Informatiebeveiligingsbeleid Havenbedrijf Rotterdam N.V.

Document beheer

Datum	Versie	Aangepast door	Wijzigingen
17-02-2014	0.6	Marijn van Schoote	Verwerken opmerkingen architecten, informatie managers en SMO
27-10-2014	0.91	Marijn van Schoote	Verwerken opmerkingen MT IV
02-03-2015	0.99	Marijn van Schoote	Verwerken opmerkingen Paul Smits
15-04-2015	1.00	Marijn van Schoote	Goedgekeurde versie

Document distributie

Datum	Versie	Naam	Organisatie / functie
19-02-2014	0.6	Jean Nijsten Frank Borsboom	HbR / Directeur HR HbR / Hoofd Facilties
24-10-2014	0.9	MT IV	HbR
27-10-2014	0.91	Frank Borsboom	HBR / Faclities
02-02-2015	0.91	Paul Smits	HBR / CFO

Document goedkeuring

Datum	Versie	Naam	Organisatie
14-04-2015	1.0	Directie team	Havenbedrijf Rotterdam

Classificatie

Openbaar

Inhoudsopgave

1 Voorwoord

Het Havenbedrijf Rotterdam N.V. (Havenbedrijf) heeft de ambitie om de haven van Rotterdam verder te ontwikkelen als Europese haven van wereldklasse en deze positie naar de toekomst toe te behouden en te verstevigen. In het ondernemingsplan staat de onderstaande missie centraal:

Het Havenbedrijf Rotterdam ontwikkelt in partnership de Europese haven van wereldklasse.

Op basis van deze missie zijn strategische doelstellingen geformuleerd die aangeven wat het Havenbedrijf de komende jaren wil bereiken. Deze strategische doelstellingen zijn leidend voor de IT strategie en de noodzakelijke best-in-class informatievoorziening van het Havenbedrijf.

Deze informatievoorziening en het correct functioneren van de informatiesystemen zijn van essentieel belang voor de bedrijfsvoering van het Havenbedrijf. Zonder betrouwbare informatievoorziening kan de veilige afhandeling van het scheepvaartverkeer nauwelijks worden gerealiseerd of kan de veiligheid van personen en de omgeving in gevaar worden gebracht.

Verder speelt informatie een belangrijke rol in de ‘Ease of doing business’. Informatie in de haven is een onderscheidende factor ten opzichte van concurrerende havens. Het delen en beschikbaar stellen van informatie stelt alle bij de haven betrokken partijen in staat om efficiënter zaken met elkaar te kunnen doen.

Beveiligingsincidenten kunnen een grote negatieve impact hebben op de reputatie van het Havenbedrijf, kunnen leiden tot aanzienlijke schade, een afname van vertrouwen door het bedrijfsleven, sancties door regelgevers, en mogelijke juridische claims (rechtsvorderingen) van klanten.

De enige manier om de gewenste mate van beveiliging en flexibiliteit in de informatievoorziening te bewerkstelligen, is om een afgewogen stelsel van beveiligingsmaatregelen te implementeren. Het proces van informatiebeveiliging en risicomanagement begint met het definiëren van beleid op dit onderwerp. Dit beleid is in het onderhavige document integraal vastgelegd voor informatiebeveiliging, privacy en bedrijfscontinuïteit en is door de directie van het Havenbedrijf vastgesteld.

Met dit beleid geven wij als directie van het Havenbedrijf een duidelijke richting aan en demonstreren dat wij informatiebeveiliging ondersteunen en handhaven.

Paul Smits

Chief Financial Officer
Havenbedrijf Rotterdam N.V.

2 Doelstellingen

De strategische doelstellingen van het Havenbedrijf en de IT doelstellingen zijn richtinggevend voor het informatiebeveiligingsbeleid.

De doelstelling van het informatiebeveiligingsbeleid is om bij te dragen aan een haven van wereldklasse door het Havenbedrijf weerbaar te maken en te houden tegen dreigingen in de digitale wereld, het borgen van de continuïteit en betrouwbaarheid van de ICT systemen en de vertrouwelijkheid van informatie.

Het doel van het informatiebeveiligingsbeleid is het vastleggen van de uitgangspunten met betrekking tot het veilig en vertrouwelijk omgaan met informatie binnen het Havenbedrijf. Het informatiebeveiligingsbeleid waarborgt - als een continu bedrijfsproces - dat risico's verbonden aan het gebruik en verwerken van informatie en persoonsgegevens worden onderkend, voorkomen en verminderd. Het uitgangspunt hierbij is om niet te verbieden, maar het faciliteren van veilige oplossingen.

De informatievoorziening en het correct functioneren van de informatiesystemen zijn van essentieel belang voor de integriteit en continuïteit van de bedrijfsvoering van het Havenbedrijf, en daarmee onderdeel van de 'license to operate' van het HbR. Bovendien kunnen beveiligingsincidenten een hoge negatieve impact hebben op de reputatie van het Havenbedrijf, leiden tot aanzienlijke financiële of reputatieschade, een afname van vertrouwen door het bedrijfsleven, sancties door regelgevers, en mogelijke juridische claims (rechtsvorderingen) van klanten.

2.1 Definitie van informatiebeveiliging

Informatiebeveiliging wordt als volgt gedefinieerd: *Het samenhangend stelsel van maatregelen dat zich richt op het blijvend realiseren van een optimaal niveau van beschikbaarheid, integriteit en vertrouwelijkheid van informatie*. Informatiebeveiliging is daarmee het geheel van maatregelen, richtlijnen en procedures voor informatie en informatiesystemen, gericht op het waarborgen van het in bedrijf zijn van de informatiesystemen en het minimaliseren van schade. Informatie heeft hierbij betrekking op alle verschijningsvormen zoals papier, digitaal of mondeling. Informatiebeveiliging spitst zich toe op drie kernbegrippen: *beschikbaarheid* (de mate waarin informatie en systemen op het gewenste moment toegankelijk zijn voor gebruikers of andere systemen), *vertrouwelijkheid* (de mate waarin de toegang tot informatie en systemen beperkt is tot een vastgestelde groep van gebruikers of systemen) en *integriteit* (de mate waarin informatie en systemen geen fouten bevatten).

Naast deze kernbegrippen gaat informatiebeveiliging ook over de *controleerbaarheid* en *onweerlegbaarheid* van uitgevoerde handelingen en de informatieverwerking. Het onafhankelijk kunnen aantonen dat informatie betrouwbaar wordt behandeld, het afleggen van verantwoording en zorgdragen dat misstanden kunnen worden ontdekt, zijn aspecten die onlosmakelijk zijn verbonden met informatiebeveiliging.

Informatiebeveiliging is een *samenhangend stelsel* van maatregelen. Dit betekent dat de verschillende maatregelen die tezamen de informatiebeveiliging vormen niet los van elkaar worden getroffen, maar in onderlinge relatie met elkaar staan. Het stelsel van beveiligingsmaatregelen heeft tot doel een *blijvend niveau van beveiliging* te realiseren. Door een zorgvuldige borging wordt bereikt dat het gewenste niveau van beveiliging ook op langere termijn blijft gehandhaafd. Daarnaast is informatiebeveiliging gericht op het realiseren van een *optimaal niveau van beveiliging.* Dit optimum wordt bereikt door een zorgvuldige afweging van kosten en baten.

2.2 Structuur, reikwijdte en geldigheid

De structuur van het informatiebeveiligingsbeleid volgt de ISO27001 standaard waarmee de organisatie van informatiebeveiliging binnen het Havenbedrijf, de verantwoordelijkheden en de uitgangspunten worden vastgelegd.

Het informatiebeveiligingsbeleid heeft een belangrijke relatie en een gedeeltelijke overlap met aanpalende beleidsterreinen, zoals safety (ARBO- en milieuwetgeving), fysieke beveiliging en business continuity.

Het informatiebeveiligingsbeleid geldt voor alle onderdelen van het Havenbedrijf, voor zowel medewerkers, gastmedewerkers, inhuurkrachten als (medewerkers van) externe leveranciers.

Indien bij samenwerking met derden sprake is van uitwisseling van informatie, waarvan het Havenbedrijf eigenaar of beheerder is, dient informatiebeveiliging een onderdeel van de samenwerkingsovereenkomst te zijn en is deze niet strijdig met het informatiebeveiligingsbeleid.

Het beleid is locatie onafhankelijk. Indien een medewerker werkzaamheden verricht op een locatie die niet tot het Havenbedrijf behoort maar waarbij men wel met informatie of informatievoorzieningen van het Havenbedrijf werkt, dient men dit beleid te respecteren.

Dit informatiebeveiligingsbeleid wordt vastgesteld voor een periode van 3 jaar. Dit beveiligingsbeleid heeft daarmee betrekking op de periode 2015 – 2018.

3 Organisatie van informatiebeveiliging

3.1 De Algemene directie

De Algemene directie stelt het informatiebeveiligingsbeleid vast en is (eind-) verantwoordelijk. Binnen de Algemene directie heeft de CFO informatiebeveiliging in zijn portefeuille. De CFO heeft de bevoegdheden die nodig zijn voor het uitvoeren van het beleid gedelegeerd aan het Hoofd Informatievoorziening (beheer informatiesystemen en onderliggende IT infrastructuren) en het Hoofd Facilities (beheer van telefonie, marifonie, radar en het archief).

3.2 Lijnmanagement

Het lijnmanagement, bestaande uit afdelingshoofden, managers en teamleiders, is verantwoordelijk voor de inrichting en uitvoering van de primaire en secundaire bedrijfsprocessen. De verantwoordelijkheid voor de bedrijfsprocessen omvat ook de beveiliging van de informatie en de ICT-infrastructuur waarvan het organisatieonderdeel eventueel zelf eigenaar is. De verantwoordelijkheid van het lijnmanagement omvat onder andere:

- positieve en actieve houding ten aanzien van informatiebeveiliging;
- fungeren als voorbeeldfunctie;
- classificeren van informatie;
- toezicht houden op de naleving van beveiligingsmaatregelen;
- medewerking verlenen aan verbeteracties;
- autoriseren van medewerkers;
- toezien op de eventueel noodzakelijke screening van medewerkers;
- informatiebeveiliging behandelen in werkoverleg, beoordelingen etc.;
- jaarlijks uitvoeren van een zelfstandige beoordeling (self assessment);
- afhandelen van beveiligingsincidenten;
- rapporteren van alle beveiligingsincidenten.

3.3 Hoofd informatievoorziening (CIO)

Het Hoofd Informatievoorziening is verantwoordelijk voor de instandhouding van de centrale geautomatiseerde informatievoorziening. Dit heeft op vele onderdelen raakvlakken met informatiebeveiliging. Zij/hij is als lijnmanager, samen met de overige leden van het Management Team van de IV-organisatie, verantwoordelijk voor de beveiliging van de centrale ICT-infrastructuur. De hoofd IV is verantwoordelijk voor:

- het opzetten en onderhouden van een overeengekomen niveau van informatiebeveiliging t.b.v. het Havenbedrijf;
- het leveren en onderhouden van een veilige IT-infrastructuur t.b.v. het Havenbedrijf;
- goedkeuren van belangrijke initiatieven met betrekking tot informatiebeveiliging en investeringen;
- jaarlijks uitvoeren van een zelfstandige beoordeling (self assessment);
- toezien op de naleving van het informatiebeveiligingsbeleid door (ICT) leveranciers;
- rapportage van significante situaties van niet-naleving aan het senior management.

Verder gelden de verantwoordelijkheden zoals opgesomd in de paragraaf lijnmanagement.

3.4 Hoofd Facilities

Het Hoofd Facilities is verantwoordelijk voor de implementatie en onderhoud van de vastgestelde beveiligingseisen en -maatregelen binnen kantoren en locaties van het Havenbedrijf evenals over de bijbehorende communicatie over deze fysieke beveiliging. Deze eisen en maatregelen dragen bij aan het gewenste niveau van informatiebeveiliging. Het hoofd Facilities is verantwoordelijk voor

- de inhuur en het functioneren van particuliere beveiligingsorganisaties en overige (fysieke) security & safety gerelateerde partijen, die in- en uitgaande (bedrijfs) goederen en afvalstromen, bouwkundige, installatietechnische en overige gebouw gerelateerde voorzieningen,
- de functionele eisen voor het juist gebruik en uitvoering van technische beveiligingsinstallaties, facility- en gebouwbeheerssystemen van de bij het Havenbedrijf in gebruik zijnde gebouwen.
- zorgdragen voor het onderhouden, ontwikkelen en uitvoering van het beveiligingsbeleid en –maatregelen.

Verder is het Hoofd Facilities verantwoordelijk voor de instandhouding van de telefonie, marifonie en radarketen (operationele systemen). Dit heeft op vele onderdelen raakvlakken met informatiebeveiliging. Zij/hij is als lijnmanager, samen met de overige leden van het Management Team van de Facilities-organisatie, verantwoordelijk voor de beveiliging van deze operationele diensten. Het hoofd Facilities is verantwoordelijk voor:

- het opzetten en onderhouden van een overeengekomen niveau van informatiebeveiliging voor de operationele systemen (telefonie, marifonie en radar) t.b.v. het Havenbedrijf;
- goedkeuren van belangrijke initiatieven met betrekking tot informatiebeveiliging en investeringen;
- jaarlijks uitvoeren van een zelfstandige beoordeling (self assessment);
- toezien op de naleving van het informatiebeveiligingsbeleid door leveranciers van operationele diensten
- rapportage van significante situaties van niet-naleving aan de algemene directie.

Verder gelden de verantwoordelijkheden zoals opgesomd in de paragraaf lijnmanagement.

3.5 Directeur Human Resources

De directeur Human Resources is verantwoordelijk voor het ontwikkelen en implementeren van beveiligingseisen en -criteria voor het selectiebeleid van nieuwe medewerkers, de opzet van een privacyreglement en ontwikkeling van het Arbo beleid alsmede voor de bijbehorende communicatie daarover. Binnen de eigen competentiegebieden wordt zorg gedragen voor het onderhouden, ontwikkelen en uitvoering van het beveiligingsbeleid, met name daar waar de verantwoordelijkheden elkaar overlappen, zoals binnen de individuele arbeidsovereenkomsten gerelateerde verplichtingen voor de medewerker zoals geheimhoudingsverklaringen. Ook wordt toegezien dat nieuwe medewerkers worden geïnformeerd over de omgang met beveiligingsprocedures en het gebruik van bedrijfsmiddelen.

Verder gelden de verantwoordelijkheden zoals opgesomd in de paragraaf lijnmanagement.

3.6 Information Security & Risk Officer

Het Havenbedrijf heeft een Information Security & Risk Officer aangesteld. Deze onderhoudt het informatiebeveiligingsbeleid en adviseert zowel het Havenbedrijf als het verantwoordelijke lijnmanagement over beveiligingsvraagstukken. De Information Security & Risk Officer is verantwoordelijk voor het opstellen en uitdragen van het beleid op het gebied van informatiebeveiliging en ziet toe op de uitvoering hiervan.

De Information Security &Risk Officer rapporteert aan het Hoofd Informatievoorziening, maar kan zich in uitzonderlijke gevallen rechtstreeks tot de algemene directie wenden.

Het onderhouden van contacten met speciale belangengroepen en specialistische platforms voor beveiliging en professionele organisatie is de verantwoordelijkheid van de Information Security & Risk Officer.

3.7 Eigenaar

Aan alle systemen en bedrijfsmiddelen worden aan een eigenaar toegekend. Van alle informatiesystemen wordt vastgelegd wie de eigenaar is en welke verantwoordelijkheden er gelden qua organisatie en handhaving van de bijbehorende beheersmaatregelen. Deze eigenaar is verantwoordelijk voor:

- Het bepalen van de classificatie van de kernapplicatie;

- De functionaliteit die de kernapplicatie biedt. Dit wordt zichtbaar in het maken van keuzes t.a.v. over nut en noodzaak van wijzigingen in de functionaliteit van de applicatie.
- De treffen van (niet technische) beveiligingsmaatregelen om de beschikbaarheid, integriteit en vertrouwelijkheid te borgen, zoals het geven van toestemming tot toegang tot de kernapplicatie en het periodiek controleren van toegangsrechten in de kernapplicatie.

De verantwoordelijkheid voor specifieke beheersmaatregelen kan door de eigenaar worden gedelegeerd, maar de eigenaar blijft verantwoordelijk voor een goede bescherming hiervan. De systeemeigenaar levert op verzoek informatie aan de Information Security & Risk Officer.

3.8 Beheerders

Naast de hiervoor genoemde functionarissen hebben beheerders van informatie en ICT-middelen elk hun eigen verantwoordelijkheid op het gebied van informatiebeveiliging. Deze beheerders bevindingen zich bij de afdeling Informatievoorziening, Facilities en Asset Management. In bijlage 1 zijn de beheerders per bedrijfsmiddel opgenomen. Ter ondersteuning van de door hen uit te voeren taken zijn hun middelen en bevoegdheden toegekend.

Aan het gebruik van deze middelen en bevoegdheden is de verantwoordelijkheid verbonden voor een deugdelijk beheer. Iedere beheerder is daarom verantwoordelijk voor alle aspecten van beveiliging binnen de eigen invloedsfeer.

Voor beheerders liggen de verantwoordelijkheden vast in beheerprocedures. De Information Security & Risk Officer adviseert de beheerders bij het opstellen van beheerprocedures.

Externe dienstverleners die voor of namens het Havenbedrijf informatie beheren zijn verplicht inzicht te geven in hun beheerprocedures. Dit wordt contractueel vastgelegd.

3.9 Medewerkers

Iedere medewerker, al dan niet in vast dienstverband bij het Havenbedrijf c.q. een derde die namens een andere rechtspersoon in opdracht van Havenbedrijf (deel) taken uitoefent, is verplicht om de regels en richtlijnen na te leven die voortvloeien uit het beveiligingsbeleid. De verantwoordelijkheden voor medewerkers zijn in de “Bedrijfscode Havenbedrijf Rotterdam N.V.” vastgelegd.

Voor posities binnen het Havenbedrijf waarbij toegang tot geheime informatie of de bediening van kritische bedrijfsprocessen vereist is, wordt bij de selectie van kandidaten een verificatie uitgevoerd, zoals van referenties, of een formele screening indien noodzakelijk.

Iedere gebruiker is persoonlijk verantwoordelijk voor de wijze waarop deze omgaat met informatie en overige bedrijfsmiddelen. Dit impliceert dat een medewerker verantwoordelijk is voor alle onder zijn user-id (account) uitgevoerde handelingen en dat deze zijn password beslist niet aan anderen kenbaar mag maken.
Tevens is iedere medewerker verplicht om (potentiële) inbreuken op het gebied van beveiliging zo spoedig mogelijk te melden bij de Servicedesk van het Havenbedrijf en/of de daartoe aangewezen verantwoordelijke functionaris binnen het Havenbedrijf.

Het Havenbedrijf heeft een formeel disciplinair beleid geïmplementeerd in overeenstemming met lokale wet- en regelgeving. Indien een medewerker inbreuk pleegt op het informatiebeveiligingsbeleid en/of gebruiksregels zal in overleg met direct leidinggevende en de directeur Human Resources een disciplinaire maatregel worden opgelegd.

3.10 Derde partijen

Derde partijen moeten contractueel verantwoordelijk worden gesteld voor het veilig uitvoeren van gedelegeerde taken. Deze verantwoordelijkheid is controleerbaar via periodieke rapportages.

Voor externe partijen die toegang nodig hebben tot de informatie en IT voorzieningen van de organisatie wordt een risico beoordeling uitgevoerd om de beveiligingsimplicaties en de beheersmaatregelen te bepalen. De overeenstemming over het stelsel te treffen beheersmaatregelen wordt vastgelegd in een overeenkomst met de externe partij.

4 Het informatiebeveiligingsraamwerk

Het informatiebeveiligingsraamwerk kent drie niveaus: strategisch, tactisch en operationeel. Het onderhavige informatiebeveiligingsbeleid vult het strategisch niveau in en beschrijft de doelstelling, organisatie en de uitgangspunten.

Het informatiebeveiligingsbeleid is uitgewerkt in een informatiebeveiligingsplan. In dit plan zijn de fysieke, personele, organisatorische en ICT maatregelen vastgelegd die afkomstig zijn vanuit wet- en regelgeving en relevante richtlijnen. Deze richtlijnen omvatten de NEN-ISO 27002 Code voor Informatiebeveiliging en richtlijnen van het Nationaal Cyber Security Centrum.
Per maatregel is een omschrijving vastgelegd en – indien noodzakelijk – aanvullende instructies voor de realisatie van de maatregel. Dit resulteert in een Havenbedrijf generiek informatiebeveiligingsplan en een generiek bedrijfscontinuïteitsplan. Samen vormen zij het basisbeveiligingsniveau voor het Havenbedrijf.

Onder coördinatie van de Information Security & Risk Officer worden de maatregelen geïmplementeerd. De status en voortgang van de realisatie alsmede de adequate werking van het informatiebeveiligingsplan wordt ieder kwartaal door de Information Security & Risk Officer gerapporteerd aan het Hoofd Informatievoorziening.

Op operationeel niveau wordt verder invulling gegeven aan de maatregelen zoals ze in het informatiebeveiligingsplan niveau zijn vastgelegd. Deze invulling kan bijvoorbeeld bestaan uit procedurebeschrijvingen, werkinstructies, (functionele en technische) documentatie of concrete standaarden om de implementatie, uitvoering en instandhouding van de maatregelen mogelijk te maken.

5 Beveiligingsuitgangspunten

Informatiebeveiliging is als een proces ingericht. Dat houdt in dat de jaarlijkse planning en controlecyclus, gebaseerd is op ISO 27001 (Plan, Do, Check, Act). Hierin worden jaarplannen opgesteld en uitgevoerd. De resultaten ervan worden geëvalueerd en vertaald naar nieuwe jaarplannen.

Het Havenbedrijf heeft als doel om haar informatiebeveiliging op een niveau te brengen en te houden dat passend is bij een grote wereldhaven die een belangrijk onderdeel is van de vitale infrastructuur van Nederland. Dit passende niveau is - op de internationale Capability Matury Model schaal van 1 (laag) tot 5 (zeer hoog) - vastgesteld op niveau 4 (hoog).

Voor de operationele processen die zorgdragen voor de afhandeling van het scheepsvaartverkeer binnen de divisie Havenmeester is 24 x7 beschikbaarheid een vereiste. Dit betekent dat de processen een hoge mate van weerstand en veerkracht moeten bieden tegen cyberaanvallen.

De risico management strategie sluit aan op de Havenbedrijf brede benadering van informatiebeveiliging, en luidt:

Het Havenbedrijf is terughoudend in het nemen van risico's, hierbij ligt de focus op het aanpakken van kwetsbare plekken in de organisatie, bij het personeel, de fysieke omgeving en de technische ICT systemen.

5.1 Risico gebaseerde aanpak

De te nemen beveiligingsmaatregelen ten aanzien van informatie worden bepaald op basis van een risico-inschatting.. Alleen als een bepaalde situatie zich kan voordoen en hierbij een dusdanige schade kan veroorzaken dat de gevolgen niet-acceptabel zijn, worden beveiligingsmaatregelen getroffen. Het te realiseren en te handhaven informatiebeveiligingsniveau is dus niet een kwestie van louter implementeren van bepaalde voorgeschreven maatregelen. Risico's worden bepaald en gewogen om kostenbewust effectieve en efficiënte beveiligingsmaatregelen te nemen die concreet bijdragen aan het invullen van de doelstellingen van het Havenbedrijf.

5.2 Normenkader

Ten aanzien van de informatiebeveiliging, privacy, bedrijfscontinuïteit en de verwerking van persoonsgegevens zijn de volgende regelgeving en normenkaders van toepassing:

- NEN-ISO/IEC 27001 - Informatietechnologie - Managementsystemen voor informatiebeveiliging – Eisen

- NEN-ISO/IEC 27002 - Informatietechnologie - Code voor informatiebeveiliging
- NEN-ISO 7131 Managementsystemen voor veiligheid, voorbereiding op incidenten en continuïteit - World Economic Forum - Partnering for Cyber Resilience Guidelines
- ISO 22301 Business Continuity Management – Managementsystemen voor bedrijfscontinuïteit
- Wet Bescherming Persoonsgegevens (Wbp)

5.3 Beveiligingsarchitectuur

De beveiligingsmaatregelen voor het omgaan met informatiebeveiliging resulteren in een security architectuur. In deze architectuur zijn de doelstellingen en het beleid van het Havenbedrijf vertaald naar beveiligingsontwerpen. Hierin is zichtbaar hoe beveiligingssystemen samenhangen en wat de impact van een wijziging op een deelsysteem is. De security architectuur vormt hiermee een onderdeel van de informatie architectuur van het Havenbedrijf.