de beveiliging van het pand. Daarnaast is de afdeling HRM & Services verantwoordelijk voor preventieve maatregelen tegen brand, waterschade, inbraak, stroomstoring etc.
- Archiefbeleid
Het archiefbeleid richt zich op het in geordende en toegankelijke staat brengen van archiefbescheiden ter ondersteuning van de primaire processen. De afdeling HRM & Services is verantwoordelijk voor het Archiefbeleid.
In het archiefbeleid wordt rekening gehouden met de bescherming van

persoonsgegevens en met de vereisten uit de Archiefwet en het Archiefbesluit.

- **Personeelsbeleid**
Richt zich op het inzetten van de diverse personeelsinstrumenten om de mogelijkheden van medewerkers zo goed mogelijk te benutten.

1.3 Doelstelling Informatiebeveiligingsbeleid

Het Informatiebeveiligingsbeleid heeft als doel het beschermen van informatie van EP-Nuffic tegen mogelijke bedreigingen en beoogt daarmee de beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening te garanderen. Dit resulteert in een zoveel mogelijk ongestoorde bedrijfsvoering en dienstverlening van EP-Nuffic. Een afgeleid doel is het minimaliseren van schade als gevolg van beveiligingsincidenten. Schade kan ontstaan door verlies van informatie en apparatuur, beschadiging van ICT faciliteiten, verstoring of verlies van activiteiten als gevolg van beveiligingsincidenten en aantasting van de reputatie van EP-Nuffic.

EP-Nuffic draagt namens opdrachtgevers zorg voor de verwerking van gegevens van derden en ook deze informatie wordt zorgvuldig verwerkt en beschermd volgens het Informatiebeveiligingsbeleid.

Door vastleggen en implementeren van het Informatiebeveiligingsbeleid voldoet EP-Nuffic aan de wettelijke eisen. Daarnaast geeft het aan welke beveiligingsaspecten in contractuele verplichtingen van belang zijn

Het Informatiebeveiligingsbeleid is de grondslag voor een samenhangend pakket aan maatregelen en procedures rondom informatiebeveiliging. Het Informatiebeveiligingsbeleid is een kader om toekomstige maatregelen in de informatiebeveiliging te toetsen.

Daarnaast worden in het beleid de uitgangspunten en de organisatie rondom informatiebeveiliging vastgelegd en gedragen door het DO. Er wordt aangegeven hoe de verantwoordelijkheden, taken en bevoegdheden zijn belegd.

Het beleid wordt periodiek geëvalueerd en herzien indien maatschappelijke en organisatorische veranderingen daar aanleiding toe geven.

1.4. Leeswijzer

In hoofdstuk 2 wordt ingegaan op de uitgangspunten van het Informatiebeveiligingsbeleid, alsmede de classificatie van informatie. Classificatie is een methode om het beveiligingsniveau van door EP-Nuffic gebruikte en gemaakte informatie te bepalen.

In hoofdstuk 3 wordt omschreven aan welke wetgeving EP-Nuffic dient te voldoen (compliance).

In hoofdstuk 4 wordt de beveiligingsorganisatie geschetst met rollen en verantwoordelijkheden. Hoofdstuk 5 beschrijft de beleidsprincipes voor het opstellen van de baseline van maatregelen en het pakket van additionele maatregelen.

In hoofdstuk 6 wordt beschreven hoe EP-Nuffic omgaat met security incidenten en in hoofdstuk 7 wordt tenslotte ingegaan op de naleving van het Informatiebeveiligingsbeleid.

2. Uitgangspunten informatiebeveiliging

2.1. Uitgangspunten

De uitgangspunten voor informatiebeveiliging bij EP-Nuffic zijn:

- Informatiebeveiliging is een **continu proces**. Regelmatige herijking van beleid en audits: technologische en organisatorische ontwikkelingen binnen en buiten EP-Nuffic maken het noodzakelijk om periodiek te bezien of men nog wel op de juiste wijze bezig is de beveiliging te waarborgen.
- **Eigendom van informatie:** EP-Nuffic is als rechtspersoon eigenaar van de informatie die onder haar verantwoordelijkheid wordt geproduceerd. Daarnaast beheert EP-Nuffic informatie, waarvan het eigendom (auteursrecht) toebehoort aan derden. EP-Nuffic werkt met een Creative Commons Licentie. D.w.z. dat de informatie die EP-Nuffic publiceert op haar website en in haar publicaties, onder naamsvermelding, uitgezonderd voor commerciële doeleinden, mag worden hergebruikt door derden. Medewerkers dienen goed geïnformeerd te zijn over de regelgeving voor het (her)gebruik van informatie.
- Informatiebeveiliging is gebaseerd op **classificatie**, zie (2.2)
- Bij de aanschaf van nieuwe systemen of bij wijzigingen in systemen, wordt **vanaf de start van het project** rekening gehouden met informatiebeveiliging.

2.2. Classificatie van informatie

EP-Nuffic werkt met verschillende typen informatie zoals vertrouwelijke informatie, privacygevoelige informatie en openbare informatie. Daarbij dient EP-Nuffic zorgvuldig om te gaan met persoonsgegevens.

Vertrouwelijke- en privacygevoelige informatie dient extra beschermd te worden t.o.v. openbare informatie.

EP-Nuffic hanteert een methode om het beveiligingsniveau van door haar gebruikte en gemaakte informatie te bepalen. Zij classificeert deze informatie per proces op vereist beveiligingsniveau. Hierbij worden twee factoren gewogen:

- 1 het risicoprofiel van het proces;
- 2 het niveau voor beveiliging van persoonsgegevens (afhankelijk van soort en complexiteit/omvang van gegevensverzameling).

2.2.1 Risicoprofiel van proces

Het risicoprofiel van het proces wordt in het Auditplan vastgesteld. Onderscheiden worden een laag, midden of hoog risicoprofiel.

Processen met een groot strategisch-, financieel en/of klantbelang en/of waarin voldoen aan wet- en regelgeving en/of eisen van verslaglegging cruciaal is scoren een hoog risicoprofiel. Het risicoprofiel van de informatie gebruikt in deze processen is derhalve ook hoog. Om de processen goed uit te kunnen voeren is het beschikken over juiste, tijdige en volledige informatie immers noodzakelijk.

2.2.2 Niveau beveiliging persoonsgegevens

Het niveau voor beveiliging van persoonsgegevens wordt bepaald conform de richtlijnen van de Registratiekamer¹. De Registratiekamer onderscheidt hierin vier risicoklassen. Een risicoklasse is het product van de kans op ongewenste gevolgen en de schade die dit kan veroorzaken voor de betrokkenen. Er wordt uitgegaan van de risicoklassen Wbp:

- risicoklasse 0: publiek niveau
- risicoklasse 1: basisniveau
- risicoklasse 2: verhoogd niveau
- risicoklasse 3: hoog risico

Voor het bepalen van de risicoklasse Wbp wordt de volgende tweestapsprocedure gehanteerd:

Ten eerste bepaling van de soort informatie.

- Risicoklasse 0: openbare persoonsgegevens (bijvoorbeeld publieke internetsites, brochures)
- Risicoklasse 1: gegevens die een relatie weergeven tussen twee personen of tussen 1 persoon en een organisatie;
- Risicoklasse 2: gegevens van bijzondere aard (religie, gezondheid, politiek, strafrechtelijk, krediet of schulden);
- Risicoklasse 3: gegevens met een hoge gevoeligheidsgraad (DNA, schade voor betrokkenen, wettelijk of anderszins geheimhoudingsplicht). EP-Nuffic werkt niet met gegevens met een hoge gevoeligheidsgraad en besteedt deze verwerking ook niet uit aan derden.

Ten tweede wordt de omvang en complexiteit van de gegevensverzameling beoordeeld. Er wordt bekeken of het gaat om dan wel een verzameling van gegevens uit diverse systemen dan wel persoonsgegevens van een groot aantal personen. Indien dit het geval is dan wordt de risicoklasse met factor 1 verhoogd (dus bijv. soort informatie is risicoklasse 1, indien het gaat om een omvangrijk bestand van personen dan wordt dit verhoogd naar risicoklasse 2). Als de omvang en complexiteit laag is blijft de risicoklasse ongewijzigd.

¹ "Beveiliging van persoonsgegevens, achtergrondstudies en verkenningen AV23"

2.2.3 Wegingsfactoren

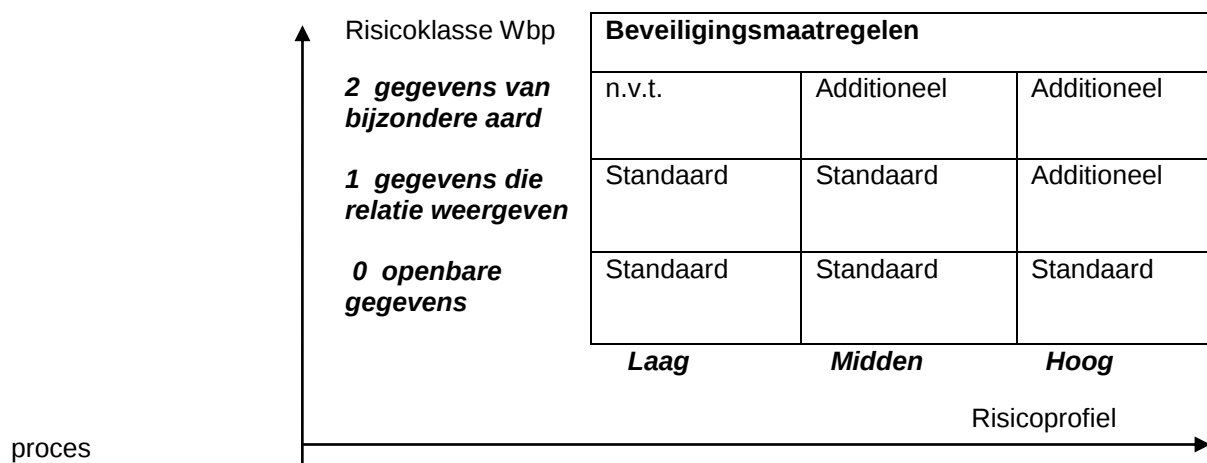
De informatie binnen EP-Nuffic wordt geclassificeerd volgens de bovengenoemde wegingsfactoren, waarbij dus twee variabelen met de volgende waarden meespelen:

Risicoprofiel proces(conform het Auditplan 2010)
Laag
Midden
Hoog

Risicoklasse Wbp
0
1
2

Per combinatie van deze twee variabelen worden “bepaald” wat het classificatieniveau is. Hiervoor is onderstaande classificatiematrix opgezet.

Figuur: Classificatiematrix



Het DO stelt de classificatie vast, waarbij de Algemeen Directeur verantwoordelijk is.

2.3 Standaard en additionele beveiligingsmaatregelen

Aan de hand van de classificatiematrix wordt het vereiste beveiligingsniveau van informatie bepaald. Hierbij wordt onderscheid gemaakt in standaardbeveiliging en additionele beveiliging.

Alle door EP-Nuffic gebruikte en gemaakte informatie wordt via een standaardpakket van maatregelen beschermd. Dit is de “baseline van maatregelen²”.

Additionele maatregelen komen bovenop de baseline van maatregelen. Het is een pakket van maatregelen dat nodig is om vertrouwelijke-, privacygevoelige- en/of bedrijfskritische informatie te beschermen. Additionele maatregelen worden vereist als een proces een hoog risicoprofiel heeft in combinatie met een hoog of “midden” niveau van beveiliging van persoonsgegevens. Ook als het risicoprofiel van het proces “midden” is, maar een hoog niveau van beveiliging van persoonsgegevens wordt vereist, is het noodzakelijk dat er additionele beveiligingsmaatregelen worden genomen.

De baseline en het pakket van additionele maatregelen zijn een aanvulling op het Informatiebeveiligingsbeleid en worden ontwikkeld door Team ICT en goedgekeurd door de DO. N.a.v. organisatorische en technische veranderingen worden de baseline en het pakket van additionele maatregelen herzien.

Tenslotte is er een beperkte set van informatie die buiten de classificatiematrix valt. Deze set gaat niet over persoonsgegevens, is vertrouwelijk en valt niet binnen een door het auditplan gespecificeerd proces. Te denken valt aan beslisdocumenten van de Raad van Toezicht,

² Zie Bijlage 1 voor verwijzing naar baseline document

welke dusdanig gevoelig zijn, dat deze ook als “kritisch” kunnen worden aangewezen. De definitie van deze set van informatie zal worden bepaald en vastgesteld door het DO. Voor het classificeren van informatie is een procedure opgesteld. Bij nieuwe informatie of nieuwe processen wordt aan de hand van deze procedure het vereiste classificatieniveau van de informatie bepaald. Periodiek wordt per proces bekeken of het al dan niet gewijzigde risicoprofiel van het proces en/of mogelijk geactualiseerde informatie aanleiding geven het proces te “herclassificeren”.

2.4 Structuur beveiligingsmaatregelen

Bij het opstellen van de maatregelen is de internationale standaard **ISO/IEC 27002**, zijnde de code voor informatiebeveiliging, als leidraad gebruikt. De maatregelen steunen op beleidsprincipes die verwoord worden in hoofdstuk 5.

De maatregelen binnen een baseline van maatregelen en een pakket van additionele maatregelen zijn van verschillende orde. Ze kunnen toezien op beveiliging van personen, omgeving, netwerken etc.

We onderscheiden de volgende categorieën maatregelen:

1. Beveiligingseisen ten aanzien van personeel
2. Maatregelen voor de fysieke beveiliging van EP-Nuffic en haar omgeving
3. Maatregelen in het beheer van communicatie- en bedieningsprocessen
4. Toegangsbeveiligingsmaatregelen
5. Beveiligingseisen voor verwerving, ontwikkeling en onderhoud van informatiesystemen
6. Continuïteitsmanagement
7. Maatregelen voor naleving

3. Wet- en regelgeving

Er wordt op de volgende wijze omgegaan met relevante wet- en regelgeving:

Wet Bescherming Persoonsgegevens

EP-Nuffic heeft de wettelijke vereisten (juistheid en nauwkeurigheid van gegevens en passende technische en organisatorische maatregelen tegen verlies en onrechtmatige verwerking) geïmplementeerd via het Informatiebeveiligingsbeleid. Naleving van de beveiligingsmaatregelen leidt tot voldoen aan de wet.

Archiefwet

EP-Nuffic heeft haar Archiefbeheer vastgelegd in een Archiefbeheerplan. Hierin wordt aangegeven op welke wijze EP-Nuffic informatie archiveert en vernietigt.

Intellectueel eigendom / Auteurswet

EP-Nuffic gaat zorgvuldig om met het intellectueel eigendom van anderen. Zij beschermt haar eigen intellectueel eigendom door passende IT maatregelen en door dit contractueel vast te leggen, waardoor een andere partij niet zomaar inbreuk kan maken op het intellectueel eigendom van EP-Nuffic.

Telecommunicatiewet

EP-Nuffic heeft maatregelen genomen ter voorkoming dat er ongevraagde e-mailberichten gestuurd worden aan derden. Daarnaast informeert EP-Nuffic gebruikers over het plaatsen van cookies en vraagt toestemming voor het plaatsen ervan.

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 organisatie en het eventueel vrijwaren van bestuurders van de organisatie.

Lokale wetgeving

Voor NESO's geldt ook lokale wetgeving.

Andere relevante documenten voor Informatiebeveiliging die EP-Nuffic hanteert zijn de Code voor Informatiebeveiliging (NEN-ISO/IEC 27001).

4. Organisatie Informatiebeveiligingsbeleid

4.1 Organisatie van de informatiebeveiligingsfunctie

In deze paragraaf wordt beschreven hoe de informatiebeveiligingsfunctie is georganiseerd, wie waarvoor verantwoordelijk is en wie welke taken uitvoert. Van belang daarbij is om onderscheid te maken naar richtinggevend of strategisch, sturend of tactisch en uitvoerend niveau. Wat betreft het strategisch niveau wordt zoveel mogelijk aangesloten bij de [Informatiemanagementorganisatie](#), d.w.z. centraal gecoördineerd informatiemanagement. De Algemeen Directeur is eindverantwoordelijk voor het Informatiebeveiligingsbeleid en stelt deze vast in het DO. Wat betreft het tactisch en uitvoerende niveau wordt de beveiligingsfunctie bij de afdelingen belegd.

De afdelingshoofden en Neso-directeuren zijn verantwoordelijk voor een goede informatiebeveiliging op hun afdeling, respectievelijk Neso-kantoor. Dit omvat ook de keuze van maatregelen en de uitvoering en handhaving ervan. De afdelingshoofden en Neso-directeuren zijn verantwoordelijk voor de administratieve organisatie. Zij dragen er zorg voor dat maatregelen en procedures blijven aansluiten op de dagelijkse praktijk. Bij wijzigingen in het stelsel van maatregelen en procedures dragen zij er zorg voor dat de beschreven administratieve organisatie wordt aangepast. De Neso-directeuren zijn verantwoordelijk voor het beheer van de lokale IT-infrastructuur. Hun verantwoordelijkheden vallen binnen de kaders van het Neso handboek. Team ICT brengt aan afdelingshoofden (of hun medewerkers) advies uit over de informatiebeveiliging, welk advies afdelingshoofden meenemen in hun besluitvorming. Op het moment dat de besluitvorming dermate dreigt af te wijken/afwijkt van het advies kan de Informatiemanager de besluitvorming voorleggen aan het DO.

Het Hoofd van Financiën & ICT is verantwoordelijk voor de beleidsvoorbereiding, ondersteuning en signalering in het kader van het Informatiebeveiligingsbeleid. Ook is deze verantwoordelijk voor het beheer van de centrale infrastructuur.

Ieder van bovengenoemde functionarissen beschikt over medewerkers waar zij taken beleggen die uit deze verantwoordelijkheden voortvloeien. Het afdelingshoofd belegt een aantal taken bij de functioneel beheerder. Deze laatste vormt een verbindende schakel tussen het afdelingshoofd, de applicatiegebruikers, leverancier en team ICT en speelt een belangrijke rol bij de informatiebeveiliging.

Informatiebeveiliging kent een multidisciplinaire benadering. Het vereist betrokkenheid- en deskundigheid van medewerkers, functioneel beheerders, Team ICT, Team JZI, Team FZ en Afdeling HRM en Services.

Hierna volgt een overzicht van medewerkers met uitvoerende taken in het kader van het Informatiebeveiligingsbeleid. Taken betrokken bij uitvoering en bij de controle daarop worden niet door dezelfde medewerkers uitgevoerd (functiescheiding).

Niveau	Functie	Taken
Strategisch	Informatiemanager	Stelt het Informatiebeveiligingsbeleid op en herzielt dit in de toekomst
Tactisch/ Uitvoerend	Financieel adviseur	Stelt het auditbeleid op.
Uitvoerend	Auditors (intern en extern)	Auditors toetsen processen op Informatiebeveiligingscriteria of voeren de audit op de ICT infrastructuur uit.
Uitvoerend	Neso medewerker	De Finance & Operations Officer van Neso-kantoren zijn aanspreekpunt voor de Security manager
Uitvoerend	Functioneel beheerder	Voert het autorisatie-, gebruiks- en wijzigingsbeheer uit en past de standaard- en additionele beveiligingsmaatregelen toe op de applicaties in zijn/haar beheer.

Niveau	Functie	Taken
Uitvoerend	Security manager	Adviseert over baseline- en additionele maatregelen en rapporteert de voortgang aan de teamcoördinator van Team ICT. Verantwoordelijk voor de afhandeling van security incidenten en rapporteert hierover.
Uitvoerend	Jurist	Beoordeelt of Wbp van toepassing is en meldt gegevensverwerkingen aan CBP. Aanspreekpunt voor verwerking van persoonsgegevens binnen EP-Nuffic en is verantwoordelijk voor voorlichting hieromtrent
Uitvoerend	Medewerkers	Verantwoordelijk voor alle aspecten van beveiliging met betrekking tot de eigen functie
Uitvoerend	Externe beheerorganisatie	Voert de beveiliging uit en rapporteert aan de proceseigenaar en de Security manager.

4.1.1 Financiering van informatiebeveiliging

Algemene zaken, zoals het opstellen van het Informatiebeveiligingsbeleid en een interne/externe audit op EP-Nuffic ICT infrastructuur, worden uit het centrale BV-budget betaald. De beveiliging en decentrale audits van informatiesystemen komen ten laste van het afdelings- of projectbudget.

4.1.2 Bescherming van persoonsgegevens en privacy

Onder het verwerken van persoonsgegevens worden alle handelingen verstaan die met persoonsgegevens kunnen worden verricht, van het verzamelen tot aan het vernietigen. De activiteiten voor beveiliging van persoonsgegevens dienen in de dagelijkse werkzaamheden van de betrokken medewerkers te zijn verankerd. EP-Nuffic meldt de verwerking van persoonsgegevens aan het College Bescherming Persoonsgegevens (CBP). EP-Nuffic heeft een informatieplicht jegens de betrokkenen van wie de persoonsgegevens worden verwerkt. Daarnaast is Juridische Zaken het aanspreekpunt voor vragen over verwerking van persoonsgegevens.

Als EP-Nuffic de verwerking van persoonsgegevens uitbesteedt aan een bewerker dient deze hetzelfde passende niveau van beveiliging te garanderen als EP-Nuffic en de persoonsgegevens niet anders te gebruiken dan voor de uitvoering van de overeenkomst. EP-Nuffic maakt hiertoe afspraken met gegevensbewerkers en ook de door EP-Nuffic gehanteerde Algemene Rijksvoorwaarden bij IT-overeenkomsten (ARBIT voorwaarden) zien hierop toe.

4.2 Bewustwording

EP-Nuffic medewerkers dienen goed bekend te worden gemaakt met het Informatiebeveiligingsbeleid en relevante procedures. De medewerkers vormen vaak onbewust de meest kritische schakels in de beveiligingsketen, wat een risico kan vormen voor de uitvoering van het beleid. Het DO en afdelingshoofden dienen zich daarom duidelijk achter dit beleid op te stellen, een voorbeeldfunctie te vervullen en medewerkers te informeren en te motiveren om dit beleid actief uit te voeren.

De afdelingshoofden zijn verantwoordelijk voor het bewustzijn van hun medewerkers rondom informatiebeveiliging en dat hun medewerkers werken conform de beveiligingseisen.

Uiteraard heeft de medewerker ook een eigen verantwoording voor de beveiliging van informatie en het signaleren van onvolkomenheden in de beveiliging van informatie. Een ieder die met vertrouwelijke gegevens werkt dient zich bewust te zijn van zijn of haar geheimhoudingsplicht. Deze geheimhoudingsplicht is vastgelegd in het arbeidscontract, doordat daarin de CAO van toepassing is verklaard, waarin de geheimhoudingsplicht is opgenomen (art. 1.16 CAO).

5. Beleidsprincipes ten aanzien van maatregelen

Voor het opstellen van de procedures rondom informatiebeveiliging, baseline van maatregelen en het pakket van additionele maatregelen worden de onderstaande beleidsprincipes gehanteerd (zie ook 2.3 en 2.4).

5.1 Medewerkers onmisbare schakel

De informatiebeveiliging kan in technische en fysieke zin optimaal georganiseerd zijn, maar als medewerkers onzorgvuldig omgaan met (vertrouwelijke) informatie is de beveiliging niet waterdicht. Medewerkers en ingehuurd personeel dienen hun verantwoordelijkheid te nemen in het beveiligen van informatie. Het bewustzijn van medewerkers op elk niveau in de organisatie over de noodzaak van beveiliging is de belangrijkste voorwaarde om dit Informatiebeveiligingsbeleid goed te laten functioneren. Daarom is het van belang medewerkers goed te blijven instrueren over hun taken en verantwoordelijkheid. Een medewerker kan geen twee taken vervullen die onverenigbaar zijn als het gaat om beveiligingsaspecten. Waar nodig dienen functies te worden gescheiden en vervuld door verschillende personen, uitgewerkt in een goed ingerichte AO.

5.2 Passende fysieke beveiliging

Informatie moet niet alleen in technische- en organisatorische zin beveiligd zijn, er is ook een passende fysieke beveiliging noodzakelijk. Er is een goed toegangsbeheer en er wordt door de receptie gecontroleerd wie het gebouw binnenkomt. Zo wordt voorkomen dat onbevoegden toegang kunnen krijgen tot informatie en informatiesystemen. Er wordt bepaald welke ruimten worden afgesloten en bepaald wie toegang tot welke ruimtes heeft. Ruimten waar ITvoorzieningen staan, welke kritieke of gevoelige informatie ondersteunen, worden beveiligd. De medewerker heeft een eigen verantwoordelijkheid voor het afsluiten van kasten, kamers en het leeg achterlaten van zijn bureau.

Daarnaast worden voorzorgsmaatregelen genomen ter bescherming van het gebouw, ruimten en daarin aanwezige informatie tegen de gevolgen van brand, waterschade, inbraak, stroomstoring etc. Hiervoor is het van belang het beveiligingsbewustzijn bij medewerkers te verhogen.

De afdeling HRM & Services is verantwoordelijk voor het toegangsbeheer en controle en voor de bescherming van het gebouw en informatie tegen genoemde schadelijke invloeden. Team ICT stelt maatregelen op om de IT infrastructuur en IT apparatuur te beschermen. Zie hiervoor de baseline van maatregelen.

5.3 Correcte en veilige bediening van IT voorzieningen

Via IT voorzieningen zoals interne en externe netwerken en systemen wordt veel informatie verspreid. Deze IT voorzieningen dienen veilig bediend en beheerd te worden.

EP-Nuffic maakt gebruik van clouddiensten. Clouddiensten zijn software-, platforms- of infrastructuurdiensten die op aanvraag via het internet beschikbaar gesteld worden. Deze diensten zijn makkelijk schaalbaar, afhankelijk van de behoefte van de klant. Clouddiensten kenmerken zich door meerdere grote datacenters zodat de continuïteit van diensten gewaarborgd is en de diensten aan meerdere klanten kunnen worden aangeboden.

Clouddiensten vereisen een aantal specifieke beveiligingsmaatregelen.

Medewerkers gaan veiliger met IT voorzieningen om, als hun taken en verantwoordelijkheden op dit vlak duidelijk zijn en ze zich bewust zijn van hun rol. Daarnaast is het van belang dat er procedures en bedieningsinstructies zijn voor het beheer en bediening van de IT-voorzieningen. Dat deze goed bekend en toegankelijk zijn en zijn bijgewerkt. Daarnaast dient het transport van informatiedragers voldoende te zijn beveiligd door medewerkers, eventueel in samenspraak met de Afdeling HRM & Services.

Medewerkers zijn zich bewust dat ze het netwerk niet belasten met virussen die voortkomen uit onverantwoordelijke acties of ongeautoriseerde programmatuur.

De IT voorzieningen worden degelijk beheerd en beschermd tegen virussen en ongewenste e-mail. Team ICT werkt daartoe met firewalls en een “DeMilitarized netwerk zone”. Virussen worden gedetecteerd, preventief verwijderd en de voorziening wordt hersteld na een aanval

van virussen. Routinebackups voorkomen dat informatie verloren gaat. Deze backups worden versleuteld en op een veilige plaats volgens afgesproken termijn bewaard. EP-Nuffic heeft een spambeleid zodat zij voldoet aan de vereisten uit de Telecomwet en haar klanten niet onnodig lastigvalt met ongewenste e-mail en cookies. Team ICT spant zich in om de ontvangst van spam door medewerkers te verminderen. Alle nieuwe software zal eerst geïnstalleerd worden in een testomgeving zodat eventuele risico's voor de productie worden geminimaliseerd. De beveiliging van IT voorzieningen is gebaseerd op classificatie van informatie. Indien bepaalde informatie additioneel moet worden beveiligd zullen bij het testen fictieve persoonsgegevens worden gebruikt. Hiermee worden persoonsgegevens beschermd bij onderhoud door derden.

5.4 Passende toegangsbeveiliging

De toegang tot informatie, IT-voorzieningen en bedrijfsprocessen is op basis van behoefte, beveiligingsniveaus en classificatie van informatie. EP-Nuffic wil voorkomen dat onbevoegden toegang krijgen tot informatie, IT-voorzieningen en bedrijfsprocessen en zij wil bewerkstelligen dat bevoegden gestructureerd toegang krijgen tot benodigde informatie. Er wordt gedefinieerd hoe een passende toegangsbeveiliging wordt gerealiseerd en geborgd. Aan de hand van een autorisatiematrix wordt per informatiesysteem bepaald welke gebruiker welke bevoegdheden heeft. Wachtwoorden dienen aan eisen te voldoen. Functies behoren expliciet te worden gescheiden om het risico van nalatigheid of opzettelijk misbruik van IT-voorzieningen te verminderen. Indien informatie additioneel moet worden beveiligd is sprake van aanvullende eisen t.a.v. gebruikersidentificatie, het loggen van toegang en het achteraf kunnen aantonen van de rechtmatigheid van overgedragen bevoegdheden.

5.5 Verwerving, ontwikkeling en onderhoud van informatiesystemen

Bij de koop en ontwikkeling van informatiesystemen/software is het van belang dat beveiliging integraal deel uitmaakt van informatiesystemen/software. Beveiligingseisen moeten worden vastgesteld tijdens de specificatie van de eisen voor het project en behoren te worden verantwoord, overeengekomen en gedocumenteerd. Daarnaast dient voorafgaande aan de productiefase een systeem/software te worden getest op het voldoen aan de beveiligingseisen. Bij wijzigingen in het systeem/software dient te worden onderzocht of het systeem/software nog steeds voldoet aan de beveiligingseisen. Om informatie te beschermen is het van belang dat in- en uitvoergegevens worden gevalideerd. In procedures voor het aangaan van nieuwe contracten, testmanagement en wijzigingenbeheer vormen de beveiligingseisen een vast onderdeel. Leveranciers van informatiesystemen moeten zich contractueel aan de beveiligingseisen houden, waarop de systeemeigenaar toeziet en de leverancier eventueel aanspreekt.

5.6 Continuïteitsmanagement

EP-Nuffic wil onderbrekingen in de bedrijfsvoering tegengaan en haar kritische processen beschermen tegen gevolgen van omvangrijke storingen. Het kan hier gaan om onvoorziene calamiteiten zoals ernstige computerstoringen, brand of waterschade. Continuïteitsmanagement is gerelateerd aan het auditbeleid. In het Auditplan wordt periodiek vastgesteld in welke mate processen kritisch zijn. De beoordeling van processen en het vereiste beveiligingsniveau van persoonsgegevens worden gewogen en resulteren in een standaard- of additioneel beveiligingsniveau van informatie. EP-Nuffic wil risico's gestructureerd identificeren, risico's verminderen en de consequenties beperken van incidenten die schade toebrengen. Dit houdt o.a. in dat informatiebeveiligingsincidenten beheerd worden, waardoor tijdig corrigerende maatregelen genomen kunnen worden (zie hoofdstuk 6). Er wordt een continuïteitsplan voor de ICT-infrastructuur ontwikkeld, welke een plan bevat voor herstel van de infrastructuur en gegevensverwerking na calamiteiten. In voorkomende gevallen dienen de oorzaak, de gevolgen en de getroffen maatregelen schriftelijk te worden vastgelegd. Het continuïteitsplan moet goed bekend zijn.

6. Melding en afhandeling van security incidenten

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

Het is van belang om te leren van security incidenten. Incidentregistratie en periodieke rapportage over opgetreden incidenten horen thuis in een goede informatie beveiligingsomgeving. Er is daarom een meldpunt ingericht bij de Security manager. Elke medewerker is verantwoordelijk voor het signaleren van incidenten en inbreuken op informatiebeveiliging en zwakke plekken in de informatiebeveiliging. De medewerker is verplicht incidenten en inbreuken te melden bij het Afdelingshoofd en de Security manager.

De incidenten worden door de Security manager geregistreerd. De incidenten worden afgehandeld in nauw overleg met de betrokkenen en de proceseigenaar. Besluitvorming door de proceseigenaar vindt plaats met in achtname van het advies van ICT, het belang van de business en de voorgestelde kosten. De besluitvorming mbt acties wordt gedocumenteerd. De incidenten dienen als input voor de incident-rapportages, waarover in het operationeel overleg wordt gesproken. Bij constatering van bepaalde trends kan hierop meteen worden ingespeeld, bijvoorbeeld door het nemen van extra maatregelen.

7. Naleving

7.1 Lijnverantwoordelijkheid

De afdelingshoofden zijn verantwoordelijk dat hun medewerkers werken conform de beveiligingseisen. Informatiebeveiliging behoort, waar relevant, een onderdeel te zijn in werkoverleg en functioneringsgesprekken. De afdelingshoofden spreken hun medewerkers aan in geval van tekortkomingen en nemen passende disciplinaire maatregelen indien een medewerker het Informatiebeveiligingsbeleid schendt of zich niet houdt aan de geheimhoudingsplicht (artikel 1.16 CAO Nederlandse Universiteiten). Medewerkers die werken met vertrouwelijke en privacygevoelige informatie behoren zich bewust te zijn van hun verantwoordelijkheid. De functioneel beheerders faciliteren de informatiebeveiliging. Ze controleren via de autorisatiematrix of bevoegdheden correct zijn toegekend en bewaken en controleren de gegevensintegriteit van de processen.

7.2 Kaderstellende rol

De afdeling Financiën en ICT vervult een kaderstellende rol en houdt toezicht op de naleving van de eisen voortvloeiend uit het Informatiebeveiligingsbeleid, baseline, additionele maatregelen en verwante procedures. Met name ook de bevordering van de naleving van de Wet Bescherming Persoonsgegevens.

7.3 Audits

De implementatie van de informatiebeveiliging wordt ook onafhankelijk beoordeeld. Om er zeker van te zijn dat de praktijk overeenkomt met het voorgesteld beleid en dat de maatregelen uitvoerbaar zijn en het beoogde effect hebben, maakt EP-Nuffic gebruik van interne en externe security auditors.

Twee verschillende type interne audits zijn relevant voor informatiebeveiliging:

1. Audit voor het beheer van de IT infrastructuur
2. Andere audits naar de primaire en ondersteunende processen van EP-Nuffic

Ad 1. De audit voor het beheer van de IT infrastructuur is een security audit welke toetst of de centrale infrastructuur conform de baseline maatregelen en het pakket van additionele maatregelen wordt beheerd. Het incidentbeheer (Team ICT-helpdesk) en wijzigingenbeheer vormen hiervan een onderdeel. Deze audit wordt opgenomen in het Auditplan en uitgevoerd in opdracht van de directeur Bedrijfsvoering, als gedelegeerd opdrachtgever van de Algemeen Directeur.

Het betreffende proces heeft een risicofactor "Midden", wat betekent dat de audit tweejaarlijks wordt gehouden. Vanwege het technische specialistische karakter zal deze over het algemeen worden uitbesteed. De rapportage, besluitvorming en opvolging vinden plaats conform het reguliere auditproces (zie Auditplan en Mavim).

Ad 2. Beheersmaatregelen van informatiebeveiliging worden geïntegreerd in de reguliere procesgerichte audits, omschreven in het Auditplan. Informatie(beveiliging) vormt immers een integraal onderdeel van processen. Bij een additioneel beveiligd proces vindt aan het begin van een project een risicoanalyse plaats. Op basis hiervan wordt bepaald in hoeverre een externe audit gewenst is en welke scope geldt.

In het normenkader voor audits naar processen worden de informatie beveiligingscriteria (beheersmaatregelen) opgenomen waaraan de auditor toetst. Eventueel worden externe security auditors ingeschakeld voor de beoordeling van ICT aspecten in bepaalde processen, op initiatief en kosten van de proceseigenaar. De auditor en Informatiemanager coördineren de opdrachtverstrekking aan deze externe security audits in overleg met de proceseigenaar. Het auditproces verloopt verder conform de procesbeschrijving in mavim en het Auditplan. De audits voor informatie beveiliging worden zoveel mogelijk geïntegreerd in de normale Planning & Control cyclus. De auditor adresseert zijn bevindingen aan de gedelegeerd opdrachtgever en de implementatie van de bevindingen wordt gemonitord in de viermaandelijke managementrapportages.

Bijlage 1 Documenten informatiebeveiliging

In het kader van informatiebeveiliging kent EP-Nuffic de volgende documenten:

1. Informatiebeveiligingsbeleid

Het Informatiebeveiligingsbeleid wordt in concept opgesteld door Team ICT. De DO stelt het vast. De actuele versie van dit document is beschikbaar via Mavim. Naar aanleiding van maatschappelijke- en organisatorische veranderingen kan het Informatiebeveiligingsbeleid worden herzien.

2. Baseline van maatregelen (basisniveau maatregelen).

Deze baseline beschrijft de maatregelen die in de dagelijkse praktijk minimaal nodig zijn om een basis niveau van informatiebeveiliging te kunnen waarborgen. Dit vloeit voort uit het beleid of uit besluiten die door het tactisch overleg genomen zijn. Deze basis maatregelen dienen dus organisatiebreed genomen te worden.

3. Pakket van additionele maatregelen

Dit pakket van maatregelen wordt bovenop de baseline van maatregelen genomen. Het is een pakket van maatregelen welke nodig is om vertrouwelijke, privacygevoelige of bedrijfskritische informatie te beschermen.