We create chemistry

Be Secure-checklist

m.b.t. informatiebescherming als hulpmiddel voor derden bij de samenwerking met BASF

Checklist
m.b.t. informatiebescherming en Cyber Security

Deze „Checklist m.b.t. informatiebescherming en Cyber Security“ is bedoeld om gebruikers te helpen bij het identificeren van potentiële gevaren bij de omgang met gevoelige informatie en om passende maatregelen te nemen zodat gevoelige informatie te allen tijde effectief beschermd is tegen verlies en onbevoegde toegang.

De ervaring heeft geleerd dat de thema's in deze checklist essentieel zijn bij de praktische uitvoering van een informatiebescherming die te allen tijde doeltreffend is.

Deze checklist heeft geen definitief karakter. De gebruiker is zelf verantwoordelijk om te beoordelen welke concrete maatregelen er nodig zijn voor informatiebescherming en Cyber Security in elk afzonderlijk geval. Daarbij mag nooit uitsluitend op technische oplossingen worden vertrouwd, maar moet steeds het gezond verstand worden gebruikt.

Colofon:

67056 Ludwigshafen

E-mail: be-secure@basf.com
Versie vanaf: oktober 2019

Fundamentele vragen

- Is de kring van personen die bevoegd zijn voor de omgang met gevoelige informatie („bevoegde personen“) vastgelegd?
- Werd met de bevoegde personen een geheimhoudingsovereenkomst afgesloten?
- Hebben de bevoegde personen een instructie over informatiebescherming en cyber security gekregen?
- Worden er regelmatig controles uitgevoerd om ervoor te zorgen dat de voorschriften inzake informatiebescherming correct worden nageleefd?
- Worden de beveiligingsnormen voor software en hardware nageleefd?

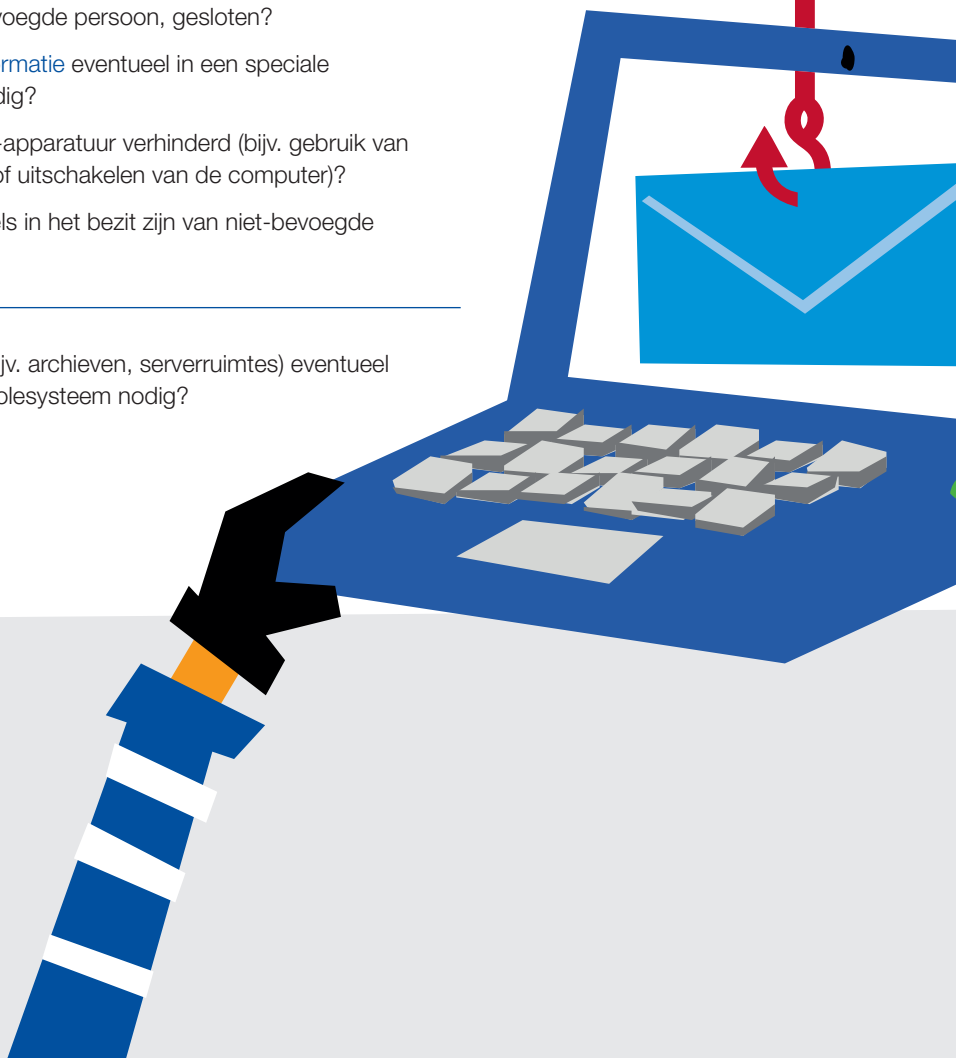
Maatregelen
tegen ongeoorloofde toegang tot gevoelige informatie

Is de toegang tot gevoelige informatie te allen tijde effectief tot de bevoegde personen beperkt en worden die toegangsrechten regelmatig gecontroleerd en – indien nodig – aangepast?

Worden er passende beschermingsmaatregelen genomen in afwezigheid van de bevoegde persoon?

- Wordt ervoor gezorgd dat er tijdens de afwezigheid van de bevoegde personen geen personen in de ruimte zijn die niet mogen beschikken over of mogen omgaan met gevoelige informatie („niet-bevoegde personen“)? Wordt bijvoorbeeld het schoonmaken van ruimtes altijd in aanwezigheid van de bevoegde persoon uitgevoerd?
- Zijn ruimtes, kasten en andere containers waarin zich gevoelige informatie bevindt, in afwezigheid van de bevoegde persoon, gesloten?
- Is het opbergen van gevoelige informatie eventueel in een speciale beveiligde opbergmogelijkheid nodig?
- Wordt onbevoegde toegang tot IT-apparatuur verhinderd (bijv. gebruik van veilige wachtwoorden, blokkeren of uitschakelen van de computer)?
- Is gewaarborgd dat er geen sleutels in het bezit zijn van niet-bevoegde personen?

Is voor bijzonder kwetsbare locaties (bijv. archieven, serverruimtes) eventueel een inbraakalarm en/of toegangscontrolesysteem nodig?



Maatregelen
tegen ongeoorloofde toegang tot gevoelige informatie

Veilige wachtwoorden voor systemen waarin gevoelige informatie opgeslagen is:

- Zijn de gekozen wachtwoorden complex genoeg (zijn ze bijv. minstens acht tekens lang en bevatten ze een hoofdletter, een kleine letter, speciale tekens en een cijfer) en worden ze regelmatig gewijzigd?
- Wordt ervoor gezorgd dat wachtwoorden niet aan derden worden doorgegeven en indien ze gedocumenteerd zijn (bv. in een geschreven versie) niet vrij toegankelijk zijn (bijv. in een verzegelde omslag opgeborgen in een kluis)?
- Wordt er twee-factor-authenticatie gebruikt?

Zijn interne postvakken zo ingericht dat niet-bevoegden geen toegang hebben tot gevoelige informatie die er kan inliggen?

Is de opgeslagen gevoelige informatie op gegevensdragers (notebooks, tablets, smartphones, harde schijven, servers, cd-roms, USB-sticks, ...) effectief beveiligd (bijv. door gebruikmaking van de meest geavanceerde versleutelingstechniek)?

Worden er effectieve maatregelen genomen bij het communiceren (bijv. e-mail, telefoon- en videoconferenties, verzending van brieven) van gevoelige informatie (bijv. versleuteling van de communicatieverbinding, opdeling van de gevoelige informatie op verschillende communicatiedragers)?

Maatregelen
tegen ongeoorloofde toegang tot gevoelige informatie

Zijn de printers en kopieerapparaten veilig geconfigureerd? Wordt ervoor gezorgd dat reproductie van afdruk- resp. kopieertaken die gevoelige informatie bevatten, niet mogelijk is? Wordt ervoor gezorgd dat originelen, afdrukken resp. kopieën onmiddellijk worden verwijderd en niet in de printer/kopieerapparaat/ faxmachine blijven liggen (evt. gebruik van de „PIN-functie“)?

- Worden vergaderingen zo uitgevoerd dat kennisneming van gevoelige informatie door niet-bevoegde personen is uitgesloten?
- Wordt ervoor gezorgd dat er uit informatie buiten de ruimte (bijv. borden) geen conclusies kunnen worden getrokken over de vertrouwelijke inhoud van de vergadering?
- Wordt ervoor gezorgd dat meeluisteren van buitenaf (bijv. hal, nevenvertrekken, ramen, deuren) niet mogelijk is?
- Wordt ervoor gezorgd dat van buitenaf inzage in vergader- of presentatiedocumenten uitgesloten is (bijv. gordijnen sluiten)?
- Wordt ervoor gezorgd dat er na afloop van de bespreking geen documenten, apparatuur, presentatiemiddelen (teksten op de flipchart of op het bord, afdrukken van slides) achterblijven?
- Wordt ervoor gezorgd dat de vergaderzaal niet toegankelijk is voor onbevoegde personen wanneer alle deelnemers afwezig zijn (bijv. in de pauzes)

Gevoelige informatie
op de juiste manier verwijderen

Gebeurt de verwijdering of het wissen van gevoelige informatie op correcte en veilige wijze?

- Worden bij de vernietiging van papier cross-cut-shredders met een maximale deeltjesgrootte van 160mm^2 gebruikt?
- Bij gebruik van opvangcontainers: Zijn de opvangcontainers gesloten? Staan ze veilig opgesteld? Is het verwijderingsproces voldoende veilig? Wordt DIN 66399 (minstens veiligheidsniveau 4) nageleefd?

Informatiebeveiligings-aspecten wanneer je buiten je BASF-omgeving werkt

- Wordt er vóór de reis gecontroleerd of het meenemen van gevoelige informatie absoluut noodzakelijk is?
- Wordt ervoor gezorgd dat niet-bevoegde personen onderweg geen inzage in gevoelige informatie (bijv. dossiers en notebook) kunnen hebben?
- Wordt ervoor gezorgd dat dossiers, notebook, ... onderweg altijd onder toezicht staan?
- Wordt ervoor gezorgd dat niet-bevoegde personen bij gesprekken of telefoontjes niet kunnen meeluisteren?
- Zijn notebooks met behulp van een geschikt slot aan een stevige structuur bevestigd en zo tegen diefstal beveiligd?
- Wordt ervoor gezorgd dat gevoelige informatie niet op internetplatforms en sociale media wordt geplaatst?
- Wordt ervoor gezorgd dat bij teruggave van het gehuurde of geleasde voertuig geen gegevens (bijv. op telefoon of navigatiesysteem) zijn opgeslagen en geen documenten worden achtergelaten?

Persoonlijke notities

Persoonlijke notities

be-secure.basf.net

versie vanaf: oktober 2019