

Informatiebeveiligingsbeleid Nuffic

Datum : 11-07-2018
Versie : 1.0

Opgesteld voor:
Nuffic

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. Risico-gebaseerde benadering.....	Fout! Bladwijzer niet gedefinieerd.
2.3 Standaard en additionele beveiligingsmaatregelen.....	6
2.4 Structuur beveiligingsmaatregelen	6
3. Wet- en regelgeving.....	7
4. Organisatie Informatiebeveiligingsbeleid	8
4.1 Organisatie van de informatiebeveiligingsfunctie	8
4.1.1 Strategisch niveau	8
4.1.2 Tactisch en uitvoerend niveau.....	8
4.1.3 Afwijken van beleid of maatregelen.....	8
4.1.4 Functies en taken	9
4.1.5 Financiering van informatiebeveiliging	10
4.1.6 Bescherming van persoonsgegevens en privacy	10
4.2 Bewustwording	10
5. Beleidsprincipes ten aanzien van beveiligingsmaatregelen	11
5.1 Medewerkers onmisbare schakel	11
5.2 Passende fysieke beveiliging	11
5.3 Veilige afname van ICT diensten.....	11
5.4 Correcte en veilige bediening van IT voorzieningen	12
5.5 Passende toegangsbeveiliging	12
5.6 Verwerving, ontwikkeling en onderhoud van informatiesystemen	12
5.7 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 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.

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 Nuffic (digitaal en fysiek), hieronder vallen persoonsgegevens;
- De beveiliging van de (geautomatiseerde) informatiesystemen en de beveiliging van ICT-voorzieningen van Nuffic,

Ook als er sprake is van het uitbesteden van (delen van) dienstverlening (outsourcing) blijft dit beleid van toepassing en blijft Nuffic verantwoordelijk voor de manier waarop de dienstverlener omgaat met informatiebeveiliging.

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 bescherming van persoonsgegevens, 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 Nuffic en het voorkomen van schade aan of verstoring van het terrein en de informatie van Nuffic. Team HR & facility management is verantwoordelijk voor de fysieke beveiliging (zie ook 52). Zij organiseert de toegangsbeveiliging- en beveiliging van ruimten en camera toezicht bij de entrees. Met de externe bewakingsdienst worden afspraken vastgelegd omtrent de beveiliging van het pand. Daarnaast is team HR & facility management verantwoordelijk voor preventieve maatregelen tegen brand, waterschade, inbraak, stroomstoring etc.

- Bescherming van persoonsgegevens
Het persoonsgegevensverwerkingsbeleid heeft als doel om de kwaliteit van de Verwerking en de beveiliging van Persoonsgegevens te optimaliseren, waarbij een goede balans moet worden gevonden tussen privacy, functionaliteit en veiligheid.
- Archiefbeleid
Het archiefbeleid richt zich op het in geordende en toegankelijke staat brengen van archiefbescheiden ter ondersteuning van de primaire processen. Team HR & facility management 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 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 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 Nuffic.

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 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 MT. 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 waaronder een risico-gebaseerde benadering. In hoofdstuk 3 wordt omschreven aan welke wetgeving 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 beveiligingsmaatregelen. In hoofdstuk 6 wordt beschreven hoe 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 Nuffic zijn:

- Informatiebeveiliging is een **continu proces**. Regelmatige herijking van beleid en audits: technologische en organisatorische ontwikkelingen binnen en buiten 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:** Nuffic is als rechtspersoon eigenaar van de informatie die onder haar verantwoordelijkheid wordt geproduceerd. Daarnaast beheert Nuffic informatie, waarvan het eigendom (auteursrecht) toebehoort aan derden. Nuffic werkt met een Creative Commons Licentie. D.w.z. dat de informatie die 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.
- een **risico-gebaseerde benadering voor informatiebeveiliging** , zie (2.2)
- Nuffic blijft verantwoordelijk voor de betrouwbaarheid (beschikbaarheid, integriteit en vertrouwelijkheid) van uitbestede diensten.
- Bij de aanschaf van nieuwe systemen of bij wijzigingen in systemen, wordt **vanaf de start van het project** rekening gehouden met informatiebeveiliging.

2.2. Risico-gebaseerde benadering

Informatiebeveiliging is gebaseerd op een risico-gebaseerde benadering.

Dit komt voort uit de Algemene Verordening Gegevensbescherming en sluit aan bij het in 2017 geïntroduceerde strategisch risico management.

Deze "risico-gebaseerde benadering" heeft als doel dat risico's beheerst en verkleind worden, dat van ervaringen geleerd wordt en dat de kwaliteit van de dienst/applicatie én maatregelen verbetert.

Voorafgaand aan een nieuwe dienst/applicatie houdt de kernopdracht/team een risico analyse. Hierin worden de grootste risico's benoemd en gekoppeld aan een eigenaar.

De functioneel beheerders en projectleiders nemen passende beveiligings- en privacy maatregelen om deze risico's te beheersen.

De security officer en JZ toetsen vervolgens de resultaten van de risico analyse aan het Informatiebeveiligingsbeleid en de beveiligings- en privacy maatregelen.

Tenslotte besluit de budgethouder welke maatregelen worden genomen.

Indien van beleid en/of maatregelen wordt afgeweken dient de werkwijze als beschreven in hoofdstuk 4 gevolgd.

Bedrijfsvoering stelt een risico analyse instrument beschikbaar voor het uitvoeren van risico analyses bij nieuwe diensten/applicaties. De Functioneel beheerders en business developers hebben een training gehad in het houden van risico analyses, waaronder Privacy impact assessments. Kernopdrachten/teams kunnen hun risico's en genomen maatregelen in dit risico analyse instrument vastleggen en evalueren.

2.3 Standaard en additionele beveiligingsmaatregelen

Aan de hand van de risico analyse wordt het vereiste beveiligingsniveau van informatie bepaald. Hierbij wordt onderscheid gemaakt in standaardbeveiliging en additionele beveiliging. Alle door Nuffic gebruikte en gemaakte informatie wordt via een standaardpakket van maatregelen beschermd. Dit is de "baseline".

Additionele maatregelen komen bovenop de baseline.. als uit de risico analyse blijkt dat er grote risico's met een nieuwe dienst/application gepaard gaan. De standaard en additionele beveiligingsmaatregelen zijn een aanvulling op het Informatiebeveiligingsbeleid en worden ontwikkeld door Team ICT in samenspraak met de functioneel beheerders en inkoopers en goedgekeurd door het MT. N.a.v. organisatorische en technische veranderingen worden de beveiligingsmaatregelen herzien.

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. Eveneens is uit onderstaande normenkaders en documenten geput:

- NEN-ISO/IEC27001 (nl), "Managementsystemen voor informatiebeveiliging - Eisen",
- Cloud Security Alliance (CSA), "The Notorious Nine: Cloud Computing Top Threats in 2013",
- NCSC beveiligingsrichtlijnen voor web applicatie
- Cloud Computing Compliance Controls Catalogue (C5), 2016
- Cloud Controls matrix version 3.01.1

De maatregelen steunen op beleidsprincipes die verwoord worden in hoofdstuk 5.

De indeling van de maatregelen is in kolommen waardoor de maatregelen kunnen worden gefilterd al naar gelang de beveiligingsgraad, de dienstverlener, scope en of er een certificering is voor betreffende norm.

Hieronder volgen de kolommen:

- Hoofdonderwerp
- Korte code (verwijst naar nieuw toegevoegde maatregelen)
- Onderwerp
- Maatregel
- Baseline beveiligd
- Additioneel beveiligd
- Scope beveiliging: intern/eter
- Verschillende ICT diensten als:
 - Hosting en Infrastructuur as a Service (IAAS) en Technisch beheer. Samengenomen is dat Platform as a Service (PaaS)
- Applicatiebeheer. Samengenomen met IaaS en PaaS heet dat Software as a Service (SaaS)
- Maatwerk (ontwikkeling)
- Interne hosting
- Degenen die bij Nuffic verantwoordelijk zijn voor het afdwingen van de maatregelen
- Door welke ISO certificering de norm wordt afgedekt. Als de dienstverlener zich jaarlijks hierop laat certificeren, dan hoeft niet aan de dienstverlener te worden uitgevraagd of deze hieraan voldoet.
- Ruimte voor opmerkingen
- Voldoet dienst aan maatregel? (ja/ne), ter beoordeling van Team ICT
- Ruimte voor vragen aan dienstverlener voor toetsing van het voldoen aan beveiligingsmaatregelen
- Motivering (van dienstverlener) of hij/zij wel/niet aan de maatregel voldoet.

3. Wet- en regelgeving

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

Algemene Verordening Gegevensbescherming

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. Nuffic sluit Verwerkersovereenkomsten af met haar dienstverleners. Bewaartermijnen voor persoonsgegevens worden per team/Kernopdracht gemotiveerd en vermeld in een overzicht.

Archiefwet

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

Intellectueel eigendom / Auteurswet

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 Nuffic.

Telecommunicatiewet

Nuffic heeft maatregelen genomen ter voorkoming dat er ongevraagde e-mailberichten gestuurd worden aan derden. Daarnaast informeert 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 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.

4.1.1 Strategisch niveau

Wat betreft het strategisch niveau wordt aangesloten op het Besturingsmodel van Nuffic, op de Informatiemanagementorganisatie, d.w.z. centraal gecoördineerd informatiemanagement en op Strategisch risico management.

De Bestuurder is eindverantwoordelijk voor het Informatiebeveiligingsbeleid en stelt het vast in het MT.

4.1.2 Tactisch en uitvoerend niveau

Wat betreft het tactisch en uitvoerende niveau wordt de beveiligingsfunctie bij de teams belegd. De proceseigenaren zijn verantwoordelijk voor het handhaven van het juiste beveiligingsniveau van (uitbestede) diensten.

De teamleiders, MT-leden, Neso-directeuren en Chief representative officers zijn verantwoordelijk voor een goede informatiebeveiliging in respectievelijk hun team, kernopdracht en Neso-kantoor. Dit omvat ook de keuze van maatregelen en de uitvoering en handhaving ervan. De teamleiders, MT-leden, Neso-directeuren en Chief representative officers 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 en Chief representative officers zijn verantwoordelijk voor het beheer van de lokale IT-infrastructuur. Hun verantwoordelijkheden vallen binnen de kaders van het Neso handboek. Team ICT en Functioneel beheerders brengen op verzoek aan teamleiders/MT leden (of hun medewerkers), aan Neso-directeuren en Chief representative officers advies uit over de informatiebeveiliging. Dit advies nemen de genoemde verantwoordelijken mee in hun besluitvorming.

Alvorens een dienst/applicatie in gebruik wordt genomen toetsen de security officer en JZ de dienst/applicatie op veiligheid.

Indien de security officer en JZ van mening zijn dat er op belangrijke punten wordt afgeweken van het Informatiebeveiligingsbeleid en de maatregelen, escaleren zij dat aan de Manager Bedrijfsvoering. Deze neemt contact op met de betreffende opdrachtgever in het team/kernopdracht

4.1.3 Afwijken van beleid of maatregelen

Bij een gewenste afwijking vanuit de kernopdracht van het Informatiebeveiligingsbeleid en/of de beveiligings- en privacy maatregelen/normen geeft de kernopdracht onderbouwd aan waarom ze willen afwijken. De kernopdracht vraagt advies over het eventueel afwijken van deze normen/maatregelen en de risico's daarvan voor de Nuffic bij de security officer en Juridische Zaken. De manager van de kernopdracht neemt op basis van het advies en de risico's het besluit wel of niet af te wijken. Mochten er uit de analyse van Juridische Zaken en de security officer grote risico's voor Nuffic aan deze afwijkingen kleven wordt de Manager bedrijfsvoering geïnformeerd en deze kijkt samen met security officer en Juridische Zaken en met de teamleiders van JZ/ICT naar de risico's. Ze bepalen of de risico's ook zo groot zijn dat de bestuurder moet worden geïnformeerd van het besluit van de kernopdracht. Afwijkingen worden daarna opgenomen in het afwijkingen register door een verantwoordelijke binnen de kernopdracht.

4.1.4 Functies en taken

Team 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.

De teamleider/ MT-lid belegt een aantal taken bij de functioneel beheerder. Deze laatste vormt een verbindende schakel tussen de teamleider/ MT-lid, 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 Team HR & facility management.

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 Tactisch	Informatiemanager	Stelt het Informatiebeveiligingsbeleid op en herziert dit in de toekomst
Tactisch/ Uitvoerend	Teamleider Finance & Control	Faciliteert strategisch risico management.
Uitvoerend	Auditors (intern en extern)	Auditors toetsen processen op Informatiebeveiligingscriteria of voeren de audit op de ICT infrastructuur uit.
Niveau	Functie	Taken
Uitvoerend	Neso medewerker	De Financial & Operational Officer (FOO) en education promotion officer van Neso-kantoren zijn aanspreekpunt voor de security officer
Uitvoerend	Functioneel beheerder	Voert het autorisatie-, gebruiks- en wijzigingsbeheer uit en past de beveiligingsmaatregelen toe op de applicaties in zijn/haar beheer. Adviseert en rapporteert aan de proceseigenaar over informatiebeveiliging.
Uitvoerend	security officer	Adviseert over informatiebeveiliging en rapporteert de voortgang aan de teamcoördinator van Team ICT. Verantwoordelijk voor de afhandeling van security incidenten en rapporteert hierover.
Uitvoerend	Jurist en JZ	Beoordeelt of Algemene Verordening Gegevensbescherming van toepassing is. Adviseert over verwerking van persoonsgegevens binnen Nuffic en is verantwoordelijk voor voorlichting hieromtrent

Uitvoerend	Medewerkers	Verantwoordelijk voor alle aspecten van beveiliging met betrekking tot de eigen functie
Uitvoerend	Externe (ICT)dienstverleners	Voert de beveiliging uit en rapporteert aan de proceseigenaar en functioneel beheerder.

4.1.5 Financiering van informatiebeveiliging

BV betaalt voor het opstellen van het Informatiebeveiligingsbeleid en een interne/externe audit op Nuffic ICT infrastructuur en Nuffic brede security audits., Teams en kernopdrachten betalen voor beveiliging en decentrale audits van hun diensten en systemen..

4.1.6 Bescherming van persoonsgegevens en privacy

Nuffic beschermt de persoonsgegevens van haar klanten en medewerkers zorgvuldig. Er worden niet meer persoonsgegevens verzameld dan voor het doel nodig zijn en persoonsgegevens worden veilig verwerkt, bewaard en tijdig vernietigd. Medewerkers worden geïnformeerd over hun verantwoordelijkheden bij het verwerken van persoonsgegevens. 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 Nuffic de verwerking van persoonsgegevens uitbesteedt aan een Verwerker dient deze hetzelfde passende niveau van beveiliging te garanderen als Nuffic en de persoonsgegevens niet anders te gebruiken dan voor de uitvoering van de overeenkomst. Nuffic sluit Verwerkersovereenkomsten met Verwerkers in aanvulling op de Algemene Rijksvoorwaarden bij IT-overeenkomsten (ARBIT voorwaarden) en Algemene Rijksvoorwaarden voor het verstrekken van opdrachten tot het verrichten van diensten (ARVODI voorwaarden). Nuffic komt met Verwerkers overeen dat Verwerkers diezelfde verplichtingen met hun subverwerkers overeenkomen.

4.2 Bewustwording

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 MT, teamleiders, Team ICT en Functioneel beheerders dienen zich daarom duidelijk achter dit beleid op te stellen. Teamleiders/MT-leden vervullen een voorbeeld functie en informeren en motiveren medewerkers om dit beleid actief uit te voeren. De teamleiders/MT-leden zijn verantwoordelijk voor het bewustzijn van hun medewerkers rondom informatiebeveiliging en dat hun medewerkers werken conform de beveiligingsmaatregelen. Team ICT informeert medewerkers over informatiebeveiliging, houdt periodiek awareness sessies en kan security awareness tests laten uitvoeren.

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 beveiligingsmaatregelen

Voor informatiebeveiligingsmaatregelen 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 vanaf hun inwerkperiode goed te blijven instrueren over hun taken en verantwoordelijkheid en periodiek een security awareness test te houden

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 en eventueel met camerabeveiliging 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 IT voorzieningen 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.

Team HR & facility management 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 beveiligingsmaatregelen.

5.3 Veilige afname van ICT diensten

Nuffic maakt gebruik van software-, platforms- of infrastructuurdiensten die op aanvraag via het internet beschikbaar gesteld worden. Deze diensten zijn makkelijk schaalbaar, afhankelijk van de behoefte van Nuffic. Een proceseigenaar laat een risico analyse uitvoeren alvorens een ICT dienst van enige omvang via Internet kan worden afgenomen. Hierin worden de risico's geïdentificeerd en beoordeeld. Hierbij wordt rekening gehouden met de waarde en gevoeligheid van de informatie en de mogelijke gevolgen voor Nuffic wanneer de beschikbaarheid, integriteit en vertrouwelijkheid van deze informatie worden aangetast. Medebepalend voor de beslissing om een dienst via Internet af te nemen is dat gegevens binnen de Europese Unie worden opgeslagen. Het initiatief om advies te vragen ligt bij een team/kernopdracht. Team ICT geeft een go/no go advies op de afname afhankelijk van de veiligheids en continuïteitsrisico's. Een proceseigenaar maakt vervolgens een afgewogen keuze waarin het advies van Team ICT wordt meegenomen. proceseigenaren nemen de beveiligingsmaatregelen, niveau van dienstverlening en het melden van security incidenten in overeenkomsten met deze dienstverleners op. De dienstverlener dient voldoende inzicht te verschaffen in hoe zij aan de vermelde maatregelen voldoet. De wijze

waarop de dienstverlener invulling geeft aan bepaalde maatregelen kan van invloed zijn op de bedrijfsvoering van Nuffic.

5.4 Correcte en veilige bediening van IT voorzieningen

Door veilig beheer en correcte bediening van IT voorzieningen wordt de informatie van Nuffic goed beschermd. 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 het team HR & facility management.

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.

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.

5.5 Passende toegangsbeveiliging

De toegang tot informatie, IT-voorzieningen en bedrijfsprocessen is op basis van behoefte, beveiligingsniveaus en een risico-gebaseerde benadering.

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.

5.6 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. Beveiligingsmaatregelen 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 beveiligingsmaatregelen. Bij wijzigingen in het systeem/software dient te worden onderzocht of het systeem/software nog steeds voldoet aan de beveiligingsmaatregelen. 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

beveiligingsmaatregelen een vast onderdeel. Leveranciers van informatiesystemen moeten zich contractueel aan de beveiligingsmaatregelen houden, waarop de systeemeigenaar toeziet en de leverancier eventueel aanspreekt.

5.7 Continuïteitsmanagement

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.

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). Nuffic en externe dienstverleners hebben een continuïteitsplan voor de ICT-infrastructuur, 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 en dienstverleners gemeld worden en de wijze waarop deze worden afgehandeld. Dit is uitgewerkt in de procedure Afhandeling security incidenten. Als bij het security incident persoonsgegevens zijn betrokken kan het tevens een datalek zijn. De beoordeling en afhandeling van een datalek zijn uitgewerkt in de procedure melden datalek.

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 officer.

Elke medewerker is verantwoordelijk voor het signaleren van incidenten en inbreuken op informatiebeveiliging en zwakke plekken in de informatiebeveiliging. De medewerker is verplicht incidenten inbreuken en vermoedelijke datalekken te melden bij de leidinggevende en de security officer. De dienstverlener is contractueel verplicht om incidenten, inbreuken en vermoedelijke datalekken te melden bij zijn/haar contactpersoon en de security officer van Nuffic.

De incidenten worden door de security officer 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 over acties wordt gedocumenteerd. De incidenten dienen als input voor periodieke rapportages, welke met teamleider ICT besproken worden.

Bij constatering van bepaalde trends kan hierop meteen worden ingespeeld, bijvoorbeeld door het nemen van extra maatregelen.

7. Naleving

7.1 Lijnverantwoordelijkheid

De teamleiders/ MT-leden zijn verantwoordelijk dat hun medewerkers werken conform de beveiligingsmaatregelen. Informatiebeveiliging behoort, waar relevant, een onderdeel te zijn in werkoverleg en functioneringsgesprekken. De teamleiders/ MT-leden 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

Het team ICT vervult een kaderstellende rol en houdt toezicht op de naleving van de eisen voortvloeiend uit het Informatiebeveiligingsbeleid, beveiligingsmaatregelen en verwante procedures.

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 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 Nuffic

Ad 1. De audit voor het beheer van de IT infrastructuur is een security audit welke toetst of de centrale infrastructuur conform de beveiligingsmaatregelen Nuffic wordt beheerd. Het incidentbeheer (Team ICT-helpdesk) en wijzigingenbeheer vormen hiervan een onderdeel. Deze audit uitgevoerd in opdracht van de Manager Bedrijfsvoering, als gedelegeerd opdrachtgever van de Bestuurder.

Vanwege het technische specialistische karakter zal deze over het algemeen worden uitbesteed. Er vindt rapportage, besluitvorming en opvolging van de geconstateerde zaken plaats.

Ad 2. Beveiligings- en privacymaatregelen worden geïntegreerd in interne en externe audits. Informatie(beveiliging) en privacy vormen immers een integraal onderdeel van processen. Aan het begin van een project/dienst/applicatie vindt een risicoanalyse plaats. Op basis hiervan wordt bepaald in hoeverre een externe of interne audit gewenst is en welke scope geldt. Een externe audit vindt plaats op initiatief en kosten van de opdrachtgever van een project/dienst/applicatie. Het team/kernopdracht coördineert de opdrachtverstrekking hiervoor. De audits voor informatiebeveiliging en privacy worden zoveel mogelijk geïntegreerd in de normale Planning & Control cyclus. De auditor toetst op het Informatiebeveiligingsbeleid en de beveiligings- en privacy maatregelen en adresseert zijn bevindingen aan de opdrachtgever en aan de security officer en JZ. De implementatie van de bevindingen wordt gemonitord in periodieke managementrapportages.

Bijlage 1 Documenten informatiebeveiliging

In het kader van informatiebeveiliging kent Nuffic de volgende documenten:

1. Informatiebeveiligingsbeleid

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

2. Beveiligings- en privacymaatregelen Nuffic

Deze bestaat uit baseline maatregelen en additionele maatregelen.

Baseline maatregelen zijn in de dagelijkse praktijk minimaal nodig 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 baseline maatregelen dienen dus organisatie breed genomen te worden.

Additionele maatregelen worden boven op de baseline maatregelen genomen. Het is een pakket van maatregelen welke nodig is om vertrouwelijke, privacygevoelige of bedrijfskritische informatie te beschermen.