|  |
| --- |
| **Gegevens Port Facility** |
| Naam Port Facility: |       | Datum: |       |
| Ingevuld door: |       | Telefoonnummer: |       |
| **Vragenlijst geheel invullen, inclusief toelichtingen. Bij vraag 1 zou de toelichting bijvoorbeeld kunnen zijn dat er een door de directie getekende beleidsverklaring is waarin Cyber Security expliciet is genoemd; bij het derde onderdeel van vraag 3 zou de toelichting kunnen zijn dat de verplichting tot het melden van cyberincidenten vastligt in een procedure (incl. naam en/of nummer van de procedure); en ten aanzien van screening (vraag 4) zou de toelichting kunnen zijn dat alleen medewerkers die in aanraking komen met gevoelige informatie worden gescreend (incl. voorbeelden van wat als gevoelig wordt beschouwd, dus zoals…..). Komt u ruimte tekort of heeft u aanvullende opmerkingen, dan kunt u die kwijt bij punt 23.** |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Nr.** | **Hoofdcategorie** | **Subcategorie** | **Onderwerp** | **Ja/Nee/Nvt** | **Verplichte toelichting** |
| 1 | Planvorming | Beleid | Is er bewustzijn op directieniveau van de mogelijke dreiging op het gebied van cyber? | [ ] Ja [ ] Nee [ ] N.v.t. |       |
| Vindt de directie cybersecurity aantoonbaar belangrijk? | [ ] Ja [ ] Nee [ ] N.v.t. |
| **Nr.** | **Hoofdcategorie** | **Subcategorie** | **Onderwerp** | **Ja/Nee/N.v.t.** | **Verplichte toelichting** |
| 2 | Planvorming | Beleid | Is er beveiligingsbeleid? | [ ] Ja [ ] Nee [ ] N.v.t. |       |
| Zijn er procedures, toewijzing van taken en verantwoordelijkheden en bevoegdheden? | [ ] Ja [ ] Nee [ ] N.v.t. |
| Is er budget? | [ ] Ja [ ] Nee [ ] N.v.t. |
| Is dit opgenomen in het PFSP/PFSA? | [ ] Ja [ ] Nee [ ] N.v.t. |
| **Nr.** | **Hoofdcategorie** | **Subcategorie** | **Onderwerp** | **Ja/Nee/N.v.t.** | **Verplichte toelichting** |
| 3 | Planvorming | Incidenten | Is er een interne incident meldprocedure? | [ ] Ja [ ] Nee [ ] N.v.t. |       |
| Is er een incidentenprocedure met noodplannen? | [ ] Ja [ ] Nee [ ] N.v.t. |
| Ligt vast dat er een wettelijke meldplicht is bij cyberincidenten (b.v. data-lekken)? | [ ] Ja [ ] Nee [ ] N.v.t. |
| **Nr.** | **Hoofdcategorie** | **Subcategorie** | **Onderwerp** | **Ja/Nee/N.v.t.** | **Verplichte toelichting** |
| 4 | Voorbereiding | Risico-bewustzijn | Hebben alle medewerkers een: |       |
| gedragscode en/of Geheimhouders verklaring ondertekend? | [ ] Ja [ ] Nee [ ] N.v.t. |
| een VOG overlegd of een medewerkersscreening ondergaan?  | [ ] Ja [ ] Nee [ ] N.v.t. |
| **Nr.** | **Hoofdcategorie** | **Subcategorie** | **Onderwerp** | **Ja/Nee/N.v.t.** | **Verplichte toelichting** |
| 5 | Voorbereiding | Risico-bewustzijn | Krijgen alle medewerkers een cyber risicobewustzijn opleiding / cyber security awareness training? | [ ] Ja [ ] Nee [ ] N.v.t. |       |
| Worden deze periodiek herhaald? | [ ] Ja [ ] Nee [ ] N.v.t. |
| **Nr.** | **Hoofdcategorie** | **Subcategorie** | **Onderwerp** | **Ja/Nee/N.v.t.** | **Verplichte toelichting** |
| 6 | Voorbereiding | Asset / configuratie management | Is er een actueel overzicht van hard en software (met besturingssystemen)? | [ ] Ja [ ] Nee [ ] N.v.t. |       |
| Zijn de configuraties en de netwerk-verbindingen ertussen met internet en de “cloud” bekend? | [ ] Ja [ ] Nee [ ] N.v.t. |
| Is in alle gevallen bekend welke medewerker of ketenpartner dit beheerd? | [ ] Ja [ ] Nee [ ] N.v.t. |
| Wordt dit regelmatig gecontroleerd? | [ ] Ja [ ] Nee [ ] N.v.t. |
| **Nr.** | **Hoofdcategorie** | **Subcategorie** | **Onderwerp** | **Ja/Nee/N.v.t.** | **Verplichte toelichting** |
| 7 | Voorbereiding | Asset management | Staan op dit overzicht ook de: |       |
| * Toegangscontrole systemen
 | [ ] Ja [ ] Nee [ ] N.v.t. |
| * Camerabewaking
 | [ ] Ja [ ] Nee [ ] N.v.t. |
| * Inbraakalarmsysteem
 | [ ] Ja [ ] Nee [ ] N.v.t. |
| * Brandmeldinstallaties
 | [ ] Ja [ ] Nee [ ] N.v.t. |
| * Klimaatbeheersingssystemen
 | [ ] Ja [ ] Nee [ ] N.v.t. |
| * Andere slimme apparaten / IoT
 | [ ] Ja [ ] Nee [ ] N.v.t. |
| **Nr.** | **Hoofdcategorie** | **Subcategorie** | **Onderwerp** | **Ja/Nee/N.v.t.** | **Verplichte toelichting** |
| 8 | Netwerk-management | Leveranciers | Is er een overzicht van leveranciers van hard- en software? Zijn zij gescreend?  | [ ] Ja [ ] Nee [ ] N.v.t. |       |
| Zijn bevoegdheden en verantwoordelijkheden vastgelegd in contracten? | [ ] Ja [ ] Nee [ ] N.v.t. |
| **Nr.** | **Hoofdcategorie** | **Subcategorie** | **Onderwerp** | **Ja/Nee/N.v.t.** | **Verplichte toelichting** |
| 9 | Voorbereiding | Gebruikers-beheer | Welke van onderstaande accounttypen worden door medewerkers gebruikt? |       |
| Generiek (gedeeld / voor allen of meerdere hetzelfde) | [ ] Ja [ ] Nee [ ] N.v.t. |
| Uniek / persoonlijke | [ ] Ja [ ] Nee [ ] N.v.t. |
| **Nr.** | **Hoofdcategorie** | **Subcategorie** | **Onderwerp** | **Ja/Nee/N.v.t.** | **Verplichte toelichting** |
| 10 | Voorbereiding | Wachtwoorden | Wordt vanuit beleid sterke regelmatig wijzigende wachtwoorden voorgeschreven waarbij alle default wachtwoorden veranderd worden?  | [ ] Ja [ ] Nee [ ] N.v.t. |       |
| Worden gebruikersrechten direct aangepast bij verandering van functie of uitdiensttreden? | [ ] Ja [ ] Nee [ ] N.v.t. |
| Worden pc’s automatisch vergrendeld na enige tijd van inactiviteit? | [ ] Ja [ ] Nee [ ] N.v.t. |
| **Nr.** | **Hoofdcategorie** | **Subcategorie** | **Onderwerp** | **Ja/Nee/N.v.t.** | **Verplichte toelichting** |
| 11 | Voorbereiding | Autorisaties | Is bekend wie waar toegang toe heeft via autorisatie en authenticatie(login)?  | [ ] Ja [ ] Nee [ ] N.v.t. |       |
| **Nr.** | **Hoofdcategorie** | **Subcategorie** | **Onderwerp** | **Ja/Nee/N.v.t.** | **Verplichte toelichting** |
| 12 | Voorbereiding | Koppelingen kantoor automatisering | Zijn de koppelingen tussen kantoornetwerken en externe systemen gescheiden en beveiligd? | [ ] Ja [ ] Nee [ ] N.v.t. |       |
| Wordt gebruik gemaakt van: | **Ja/Nee/N.v.t.** |
| * firewalls
 | [ ] Ja [ ] Nee [ ] N.v.t. |
| * gateways
 | [ ] Ja [ ] Nee [ ] N.v.t. |
| * proxy-servers
 | [ ] Ja [ ] Nee [ ] N.v.t. |
| * encryptie
 | [ ] Ja [ ] Nee [ ] N.v.t. |
| * beveiligde verbindingen
 | [ ] Ja [ ] Nee [ ] N.v.t. |
| * andere beveiligingstechnieken
 | [ ] Ja [ ] Nee [ ] N.v.t. |
| **Nr.** | **Hoofdcategorie** | **Subcategorie** | **Onderwerp** | **Ja/Nee/N.v.t.** | **Verplichte toelichting** |
| 13 | Maatregelen | Anti virus | Wordt gebruik gemaakt van antivirus software? | [ ] Ja [ ] Nee [ ] N.v.t. |       |
| **Nr.** | **Hoofdcategorie** | **Subcategorie** | **Onderwerp** | **Ja/Nee/N.v.t.** | **Verplichte toelichting** |
| 14 | Maatregelen | Verouderings-risico’s | Wordt er nog gebruik gemaakt van verouderde en/of maatwerk Hardware, software, besturingssystemen? | [ ] Ja [ ] Nee [ ] N.v.t. |       |
| **Nr.** | **Hoofdcategorie** | **Subcategorie** | **Onderwerp** | **Ja/Nee/N.v.t.** | **Verplichte toelichting** |
| 15 | Maatregelen | Wijzigings-management | Is er beleid m.b.t. updates en patches voor besturingssystemen en kwetsbare applicaties? Incluis alle logische of fysieke aan het netwerk gekoppelde systemen? | [ ] Ja [ ] Nee [ ] N.v.t. |       |
| **Nr.** | **Hoofdcategorie** | **Subcategorie** | **Onderwerp** | **Ja/Nee/N.v.t.** | **Verplichte toelichting** |
| 16 | Maatregelen | Wifi / Netwerken | Hoe is toegang tot en via draadloze (wifi, bluetooth, 3G, e.d.) netwerken beveiligd en beperkt? |       |
| * Wachtwoord (anders dan fabrieksinstelling)
 | [ ] Ja [ ] Nee [ ] N.v.t. |
| * Hardware herkenning (MAC adres)
 | [ ] Ja [ ] Nee [ ] N.v.t. |
| * Zonering
 | [ ] Ja [ ] Nee [ ] N.v.t. |
| * Anders
 | [ ] Ja [ ] Nee [ ] N.v.t. |
| Zijn kabels netjes en ontoegankelijk weggewerkt | [ ] Ja [ ] Nee [ ] N.v.t. |
| **Nr.** | **Hoofdcategorie** | **Subcategorie** | **Onderwerp** | **Ja/Nee/N.v.t.** | **Verplichte toelichting** |
| 17 | Maatregelen | Hardening | Is niet noodzakelijke hard en soft ware verwijderd? | [ ] Ja [ ] Nee [ ] N.v.t. |       |
| **Nr.** | **Hoofdcategorie** | **Subcategorie** | **Onderwerp** | **Ja/Nee/N.v.t.** | **Verplichte toelichting** |
| 18 | Maatregelen | Remote | Is toegang op afstand mogelijk? | [ ] Ja [ ] Nee [ ] N.v.t. |       |
| Indien ja, hoe is dit beveiligd? |  |
| * Tweetrapsauthenticatie
 | [ ] Ja [ ] Nee [ ] N.v.t. |
| * Anders
 | [ ] Ja [ ] Nee [ ] N.v.t. |
| **Nr.** | **Hoofdcategorie** | **Subcategorie** | **Onderwerp** | **Ja/Nee/N.v.t.** | **Verplichte toelichting** |
| 19 | Maatregelen | Netwerk monitoring en malware detectie | Wordt het gebruik van hard- en software gelogd?  | [ ] Ja [ ] Nee [ ] N.v.t. |       |
| Zijn er monitoring- en detectievoorzieningen op het netwerk, incluis aansluiten van harde schijven, usb sticks, e.d. | [ ] Ja [ ] Nee [ ] N.v.t. |
| **Nr.** | **Hoofdcategorie** | **Subcategorie** | **Onderwerp** | **Ja/Nee/N.v.t.** | **Verplichte toelichting** |
| 20 | Test | Pentest | Wordt de werking van het stelsel van beveiligingsmaatregelen regelmatig getest? (bv hacktest netwerk) | [ ] Ja [ ] Nee [ ] N.v.t. |       |
| **Nr.** | **Hoofdcategorie** | **Subcategorie** | **Onderwerp** | **Ja/Nee/N.v.t.** | **Verplichte toelichting** |
| 21 | Back-up | Back-up / noodstroom | Worden van de systemen, IT applicaties en gegevens back-ups gemaakt? | [ ] Ja [ ] Nee [ ] N.v.t. |       |
| Wordt beschikbaarheid en integriteit geregeld getest? | [ ] Ja [ ] Nee [ ] N.v.t. |
| Wordt er gebruik gemaakt van een noodstroomvoorziening? | [ ] Ja [ ] Nee [ ] N.v.t. |
| Worden deze met regelmaat getest? | [ ] Ja [ ] Nee [ ] N.v.t. |
| **Nr.** | **Hoofdcategorie** | **Subcategorie** | **Onderwerp** | **Ja/Nee/N.v.t.** | **Verplichte toelichting** |
| 22 | Response | Meldplicht & oefenen | Wanneer er een cyberincident plaatsvindt is dan helder wie er geïnformeerd moet worden? | [ ] Ja [ ] Nee [ ] N.v.t. |       |
| Kan men snel schakelen? | [ ] Ja [ ] Nee [ ] N.v.t. |
| Wordt er voldaan aan de meldplicht? | [ ] Ja [ ] Nee [ ] N.v.t. |
| Wordt er aangifte gedaan? | [ ] Ja [ ] Nee [ ] N.v.t. |
| Wordt crisisproces geoefend? | [ ] Ja [ ] Nee [ ] N.v.t. |
| **Nr.** | **Aanvullende opmerkingen** |
| **23** |       |