grafische groep van der eems

Informatiebeveiligingsbeleid Drukkerij van der Eems

Door	:	Sjoukje van der Eems
Datum	:	26-4-2018
Versie	:	1
Status	:	Definitief

Algemeen

Belang van Informatiebeveiliging

De beschikbaarheid, exclusiviteit en integriteit van informatie dient te worden gegarandeerd om de continuïteit van de organisatie te beschermen. Gevoelige informatie aangaande de eigen bedrijfsvoering dient te worden beschermd. Informatiebeveiliging moet 'in control' zijn. Risico's op dit gebied moeten worden onderkend en er moet bepaald worden in hoeverre zulke risico's afgedekt moeten worden met maatregelen. Kwalitatieve informatiebeveiliging wordt gerealiseerd door toepassing van een combinatie van technische maatregelen en procedures en processen. Waar technische maatregelen voornamelijk gericht zijn op beveiliging van systemen, hebben processen en procedures invloed op de gehele werkwijze van organisatie en medewerkers. Het uiteindelijke doel is om beveiligingsincidenten zoveel mogelijk te voorkomen en eventuele schade zoveel mogelijk te beperken

Privacy is een belangrijke randvoorwaarde van informatiebeveiliging. Dit is de reden waarom de EU in mei 2016 met een nieuwe wetgeving is gekomen: de Algemene Verordening Gegevensbescherming (AVG), gericht op een eenduidige privacywetgeving binnen de EU. De wetgeving zorgt voor nog maar één privacywet in de hele Europese Unie (EU) in plaats van 28 verschillende nationale wetten. De prioriteit op het naleven van de wetgeving is hoog en het niet naleven van deze wetgeving kan vanaf 25 mei 2018 leiden tot hoge boetes voor organisaties waarbij bestuurders persoonlijk aansprakelijk gesteld kunnen worden.

Risicobenadering

De benadering van de meting van informatiebeveiliging (IB-beleid) is 'risk based'. Dat wil zeggen dat het doel is om noodzakelijke beveiligingsrisico's in kaart te brengen op basis van de impact die mogelijke risico's met zich meebrengen. Dit wordt gedaan om een zo efficiënt informatiebeveiligingsbeleid te voeren en de juiste maatregelen te kunnen bepalen.

1. Organisatie van de informatiebeveiliging

1.1 Interne organisatie

Doel

Er dienen rollen en verantwoordelijkheden te worden belegd binnen een organisatie omtrent het informatiebeveiligingsbeleid, de implementatie ervan en de controle en eventuele wijzigingen daarop.

Risico

Het niet beleggen van rollen en verantwoordelijkheden omtrent informatiebeveiliging verhindert het naleven van het informatiebeveiligingsbeleid met alle mogelijke consequenties.

1.2 Rollen en verantwoordelijkheden

De Directie en Business Controller zijn verantwoordelijk voor het informatiebeveiligingsbeleid en het Privacybeleid. Dit zijn o.a. hun taken en verantwoordelijkheden.

Rol/Verantwoordelijkheid
Stelt beleidskaders op voor de informatiebeveiliging
Geeft sturing aan/ draagt uit de uitvoering van het beleid
Evalueert periodiek het beleid
Stuur op beveiligingsbewustzijn
Verantwoordelijk voor het implementeren, naleven en evalueren van de beheersmaatregelen
Verantwoordelijk voor beveiliging van de informatievoorziening en implementatie van beveiligingsmaatregelen
Verantwoordelijk voor alle beheeraspecten van informatiebeveiliging, zoals ICT security management, incident en problem management, facilitaire en personele zaken;
Verzorgt monitoring en rapportage indien mogelijk/wenselijk
Draagt (een) verantwoordelijke(n) aan waarnaar geëscaleerd kan worden en welke zorgt draagtvoor informatiebeveiligingsincidenten en/of mogelijke datalekken

1.3 Externe organisatie

Het Informatiebeveiligingsbeleid geldt ook voor externe partijen waarmee wordt samengewerkt. IB-beleid, landelijke normen en wet en regelgeving gelden ook voor externe partijen met als doel risicobeheersing.

1.4 Evaluatie en Continu Verbeteren

Informatiebeveiliging is een continu proces. Dit beleid wordt dan ook minimaal 1x per jaar geëvalueerd. Door middel van Continu Verbeteren kunnen punten ter verbetering worden geregistreerd en opgepakt.

Veelal wordt hiervoor gebruikt gemaakt van PDCA (Plan-Do-Check-Act)

2. Beheer van bedrijfsmiddelen

2.1 Verantwoordelijkheid voor bedrijfsmiddelen

Doel

Zorgdragen voor een adequate bescherming van bedrijfsmiddelen van de organisatie. Voor alle bedrijfsmiddelen is de eigenaar vastgelegd. Dit kunnen zowel mobiele apparaten zijn evenals sleutels of toegangscodes.

Risico's:

Bedrijfsmiddelen en informatie zijn blootgesteld aan risico's zoals diefstal, beschadiging of onoordeelkundig gebruik, waarbij niet voor alle ICT-configuratie items is vastgelegd wie de eigenaar/hoofdgebruiker is.

Beheersmaatregelen

- Alle bedrijfsmiddelen zijn geïdentificeerd en de inventaris wordt bijgehouden
- De directie en business controller zijn verantwoordelijk voor het beheren van de bedrijfsmiddelen
- De organisatie heeft passende technische en organisatorische maatregelen tegen verlies of tegen enige vorm van onrechtmatig gebruik genomen.
- Bij indiensttreding wordt vastgesteld welke middelen bij het dienstverband horen en deze worden geregistreerd. Bij uitdiensttreding of wijziging van het dienstverband worden de middelen dan wel ingenomen dan wel herzien.

3. Fysieke toegangsbeveiliging

3.1 Fysieke (omgevings)beveiliging

Doel

Het voorkomen van onbevoegde fysieke toegang tot, schade aan of verstoring van het terrein en de informatie van de organisatie, bedrijfsmiddelen en onderbreking van de bedrijfsactiviteiten om zodoende de vertrouwelijkheid, integriteit of beschikbaarheid van informatie van de organisatie te waarborgen.

Risico's

- Toegang tot rond liggende vertrouwelijke informatie
- Onbevoegde toegang tot kritieke systemen of waardevolle informatie. Bij het ontbreken van registratie zijn incidenten bovendien niet herleidbaar tot individuen.

Beheersmaatregelen Fysieke toegang

- Er is een Clean/clear desk policy geïmplementeerd om te voorkomen dat mogelijk vertrouwelijke informatie rondslingert
- De schade door bedreigingen van buitenaf (zoals brand, overstroming, explosies, oproer, stroomonderbreking) wordt beperkt door passende preventieve maatregelen.
- Toegang tot niet-openbare gedeelten van gebouwen of beveiligingszones is alleen mogelijk na autorisatie daartoe.

- Serverruimtes, datacenters en daaraan gekoppelde bekabelingsystemen zijn ingericht in lijn met geldende ‘best practices’.
- (Data)verbindingen worden beschermd tegen interceptie of beschadiging.
  Back-ups worden op een externe locatie bewaard.
- Er is een calamiteitenplan- continuïteitsplan beschikbaar met o.a. maximale uitvalduur en maximaal gegevensverlies.

Beheersmaatregelen authenticatie en autorisatie

- De toegang tot systemen is beveiligd met een loginnaam en wachtwoord.
- 1 keer per jaar moet een gebruiker zijn wachtwoord wijzigen. Het nieuwe wachtwoord moet voldoen aan een aantal beveiligingseisen en bestaat uit een wachtwoord zin.
- In de autorisatiematrix is per systeem vastgelegd wie waartoe rechten heeft.
- Wanneer ingelogd wordt vanaf een externe locatie is naast een loginnaam en wachtwoord, ook een passcode (ook wel ‘token’ genoemd) benodigd. De passcode wordt beschikbaar gesteld via de mobiele telefoon van de gebruiker. De code wordt na elke inlogpoging vernieuwd.
- De fysieke poorten zijn beveiligd middels een firewall, deze staat onder beheer van de systeembeheerder.

Beheersmaatregelen medewerkers en inhuur

- Er is een procedure voor het melden en afhandelen van beveiligingsincidenten
- Bij beëindiging van het dienstverband en inhuur worden alle bedrijfsmiddelen van de organisatie geretourneerd. Autorisaties worden geblokkeerd.
- De directie bepaalt welke rol(len) de medewerker moet vervullen en welke autorisaties voor het raadplegen, opvoeren, muteren en afvoeren van gegevens moeten worden verstrekt.
- Alle medewerkers (en voor zover van toepassing externe gebruikers van onze systemen) Dienen de regels rondom informatiebeveiliging te kennen. Deze staan o.a. in het huishoudelijk reglement.
- Regels die volgen uit dit beleid gelden ook voor externen, die in opdracht van de organisatie werkzaamheden uitvoeren.
- Er wordt door medewerkers een geheimhoudingsverklaring ondertekend (Meldplicht Datalekken) welke ook na uitdiensttreding geldig is.

4 Beveiliging van apparatuur en informatie(systemen)

4.1 Beveiliging van apparatuur en informatie

Doel

Waarborgen van een correcte en veilige bediening van ICT-voorzieningen met als doel het beschermen van gegevens om zodoende de vertrouwelijkheid, integriteit en beschikbaarheid te waarborgen. Het gaat hierbij om data welke zich op het netwerk en in de applicaties bevindt.

Risico’s

- Het ontbreken van documentatie kan leiden tot fouten, niet-uniforme wijze van gegevensinvoer, of in geval de beheerder/bediener uitvalt, tot problemen rondom de continuïteit.

- Onjuiste autorisaties kunnen leiden tot oneigenlijk gebruik
- Programmatuur en ICT-voorzieningen zijn kwetsbaar voor virussen.

Beheersmaatregelen

- Op applicaties die strikt vertrouwelijke gegevens bevatten, zijn extra beveiligingsmaatregelen getroffen
- Informatie wordt beschermd door het instellen van gebruikersrechten,
- Één keer per dag wordt er automatisch een back-up gemaakt van alle data
- Om de beschikbaarheid van informatiesystemen te optimaliseren zijn de kritische hardware componenten redundant uitgevoerd.
- De back-up en herstelprocedures worden regelmatig getest om de betrouwbaarheid ervan vast te stellen: Het restore proces functioneert 4 goed gemiddeld 4 keer per jaar.
- Er is een procedure opgesteld rondom de uitgifte en beheer van bedrijfsmiddelen
- Er vindt monitoring plaats op bedrijf kritische applicaties en servers om storingen te voorkomen en ten behoeve van een tijdige aanpassing van de beschikbare capaciteit aan de vraag.
- Er is een scheiding tussen beheertaken en overige gebruikstaken. Beheerwerkzaamheden worden alleen uitgevoerd wanneer ingelogd als beheerder, normale gebruikstaken alleen wanneer ingelogd als gebruiker.

Organisatorische aspecten

Er heeft niemand autorisaties om een gehele cyclus van handelingen in een informatiesysteem te beheersen, zodanig dat beschikbaarheid, integriteit of vertrouwelijkheid kan worden gecompromitteerd.

- Er is een scheiding tussen beheertaken en overige gebruikstaken. Beheerwerkzaamheden worden alleen uitgevoerd wanneer ingelogd als beheerder, normale gebruikstaken alleen wanneer ingelogd als gebruiker.
- Bij externe hosting van data en/of services (uitbesteding, cloud computing) is Drukkerij van der Eems eindverantwoordelijk voor de betrouwbaarheid van uitbestede diensten. Dit is gebonden aan regels en vereist goede (contractuele) afspraken.

4.2 Beheer van de dienstverlening door een derde partij

Bij beheer van systemen en gegevens door een derde partij kan ook informatie op straat komen te liggen. De organisatie blijft verantwoordelijk voor de informatiebeveiliging van haar gegevens in dat deel van de keten, waarbij het beheer bij een andere partij ligt. Vanuit de AVG spreekt men hierbij van verwerkersverantwoordelijke (de organisatie) en verwerker (derde partij).

Doelstelling: Een passend niveau van informatiebeveiliging implementeren en bijhouden en dit vastleggen in een verwerkersovereenkomst, contracten en/of convenanten.

4.3 Classificatie van informatie

Om te kunnen bepalen welke beveiligingsmaatregelen moeten worden getroffen t.a.v. processen en informatiesystemen worden beveiligingsclassificaties gebruikt. Classificatie maakt het vereiste beschermingsniveau zichtbaar en maakt direct duidelijk welke maatregelen nodig zijn.

Risico's:

- Onjuiste classificatie draagt bij aan het onjuist beschermen van informatie en bedrijfsmiddelen met als risico, dat deze verloren kunnen gaan of openbaar worden gemaakt terwijl dat niet de bedoeling is.
- Geen inzicht in welke componenten, zowel hardware als software, het belangrijkst zijn voor de primaire processen.

Beheersmaatregelen

Er is door Drukkerij van der Eems een schema opgesteld waarin is bepaald welke soort informatie als vertrouwelijk behandeld dient te worden. (zie bijlage 6)

5. Informatiebeveiligingsincidenten en Meldplicht Datalekken

5.1 Informatiebeveiligingsincidenten

Doel

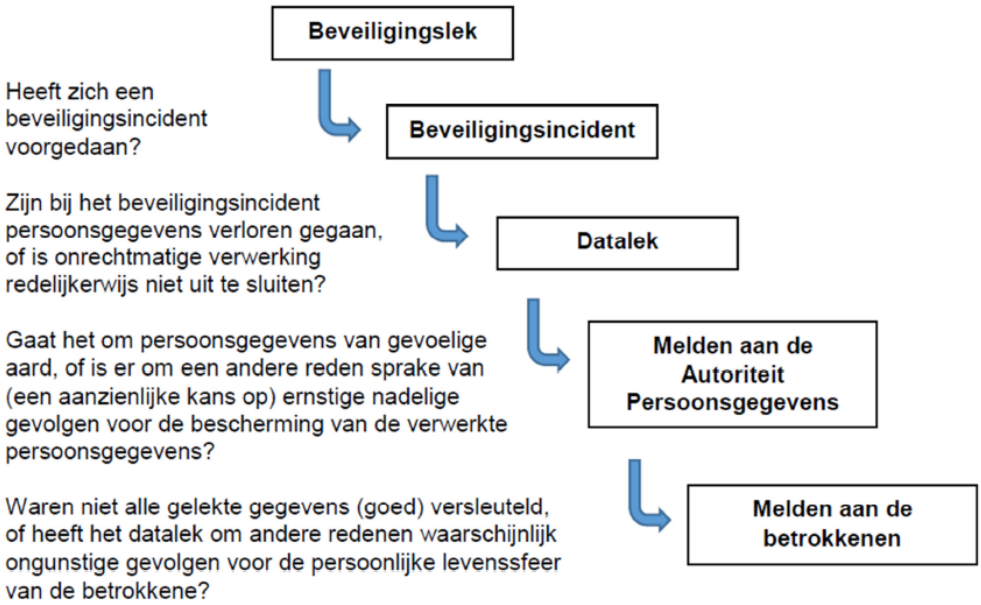
Dit proces heeft ten doel het bewerkstelligen dat informatiebeveiligingsincidenten, zwakheden en (mogelijke) datalekken zodanig kenbaar worden gemaakt dat tijdig corrigerende maatregelen kunnen worden genomen.

Risico's

Indien incidenten niet worden geregistreerd, is er geen lerend effect in de organisatie en zullen er geen maatregelen worden getroffen om verbeteringen door te voeren. De kans op mogelijke incidenten zoals datalekken blijven een hoog risico.

5.2 Registratie en opvolging

- Er is een procedure voor het melden en afhandelen van beveiligingsincidenten
- Naast een eerste correctie wordt er door Business Controller een oorzaakanalyse gedaan en in samenspraak met de directie bepaald wat voor opvolging het incident nodig heeft.
- Afhankelijk van de ernst van een incident is er een meldplicht bij de Autoriteit Persoonsgegevens. Hierbij wordt onderstaand schema opgevolgd.



6. Algemene Verordening Gegevensbescherming

De Algemene Verordening Gegevensbescherming (AVG) stelt verschillende eisen aan organisaties. Deze eisen zijn veelal verwerkt in bovenstaand Informatiebeveiligingsbeleid waar u o.a. de technische en organisatorische maatregelen kunt terugvinden evenals de procedure voor de Meldplicht Datalekken. Naast deze onderdelen hebben wij nog enkele beheersmaatregelen getroffen om te voldoen aan de AVG.

Beheersmaatregelen

- Wij hebben een verwerkingsregister opgesteld
- Wij hebben indien nodig verwerkersovereenkomsten afgesloten met derde partijen waarin wij zowel als verwerkersverantwoordelijke als verwerker kunnen worden aangemerkt
- Wij hebben een veelvoud aan technische en organisatorische maatregelen geïmplementeerd om zorg te dragen voor persoonsgegevens
- Wij sturen aan op bewustzijn bij onze medewerkers over de risico's op het gebied van privacy en hoe deze kunnen worden geminimaliseerd/voorkomen
- Wij hebben een procedure voor de Meldplicht Datalekken
- Wij hebben verantwoordelijkheden en rollen aangewezen om toe te zien op bovenstaande taken en wet- en regelgeving te volgen.