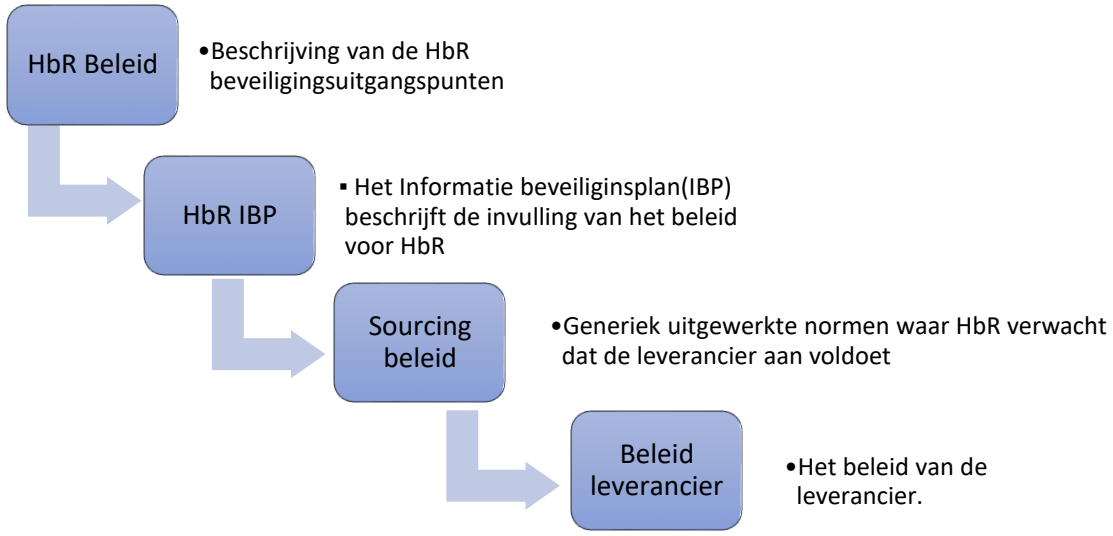
Inleiding:

Het Havenbedrijf Rotterdam hecht waarde aan de informatie van haar klanten, zakelijke partners en werknemers en behandelen deze met gepaste zorgvuldigheid. Het Havenbedrijf wil informatie-veiligheidsrisico's vermijden en is verantwoordelijk voor in de operationele processen, systemen en projecten ingebedde informatiebeveiliging beheersmaatregelen, zodat de continuïteit en de veiligheid van de informatie is geborgd. Het Havenbedrijf Rotterdam verwacht van haar leveranciers deze zelfde mate van zorgvuldigheid. Om dit te realiseren heeft het Havenbedrijf Rotterdam dit sourcingsbeleid opgesteld.

Hiermee vormt dit sourcingsbeleid een verbindende factor tussen het HbR beleid, informatiebeveligingsplan (IBP) en het beleid van de leverancier.

De opbouw voor het gehele kader als volgt weergegeven worden:



Het sourcing beleid richt zich op de globale uitgangspunten per categorie, zoals deze beschreven zijn in het IBP. Dit zijn de volgende categorieën:

1. Basisuitgangspunten
2. Classificatie van informatie en risico’s
3. Personele beveiliging
4. Toegangsbeveiliging
5. Beheer van communicatie en bedieningsprocessen
6. Beheer van informatiebeveiligingsincidenten
7. Bedrijfscontinuïteitsbeheer

De maatregelen hebben betrekking op de beschikbaarheid, integriteit, vertrouwelijkheid en authenticiteit van de netwerk- en informatiesystemen van de leverancier waar HbR de diensten van afneemt.

1 Basisuitgangspunten

De basisuitgangspunten zijn van toepassing op alle diensten die de leverancier levert aan HbR. De uitbestedende partij blijft verantwoordelijk voor de betrouwbaarheid en veiligheid van uitbestede diensten. Hieronder valt onder meer, maar niet uitsluitend het personeel, de IT-voorzieningen, gebouwen, informatie van de leverancier.

De leverancier moet ten aanzien van de geleverde ICT-diensten en beheerprocessen voldoen en zijn gecertificeerd conform de ISO 27001 norm voor informatiebeveiliging.

De leverancier dient op verzoek van HbR een van gecertificeerde audit rapportages o.b.v. de ISO 27001/15118 of andere op het domein relevante security standaarden welke conformiteit aantoont.

De leverancier beschikt over een actueel, gedocumenteerd en door haar management geaccordeerde risicoanalyse, uitgevoerd voor de te leveren ICT- of autonome voertuigdiensten. Bij deze risicoanalyse moeten de bedreigingen voor de bedrijfsmiddelen, kwetsbaarheden en de invloeden op de organisatie zijn vastgesteld en het bijbehorende risiconiveau te zijn bepaald.

De leverancier maakt aantoonbaar dat het hoogste niveau van cybersecurity, welke binnen de organisatie van toepassing is, wordt toegepast en nageleefd voor de gehele CER dienstverlening.

HbR heeft het recht om naast de opgeleverde audits tevens (op eigen kosten) door onafhankelijke derden een audit te laten uitvoeren. Indien er afwijkingen worden geconstateerd op de afgesproken dienstverlening zijn de kosten voor de leverancier.

HbR heeft het recht om penetratie testen uit te laten voeren (op eigen kosten) door onafhankelijke derden partijen. Indien er afwijkingen worden geconstateerd op de afgesproken dienstverlening zijn de kosten voor zowel het onderzoek alsook de herstelkosten voor de leverancier.

De leverancier stelt resources beschikbaar om deel te nemen aan security afstemming, evaluaties binnen HbR.

2 Classificatie van informatie en risico’s

Het doel van de Classificatie van informatie en risico’s is het bereiken en handhaven van een adequate bescherming van de bedrijfsmiddelen. Conform de ISO-definitie is een bedrijfsmiddel alles dat waarde heeft voor een organisatie. HbR verwacht dan ook dat de leverancier met betrekking tot de classificatie van informatie en risico’s aantoonbaar kan maken dat ten minste de volgende zaken gerealiseerd heeft:

- Alle informatie en informatiesystemen van de leverancier zijn voorzien van een classificatie over de as van beschikbaarheid, integriteit, vertrouwelijkheid.

- De leverancier heeft o.b.v. de bovengenoemde classificatie een risicoanalyse uitgevoerd. De risicoanalyse omvat o.a. maar niet uitsluitend de identificatie van de aan de systeem, applicatie, netwerk- en dataopslag systemen verbonden risico’s. Dit is gekwantificeerd op basis van “kans x impact”. De risicoanalyse wordt jaarlijks geactualiseerd tenzij dreigingsinformatie uitwijst dat de risico’s significant zijn toe- of afgenomen en bijstelling eerder noodzakelijk is. In deze risicoanalyse is ook het risico binnen de keten van toeleveranciers en afnemers opgenomen voor zover er sprake is van een gezamenlijk risico.

- De leverancier de bovengenoemde risico's geplot binnen een risico matrix waarop zichtbaar is welke risico's boven de risico bereidheid van de leverancier vallen.

3 Personele beveiliging

Het doel van beveiliging van personeel is het zo goed mogelijk benutten en op het vereiste niveau houden van de kennis en ervaring van de werknemers ter bevordering van de informatiebeveiliging alsmede het verminderen van de risico's van al dan niet opzettelijk menselijk handelen. Onderdeel van deze doelstelling is dat werknemers, ingehuurd personeel en externe gebruikers hun verantwoordelijkheden begrijpen en zich bewust zijn van bedreigingen en gevaren van informatiebeveiliging en van hun verantwoordelijkheid en aansprakelijkheid. HbR verwacht van de leverancier dat ten miste de volgende zaken hiervoor zijn ingericht:

- De leverancier heeft in het beleid eisen opgenomen t.a.v. nieuwe medewerkers, medewerkers die van functie wisselen en medewerkers waarvan het dienstverband beëindigd wordt.

- De leverancier heeft een up-to-date screeningsbeleid en is bereid deze te delen met HbR.

- De leverancier toets aantoonbaar periodiek het screeningsbeleid.

4 Toegangsbeveiliging

Het doel van toegangsbeveiliging is het voorkomen van onbevoegd of onnodige (fysieke)toegang tot bedrijfsmiddelen, informatiesystemen en informatie. Dit ter beperking van onbevoegde kennisneming, verminking of diefstal van bedrijfsmiddelen, informatiesystemen en informatie dan wel schade aan of hinderlijke storing van bedrijfsmiddelen of informatiesystemen of ongewenste beïnvloeding van het bedrijfsproces. HbR verwacht van de leverancier dat ten miste de volgende zaken hiervoor zijn ingericht:

- Het implementeren en documenteren van fysiek toegangsbeveiligingsbeleid. Dit betreft toegang tot ruimtes, apparatuur, ruimtes, etc. waaronder het identiteitenbeheer en autorisatiebeheer (uitgeven, monitoren en terugtrekken van rechten), en, afhankelijk van het vereiste beveiligingsniveau de toepassing voor 2-factor authenticatie. De toegangsrechten dienen conform het beleid minimaal jaarlijks beoordeeld en geactualiseerd te worden.

- Het implementeren en documenteren van logische toegangsbeveiligingsbeleid. Dit betreft toegang tot de netwerk- en informatiesystemen (identity en access management) waaronder het identiteitenbeheer en autorisatiebeheer (uitgeven, monitoren en terugtrekken van rechten), en, afhankelijk van het vereiste beveiligingsniveau de toepassing voor 2-factor authenticatie. De toegangsrechten dienen conform het beleid minimaal jaarlijks beoordeeld en geactualiseerd te worden.

5 Beheer van communicatie en bedieningsprocessen

De doelstelling van beheer van communicatie- en bedieningsprocessen is het verzorgen van een juiste, correcte en veilige bediening van IT-voorzieningen als systeem-, applicatie-, data- en netwerkcomponenten. HbR verwacht van de leverancier dat ten miste de volgende zaken hiervoor zijn ingericht:

- Alle ICT-systemen ten dienste van de leverancier dienen over voorzieningen te beschikken voor adequate en actuele bescherming tegen ongewenste invloeden door kwaadaardige software (malware) zoals virussen, wormen, Trojaanse paarden e.d. Dit geldt voor alle IT-voorzieningen van leverancier welke direct en/of indirect toegang hebben tot het IT-voorzieningen van het Havenbedrijf. Deze voorzieningen worden up-to-date gehouden.

- Er zijn periodiek geteste procedures voor back-up en recovery van informatie en configuratie voor herinrichting en foutherstel van verwerkingen. De procedures, inclusief een daadwerkelijke restore, worden regelmatig (tenminste 1 x per jaar) getest om de betrouwbaarheid ervan vast te stellen.

- Er zijn minimaal logisch gescheiden systemen voor Ontwikkeling, Test, Acceptatie en/of Productie (OTAP). De systemen en applicaties in deze zones beïnvloeden systemen en applicaties in andere zones niet. In de ontwikkel, test en acceptatie omgeving worden testaccounts gebruikt. Er wordt in beginsel niet getest met productieaccounts, tenzij voor de test absoluut noodzakelijk.

6 Beheer van informatiebeveiligingsincidenten

De doelstelling van het beheer van informatiebeveiligingsincidenten is het bewerkstelligen dat informatiebeveiligingsgebeurtenissen en zwakheden die verband houden met informatiesystemen zodanig kenbaar worden gemaakt dat tijdig corrigerende maatregelen kunnen worden genomen op basis van een risicoafweging. HbR verwacht van de leverancier dat ten miste de volgende zaken hiervoor zijn ingericht:

- Er processen en beleidsmaatregelen zijn ingericht om incidenten te melden en om tekortkomingen en kwetsbare plekken in de netwerk- en informatiesystemen te identificeren, inclusief het melden van incidenten door personeel of via responsible disclosure op een centraal punt.

- Er is beschreven welke beveiliging gerelateerde handelingen in het systeem worden gelogd en welke bij parameters dit leidt tot een meldingen die geanalyseerd moeten worden. De leverancier stelt deze logging realtime secure beschikbaar aan het Havenbedrijf.

- Er is beschreven welke methode van monitoring is toegepast, hoe dit is geïmplementeerd en hoe opvolging plaatsvindt.

- De leverancier test jaarlijks de detectieprocessen en -procedures om ervoor te zorgen dat afwijkende gebeurtenissen tijdig worden opgemerkt, geclassificeerd en, indien noodzakelijk, worden opgevolgd.

- De leverancier meldt middels de externe rapportage de resultaten van de genomen maatregelen. In dit verband worden tevens incidenten geclassificeerd, onderzocht en verholpen, zodat de duur en impact van de verstoring zoveel mogelijk wordt beperkt,

7 Bedrijfscontinuïteitsbeheer

De doelstelling van bedrijfscontinuïteitsbeheer is het treffen van voorbereidingen voor de opvang van omvangrijke of niet-voorziene storingen en calamiteiten alsmede de voortzetting van de kritieke bedrijfsprocessen. HbR verwacht van de leverancier dat ten miste de volgende zaken hiervoor zijn ingericht:

- Een vastgesteld beleid om de bedrijfscontinuïteit te waarborgen

- Een vastgesteld continuïteitsplan waarin is opgenomen hoe, in geval van calamiteiten, de getroffen ICT-dienst of het getroffen informatiesysteem weer zo snel mogelijk operationeel gemaakt kan worden en waarbij ten minste aandacht wordt besteed aan:
    - Geïdentificeerde risico's;
    - Identificatie van essentiële procedures voor bedrijfscontinuïteit, wie het plan mag activeren en wanneer;
    - Wanneer er weer gecontroleerd wordt teruggegaan;
    - Back-up strategie;
    - Veilig te stellen informatie (aanvaardbaarheid van verlies van informatie), prioriteiten en volgorde van herstel en reconstructie;
    - Documentatie van systemen en processen;
    - Kennis en kundigheid van personeel om de processen weer op te starten;
    - Continuïteitsvoorzieningen voor informatiemiddelen zijn zoveel mogelijk gestandaardiseerd en worden ingezet in overeenstemming met de beveiligingsklasse.

- Het vastgestelde plannen continuïteitsplan wordt jaarlijks beoordeeld en getest, bijvoorbeeld door middel van oefeningen.

- Vastgestelde procedures voor het tijdig delen van relevante informatie over incidenten en mogelijke impact met externe ketenpartners. Hieronder wordt ook verstaan deelnemen aan eventuele CERT-teams vanuit HbR indien er zich een incident voordoet.