TT3P Template Informatiebeveiligingsbeleid

Informatiebeveiliging is onmisbaar voor iedere organisatie om risico's op datalekken en cybercriminaliteit zo klein mogelijk te houden. Van eenmansbedrijf tot overheidsorgaan, non-profitorganisatie of multinational, informatiebeveiliging kan alleen succesvol werken als er vanaf de basis goed over is nagedacht en als het is uitgewerkt in een actueel beleid op papier.

Dit standaard template wordt aangeboden door The Trusted Third Party (TT3P) aan relaties en kan vrij worden gebruikt en aangepast door organisaties om zelf een beleid te ontwikkelen en vast te leggen.

Met vriendelijke groet,

Cyber Security Team van TT3P

[DIT IS EEN INTRODUCTIE U KUNT DEZE TEKST UIT UW PLAN VERWIJDEREN]

Wat is cyber security?

Cyber security is het pakket van activiteiten en maatregelen gericht op het voorkomen van cyber aanvallen. Een cyberaanval is een digitale aanval gericht op systemen, netwerken en programma's van een organisatie, met als doel om systemen te vergrendelen, onklaar te maken, data te stelen of data te vergrendelen. Cyber security is een onderdeel van het totale pakket van informatiebeveiligingsmaatregelen van een organisatie. De wet (Artikel 32 EU-AVG "Beveiliging van de verwerking) schrijft voor dat iedere organisatie, groot en klein, passende technische en organisatorische maatregelen moet nemen om digitaal veilig te werken en persoonsgebonden informatie te beschermen. Daarnaast schrijft de wet ook voor dat datalekken gemeld moeten worden bij de Autoriteit Persoonsgegevens.

Waarom een informatiebeveiligingsbeleid?

Elke organisatie moet wettelijk de basis informatiebeveiliging organiseren. De AVG zegt hierover in artikel 32 EU-AVG "Beveiliging van de verwerking" letterlijk:

"Rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen, treffen de verwerkingsverantwoordelijke en de verwerker passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen, die, waar passend, onder meer het volgende omvatten:

a) de pseudonimisering en versleuteling van persoonsgegevens;
b) het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen;
c) het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen;
d) een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.

Er dienen dus passende technische en organisatorische maatregelen te worden genomen. Bovendien zal een organisatie steeds vaker moeten aantonen in samenwerkingen dat informatiebeveiliging onder controle is. Dat kan met een beleidsdocument.

Hoe zo'n beleid moet worden vormgegeven kunt u terugvinden in dit document. Wij kunnen ons voorstellen dat u tegen het opstellen van zo'n document opziet, maar we adviseren u hier toch energie in te stoppen. Dat is nu belangrijker dan ooit met alle vormen van cybercrime, zoals bijvoorbeeld phishing, gijzelsoftware (ransomware) en DDoS-aanvallen.

Wat zijn passende technische en organisatorische maatregelen?

De sleutel zit hier in het woord 'passend'. **Passend** betekent dat de invulling per organisatie kan verschillen. En dat is ook terecht. De ene organisatie is nou eenmaal niet de andere als het gaat om beveiliging van informatie.

Technische maatregelen zijn software en hardware oplossingen om cyberaanvallen tegen te gaan en andere informatiebeveiligingsrisico's te beperken. Denk hierbij bijvoorbeeld aan ICT-Infrastructuur die up to date is en de juiste security mogelijkheden biedt, beveiliging van in de cloud opgeslagen informatie (belangrijk in het kader van cloudificatie van netwerken en applicaties), netwerk beveiliging, toegangsbeveiliging, beveiliging tegen virussen, ransomware en malware, versleuteling van gegevens, penetratietesten en gebruik maken van ethisch hacken voor het testen van systemen en applicaties. Deze producten en diensten worden doorgaans geleverd door IT-leveranciers.

Organisatorische maatregelen zijn alle voorzieningen die zijn getroffen om ervoor te zorgen dat een organisatie informatiebeveiligingsbeleid opzet, procedures maakt, uitvoert en controleert en dat de technische maatregelen blijven werken. Bij organisatorische maatregelen kunt u bijvoorbeeld denken aan het aanstellen van information security officer, het vormen en, het aanleggen van een security administratie, het opzetten van een incident response procedure (wat moet u doen als u bijvoorbeeld nu gehackt bent), cyber security awareness opzetten voor medewerkers, medewerkers cyber security opleiding of cyber security cursus laten volgen, cyber security training en e-learning aan medewerkers bieden en phishing simulaties uitvoeren.

Wat zijn de gevolgen van een cyber aanval?

Een cyber aanval kan vergaande gevolgen voor een organisatie hebben. En zelfs uitmonden in een faillissement. Nadat een cyber crimineel in de systemen van een organisatie is binnengedrongen, zal deze proberen de systemen te vergrendelen met gijzelsoftware (ook wel ransomware) en de organisatie daarna onder druk zetten om losgeld te betalen. Daarnaast zijn er meer schadeposten. Bijvoorbeeld juridische kosten en kosten voor cyber security consultants van gespecialiseerde cyber security bedrijven. In het kort gaat het over financiële gevolgen die gepaard gaan met:

- Onderbreking van uw organisatieactiviteit
- Chantabele positie
- Herstel- en juridische werkzaamheden
- Hoge boetes voor datalekken
- Schadeclaims van benadeelden
- Reputatieschade
- Management tijd

Wat is een datalek?

Niet iedere cyber aanval veroorzaakt ook daadwerkelijk een datalek. Een datalek, in de zin van de wet, is een lek waar persoonsgegevens bij zijn betrokken. Dat zijn gegevens die direct of indirect herleidbaar zijn tot een individu. Bij een datalek gaat het om ongeautoriseerde toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens bij een organisatie. Betrokken personen kunnen hierdoor schade ondervinden. Bijvoorbeeld als gevolg van identiteitsdiefstal.

Een datalek moet binnen 48 uur gemeld worden bij de Autoriteit Persoonsgegevens. En ook bij de personen van wie de gegevens gelekt zijn. Op zichzelf is een datalek niet beboetbaar, tenzij het lek is veroorzaakt door dermate slechte informatiebeveiliging dat een organisatie had kunnen weten dat het risico op een lek hoog was.

Het niet melden van een datalek kan een boete opleveren van maximaal 20 miljoen euro of 4% van de wereldwijde jaaromzet.

Tot slot

Als uw organisatie data verwerkt of informatie technologie gebruikt in de bedrijfsvoering, en dat doet vrijwel elke organisatie, is het opstellen van een Informatiebeveiligingsbeleid bepaald geen luxe. Het dwingt u tot het gestructureerd benaderen van informatiebeveiliging en dat is noodzakelijk.

Mocht u er niet uitkomen, vragen hebben of hulp nodig hebben, laat het ons dan weten op:

- **088 - 38 38 38 3**
- of per e-mail op info@tt3p.nl

Wij helpen u graag.

[De teksten in het blauw zijn bedoeld als toelichting in dit standaard document en deze kunt u later verwijderen. Het lukt nooit helemaal om weg te blijven van 'vaktaal' in een document als dit. Gelukkig kunt u alle begrippen opzoeken op het internet. Maar u mag ons ook altijd bellen en wij helpen u verder. En nee daar sturen we ook niet direct een factuur voor.

De absolute basismaatregelen voor elke organisatie zijn:

- Zorg dat elke applicatie en elk systeem voldoende loginformatie genereert
- Pas multifactor authenticatie toe waar nodig
- Bepaal wie toegang heeft tot uw data en diensten
- Segmenteer netwerken
- Versleutel opslagmedia met gevoelige bedrijfsinformatie
- Controleer welke apparaten en diensten bereikbaar zijn vanaf het internet en bescherm deze
- Maak regelmatig back-ups van uw systemen en test deze
- Installeer altijd direct software-updates]

1 INLEIDING

[WERK DE ONDERSTAANDE PUNTEN UIT]

- Geef een introductie van uw organisatie en wat deze doet;
- Beschrijf hoe uw organisatie ICT inzet;
- Beschrijf welke type (persoons)gegevens uw organisatie verwerkt;
- Beschrijf met welk doel u dit informatiebeveiligingsbeleid opstelt.

[Tip: het bovenstaande moet duidelijk maken wat u te beschermen hebt, dus welke systemen en welk type gegevens. Data is alle digitale informatie van een organisatie. Dus dat gaat om gegevens van personen, maar ook om bijvoorbeeld productiedata, intellectuele eigendommen etc. Maar denk ook aan fysieke documenten, zoals mappen met arbeidsovereenkomsten of contracten met klanten. Deze paragraaf moet duidelijk maken dat uw organisatie planmatig over informatiebeveiliging heeft nagedacht en dat het beleid wordt gedragen door de top van uw organisatie.

Voorzie dit informatiebeveiligingsbeleid van een naam van de auteur, datum en versienummer.]

2 INFORMATIEBEVEILIGING

2.1 DEFINITIE

- Beschrijf wat uw organisatie verstaat onder informatiebeveiliging.

2.2 DOELSTELLINGEN EN SCOPE

- Geef een opsomming van de doelstellingen van uw Informatiebeveiligingsbeleid;
- Beschrijf de ambitie van uw organisatie op het gebied van informatiebeveiliging;
- Beschrijf er wat binnen uw organisatie valt onder het Informatiebeveiligingsbeleid;
- Beschrijf op wie het Informatiebeveiligingsbeleid is gericht.

[Tip: met ambitie wordt bedoeld dat u een afgewogen beslissing heeft genomen over de hoeveelheid beheersmaatregelen en de investering hierin. Het is geen optie dat u niets doet of ad hoc maatregelen treft. Dat maakt u te kwetsbaar, maar u bent ook geen bank of een kerncentrale waarschijnlijk. Beschrijf verder voor wie het document bedoeld is. Bijvoorbeeld medewerkers, klanten, aandeelhouders, financiers etc.]

3 BELEIDSUITGANGSPUNTEN

- Beschrijf hoe het informatiebeveiligingsmanagement proces is ingericht (bijvoorbeeld met een planning en control cyclus) en welke uitgangspunten hierbij van toepassing zijn, zoals:
    - Wet- en regelgeving;
    - Management verantwoordlijkheden;
    - Bewustwording;
    - Borging van beveiligingsaspecten beschikbaarheid, integriteit en vertrouwelijkheid;
    - Gehanteerde principes (bijv. “zo min mogelijk rechten”);
    - Regelmatige herziening van beleid en uitvoering van audits;
    - Eigendom van informatie;
    - Samenwerkingsverbanden met externe partijen en bijbehorende overeenkomsten;
    - Gedragsregels.

[Tip: met een planning-en-control cyclus wordt informatiebeveiliging op een systematische manier uitgevoerd. Bij informatiebeveiliging is de PDCA (plan-do-check-act) cyclus gangbaar. PDCA staat een planmatige benadering van informatiebeveiligingsrisico's voor. Hierbij worden beheersmaatregelen passend bij de hoogte van de risico's en gevoeligheid van systemen en data geïmplementeerd, gecontroleerd en beheerd.

De wet zegt bijvoorbeeld over de beveiliging van persoonsgegevens (en die heeft echt vrijwel elke organisatie in huis):

AVG artikel 24 lid 1

Rekening houdend met de aard, de omvang, de context en het doel van de verwerking, alsook met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen, treft de verwerkingsverantwoordelijke (dat is uw organisatie) passende technische en organisatorische maatregelen om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met deze verordening wordt uitgevoerd. Die maatregelen worden geëvalueerd en indien nodig geactualiseerd.

U moet dus een 'levend systeem' creëren. Een continu proces.]

4 ORGANISATIE

- Beschrijf hoe de verantwoordelijkheden, taken en bevoegdheden met betrekking tot informatiebeveiliging zijn geregeld;
- Plaats een organigram van uw organisatie en beschrijf deze bondig.

[Tip: zorg altijd dat de werkzaamheden voor informatiebeveiliging duidelijk bij een persoon zijn belegd en dat er is nagedacht over afwezigheid van een dergelijk persoon door ziekte, vakantie etc. In die gevallen moet cyber security ook geborgd zijn namelijk. Het kan ook zijn een expert van buitenaf wordt ingehuurd om deze werkzaamheden te verrichten. De eindverantwoordelijkheid voor informatiebeveiliging dient ook in de top van een organisatie te zijn belegd.]

5 INFORMATIEBEVEILIGING DOCUMENTEN

- Geef een opsomming en beschrijving van de documenten die uw organisatie in het kader van informatiebeveiliging heeft opgesteld of waarvan informatiebeveiliging deel uit maakt, zoals:
    - dit Informatiebeveiligingsbeleid;
    - arbeidsreglementen en gedragsregels;
    - service diensten overeenkomsten (SLA's);
    - inhuur- en uitbestedingscontracten;
    - incident response plan.

[Tip: neem hier alle documenten op, waarin inhoud met betrekking tot informatiebeveiliging is opgenomen. Dat zijn dus ook (standaard)contracten met bijvoorbeeld leveranciers, partners, opdrachtgevers en medewerkers. Doe er ook een korte beschrijving bij. Het doel is het hebben van een overzicht van bedoelde documenten om ook hierin een actualisatie of wijziging aan te kunnen brengen als het beleid van de organisatie wijzigt.

Het incident response plan is een belangrijke in het kader van bijvoorbeeld cyber security. Dit plan is een plan waarin de procedures zijn vastgelegd die in werking treden als een organisatie wordt getroffen door een cyber aanval.]

6 CONTROLE EN NALEVING

- Beschrijf hoe er binnen de organisatie doorlopend wordt gecontroleerd op naleving van dit Informatiebeveiligingsbeleid en waarop die controles zijn gericht (zoals op de in het informatiesysteem vastgelegde gegevens, op de inventarisatie van risico's, op de genomen beveiligingsmaatregelen en op de samenhang hiertussen);
- Beschrijf of en hoe er ook door een externe onafhankelijke partij frequent op naleving van dit Informatiebeveiligingsbeleid wordt gecontroleerd indien dat van toepassing is).

[Tip: Controles zijn essentieel om vast te stellen (in welke mate) de gewenste doelen voor het compliant zijn/blijven met informatiebeveiligingsvereisten zijn behaald. Voor het uitvoeren van succesvolle controles, stel de volgende vragen:

1. Wat wordt er gecontroleerd?
2. Hoe wordt er gecontroleerd en hoe vaak wordt er gecontroleerd?
3. Door wie wordt er gecontroleerd?
4. Waarin wordt de controle vastgelegd?
5. Wie legt vast dat de controle is uitgevoerd en gerapporteerd?]

7 VERANTWOORDELIJKHEDEN

- Beschrijf hoe de verantwoordelijkheden zijn belegd m.b.t onderhoud van het Informatiebeveiligingsbeleid en van de voorgeschreven geïmplementeerde beheersmaatregelen;
- Beschrijf hoe de verantwoordelijkheden zijn belegd m.b.t het up-to-date houden van het Informatiebeveiligingsbeleid en het aanpassen van de beheersmaatregelen;
- Beschrijf hoe de verantwoordelijkheden zijn belegd m.b.t. de controle en naleving van de uitvoering van dit Informatiebeveiligingsbeleid.

8 DEELBELEID BESCHRIJVINGEN

8.1 SOFTWARE-MIDDELEN

Neem hier een overzicht of een verwijzing naar een overzicht op van welke software applicaties de organisatie inzet. Beschrijf daarbij de technische en organisatorische beheersmaatregelen die ervoor moeten zorgen dat de applicaties veilig werken en dat de security instellingen juist zijn geconfigureerd. Denk hierbij aan:

- Besturingssystemen;
- Applicaties en bijbehorende databases, gegevensbestanden, documentatie en procedurebeschrijvingen;
- Software as a Service (SaaS).

Beschrijf ook wat de gevolgen kunnen zijn als de beheersmaatregelen niet of niet juist worden toegepast of uitgevoerd, zoals een verhoogd risico op ongeautoriseerde toegang, datalekken, vernietiging of aantasting van gegevens, het niet beschikbaar zijn van de ICT-infrastructuur.

8.2 HARDWARE-MIDDELEN

Neem hier een overzicht of een verwijzing naar een overzicht op van welke hardware de organisatie inzet. Beschrijf daarbij de technische en organisatorische beheersmaatregelen die ervoor moeten zorgen dat de hardware-middelen veilig werken en dat de security instellingen juist zijn geconfigureerd. Denk hierbij aan:

- Werkplekken;
- Servers;
- Printers;
- Opslag;
- Netwerkcomponenten (switches, routers);
- Mobiele apparaten zoals tablets en smartphones.

Beschrijf ook wat de gevolgen kunnen zijn als de voorgeschreven beheersmaatregelen niet of niet juist zijn toegepast, zoals een verhoogd risico op ongeautoriseerde toegang, vernietiging of aantasting van gegevens of het niet beschikbaar zijn van de ICT-infrastructuur.

8.3 NETWERK

Beschrijf hier alle technische en organisatorische beheersmaatregelen die moeten zorgen voor een optimaal beveiligd netwerk. Denk hierbij aan:

- firewall inrichting
- eindpunt beveiliging (antivirus, anti-malware)
- Wi-Fi configuratie
- externe toegang.

Beschrijf ook wat de gevolgen kunnen zijn als de in dit beleid voorgeschreven beheersmaatregelen niet of niet juist worden toegepast, zoals ongeautoriseerde toegang, vernietiging of aantasting van gegevens of het niet beschikbaar zijn van de ICT-infrastructuur.

8.4 INCIDENTEN

Beschrijf hier alle technische en organisatorische beheersmaatregelen die ervoor moeten zorgen dat een incident adequaat gedetecteerd, gemeld en behandeld wordt. Het primaire doel van incidentbeleid is de ontwikkeling van een goed begrepen en voorspelbare reactie op schadelijke gebeurtenissen en computerinbraken in de meest brede zin van het woord. Leg hier een duidelijke link naar het incident response plan van de organisatie.

Beschrijf ook wat de gevolgen kunnen zijn als de in dit beleid voorgeschreven beheersmaatregelen niet of niet juist worden toegepast, zoals dat een incident niet, niet tijdig en/of niet adequaat gedetecteerd, gemeld en behandeld wordt, waardoor het risico op uitval van bedrijfsvoering processen of schade ontstaan als gevolg van een incident onacceptabel groot is.

8.5 WIJZIGINGENBEHEER

Beschrijf hier alle voorgeschreven beheersmaatregelen welke ervoor moeten zorgen dat er gecontroleerd wijzigingen doorgevoerd kunnen worden (change management) in de ICT-infrastructuur.

Beschrijf ook wat de gevolgen kunnen zijn als de in dit beleid voorgeschreven beheersmaatregelen niet of niet juist worden toegepast, zoals dat wijzigingen dan kunnen

leiden tot negatieve gevolgen voor de ICT-infrastructuur door onderbrekingen en beveiligingsincidenten.

8.6 BACK-UP EN HERSTEL

Beschrijf hier alle technische en organisatorische beheersmaatregelen die ervoor moeten zorgen dat er corrupte, verloren, ongeautoriseerd versleutelde of vernietigde bedrijfsinformatie hersteld kan worden. Een goede back-up op meerdere plekken on en offline in een juist back-up schema zorgt ervoor dat een herstel ook daadwerkelijk succesvol kan zijn.

Beschrijf ook wat de gevolgen kunnen zijn als de beheersmaatregelen niet of niet juist worden toegepast, zoals dat herstel van gegevens en/of programmatuur na het zich voordoen van een (cyber)incident of een calamiteit (ramp) niet of niet afdoende mogelijk is. Dit kan de bedrijfsvoering ernstig beschadigen of zelfs stilleggen. Bovendien kan wetgeving die eisen stelt aan back-up en herstel hierdoor worden overtreden.

8.7 VEILIGHEIDSBEWUSTZIJN BIJ MEDEWERKERS

Beschrijf hier alle technische en organisatorische beheersmaatregelen die ervoor moeten zorgen dat alle medewerkers zijn getraind in het (her)kennen van regels, verantwoordelijkheden, informatiebeveiligingsrisico's en het gebruik van beveiligingsprocedures.

Beschrijf ook wat de gevolgen kunnen zijn als de beheersmaatregelen niet of niet juist worden toegepast. Zo kan onvoldoende bewustzijn ervoor zorgen dat medewerkers risico's niet (h)erkennen hetgeen kan leiden tot gevaarlijk gedrag. Daarnaast heeft een gebrek aan risicobewustzijn een negatief effect op het beheersen van risico's in het algemeen. Denk hierbij specifiek ook aan nieuwe medewerkers die in dienst treden. Een succesvolle bewustzijnscyclus heeft een continu karakter. *Eén training is geen training.*

8.8 INCIDENT RESPONSE

Beschrijf hier alle technische en organisatorische beheersmaatregelen die ervoor moeten zorgen dat de gevolgen van een beveiligingsincident geminimaliseerd worden en de organisatie in staat stellen de meest kritische functies snel weer op te starten. Maak een Incident Response Plan en leg hier een duidelijke link naar dat plan.

Beschrijf ook wat de gevolgen kunnen zijn als de beheersmaatregelen niet of niet juist worden

toegepast. Zo kan de business continuïteit groot gevaar lopen na een calamiteit als rollen en acties niet, niet tijdig of niet afdoende kunnen worden uitgevoerd doordat ze niet in een beleid en plan beschreven zijn.

8.9 KWESTBAARHEDEN

Beschrijf hier alle technische en organisatorische beheersmaatregelen die ervoor moeten zorgen dat op basis van nieuwe informatie kwetsbaarheden onderkend worden en er vervolgens acties genomen kunnen worden om deze kwetsbaarheden binnen uw organisatie te identificeren en te herstellen. Als bron voor nieuwe ontdekte kwetsbaarheden kunt u www.ncsc.nl gebruiken.

Beschrijf ook wat de gevolgen kunnen zijn als de beheersmaatregelen niet of niet afdoende zijn geïmplementeerd. Zo loopt de organisatie het risico dat kwetsbaarheden niet worden onderkend en er niet aan een oplossing kan worden gewerkt, wat het risico op ongeautoriseerde toegang, vernietiging of aantasting van gegevens of het niet beschikbaar zijn van de ICT-omgeving verhoogt.

8.10 ROLLEN EN TOEGANGSRECHTEN

Beschrijf hier alle technische en organisatorische beheersmaatregelen die ervoor moeten zorgen dat toegangsrechten van gebruikers correct worden toegepast en toegewezen op computers, op het netwerk en binnen applicaties conform hun rol(len).

Beschrijf ook wat de gevolgen kunnen zijn als de beheersmaatregelen niet of niet juist worden toegepast. Zo kan de organisatie een onacceptabel hoog risico lopen op ongeautoriseerde toegang, lekken, vernietiging of aantasting van gegevens of het niet beschikbaar zijn van de ICT-omgeving.

8.11 SOFTWARE ONTWIKKELING (INDIEN VAN TOEPASSING)

Beschrijf hier alle technische en organisatorische beheersmaatregelen die moeten zorgen voor het veilig ontwikkelen en onderhouden van eigen software. Hanteer het principe van security by design. Letterlijk vertaald: Veilig door ontwerp, in software-engineering, betekent dat softwareproducten dusdanig zijn ontworpen dat ze fundamenteel veilig te zijn.

Beschrijf ook wat de gevolgen kunnen zijn als de beheersmaatregelen niet of niet juist worden toegepast, zoals dat de ontwikkelde software niet voldoet aan de hieraan gestelde beveiligingseisen. Dit verhoogt het risico op onveilige software door bijvoorbeeld ongeautoriseerde toegang, vernietiging of aantasting van gegevens.