

Vertrouwelijkheidsverklaring

Hiermee bevestig ik....

Voorletter(s):

Achternaam:

Zakelijk emailadres:

Plaats:

Datum:

Handtekening:

...de inhoud van dit document te hebben gelezen en begrepen,

...mij te realiseren dat ik (zeer-)vertrouwelijke informatie bewerk voor de werkzaamheden en de periode die overeen zijn gekomen

... mij te realiseren dat het bewerken van informatie in de brede zin bedoeld wordt: lezen, bewerken, opslaan, verwijderen en delen

... mij te realiseren dat informatie over cybersecurity **hazards, kwetsbaarheden** en **maatregelen** ook onbewust, onder bereik van kwaadwilligen **herleidbaar** kan zijn tot nieuwe kwetsbaarheden, een hoog hazard-risico betreft en kan leiden tot forse schade of letsel

... mij te realiseren dat lekken en ongeautoriseerd delen van **persoonsgegevens** (zoals camerabeelden, audiostreams en OV-chipkaartgegevens) eveneens een hoog hazard-risico betreft en kan leiden tot forse schade of letsel

... alleen met andere direct betrokkenen (Zeer-)Vertrouwelijke informatie mag delen; en waarbij betrokkenen medewerkers zijn van gemeente, leveranciers en partners waarvan bekend is dat zij deze Vertrouwelijkheidsverklaring hebben getekend.

... weet dat andere betrokkenen te identificeren zijn door de deelname aan de beveiligde omgeving en/of door aangeven van de cybersecurity officer

... vertrouwelijke informatie alleen op te slaan op een beveiligde computer/laptop, zich te vergewissen dat de computer/laptop beveiligd is (met persoonlijke identificatie zoals wachtwoord of bio-kenmerken en encryptie) en te delen via een beveiligde applicatie(omgeving) en een beveiligde verbinding (certificeerd versleuteld)

... zeer-vertrouwelijke informatie alleen te bewerken door middel van beveiligde omgeving en verder extreem terughoudend is met het opslaan op en delen naar een persoonlijk en beveiligde applicaties/omgevingen en beveiligde computers/laptops

... zich te realiseren dat de standaard kantoorautomatiseringomgeving(en) geschikt is om vertrouwelijke informatie te bewerken, maar NIET GESCHIKT is **Ze**er-Vertrouwelijke ('Geheime') informatie te bewerken en (vertrouwelijk) te delen met partners en leveranciers, vanwege de relatieve openheid van het systeem voor niet betrokken collega's en de kans op (onbewust) delen van informatie

... andere betrokkenen attent te (blijven) maken op het (blijvend) handhaven van maatregelen en dit zonder terughoudendheid te bespreken indien van toepassing en eventueel te melden bij de cybersecurity officer, die de melding vertrouwelijk zal behandelen met in acht-neming van de privacy-regelgeving (AVG)

... zich te realiseren dat indicaties voor malversaties vaak een gevolg van frustraties/wrok, persoonlijke en/of financiële problemen en dat indien die indicaties van een Betrokkenen zich voordoen, contact wordt opgenomen met de Integriteitscommissie van de betrokken organisatie, die de melding vertrouwelijk zal behandelen met in acht-neming van de privacy-regelgeving (AVG)

... zich te realiseren dat de cybersecurity officer de toegang tot (zeer-)vertrouwelijke informatie (tijdelijk) kan stopzetten door de toegang tot de beveiligde omgeving en (zeer-)ver-trouwelijke informatie te ontzien en te verwijderen van de eigen (beveiligde) computer/laptop indien het dienstverband of contract wordt beëindigd

... zich te realiseren dat het Nederlands strafrecht van toepassing is op het opzettelijk ple-gen van inbreuk op de vertrouwelijkheid en integriteit van (Zeer-)Vertrouwelijke informatie

Dit document geeft de handvatten voor

- het bepalen van de **vertrouwelijkheidsniveau's** van cybersecurity informatie en voor
- het vertrouwelijk delen/opslaan/bewerken van cybersecurity informatie en voor
- het gebruik van de vertrouwelijkheidsverklaring voor betrokkenen.

Vertrouwelijkheidsniveau's en Vertrouwelijkheidsmaatregelen

Vertrouwelijkheidsniveau's

De vertrouwelijkheidsniveaus zijn bedoeld om **medewerkers van GVB, (keten)partners en leveranciers** (Betrokkenen) die samen werken aan de OT te laten vaststellen of en in welke mate informatie over cybersecurity vertrouwelijk behandeld dient te worden. Voor het delen van cybersecurity-informatie voor OT gelden de 3 Vertrouwelijkheidsniveau's hieronder.

Vertrouwelijkheidsniveau's Cybersecurity OT

1. Bedrijfsvertrouwelijk
2. Vertrouwelijk

Ad 1. Bedrijfsvertrouwelijk

Dit betreft informatie die **inhoudelijk** niet gaat over cybersecurity hazards, kwetsbaarheden of maatregelen. Hiervoor geldt de normale vertrouwelijkheid voor vaste en tijdelijke medewerkers. Procesinformatie en informatie over het ISMS zijn niet-vertrouwelijk, tenzij het (toch) inhoudelijke informatie betreft. Deze informatie mag worden gedeeld via de (gewone) email, opgeslagen worden in documenten op de devices van de betrokken organisaties. Deze documenten mogen onversleuteld worden opgeslagen. Het betreft informatie die niet bedoeld is voor openbare/publieke publicaties of distributie in welke vorm dan ook.

Ad 2. Vertrouwelijk

Dit betreft **inhoudelijke informatie** over

- technische informatie van of over systemen en processen die in handen van kwaadwilligen tot digitale aanvallen of besmettingen kunnen leiden en
- cybersecurity **hazards, kwetsbaarheden of maatregelen**, waarvan
 - dat gedetailleerde c.q. specifieke inhoudelijke informatie over cybersecurity hazards, die **herleidbaar** kunnen zijn naar kwetsbaarheden en maatregelen, of
 - waarvan nog niet zeker is cq nog niet is vastgesteld wat de cybersecurity hazard-risico is, of
 - waarvan door cybersecurity board is vastgesteld dat de Hazard-risico Middel of Hoog is.
- **persoonsgegevens**, zoals camerabeelden, OV-chipkaartgegevens en audiostreams

Deze informatie mag alleen via de Beveiligde Omgeving worden opgeslagen en gedeeld (niet via de (gewone) email). Het opslaan van locale documenten op eigen devices, mag alleen indien deze documenten versleuteld zijn opgeslagen. Het downloaden van documenten uit de Beveiligde Omgeving dient te worden vermeden.

Vertrouwelijkheidsmaatregelen

Om (Zeer)-Vertrouwelijke informatie te bewerken (opslaan, delen, aanpassen, verwijderen) zijn de volgende maatregelen van toepassing, te weten:

1. Vertrouwelijkheidsverklaring

Vertrouwelijke informatie mag alleen gedeeld worden tussen **Betrokkenen** die een Vertrouwelijkheidsverklaring hebben getekend.

Opmerking.

Juridisch gezien is geheimhoudingsverklaring die door medewerkers is getekend voldoende. De vertrouwelijkheidsverklaring geeft een expliciete aandacht aan het werken met en delen van vertrouwelijke informatie.

2. Versleutelde/Vergrendelde documenten

Vertrouwelijke informatie dient vergrendeld (versleuteld) te worden opgeslagen en gedeeld door middel van het aanbrengen van een wachtwoord op het document. Het wachtwoord wordt separaat aan de lezer gedeeld, via een andere medium (zoals sms) of via een separate email in een beveiligd netwerk. De standaard wachtwoordfuncties van bijvoorbeeld Microsoft of Apple worden als voldoende secure beoordeeld.

3. Beveiligde omgeving

De Beveiligde omgeving is bedoeld om Betrokkenen te faciliteren om informatie Vertrouwelijk op een beveiligde manier te behandelen. Veelal waar het inhoudelijke cybersecurity-informatie betreft; zoals risico-analyses, kwetsbaarheden, maatregelen etc. Via de Beveiligde omgevingen is voor alle Betrokkenen inzichtelijk welke personen een Vertrouwelijkheidsverklaring hebben getekend.

Met bewerken wordt (in brede zin) bedoeld: opslaan, delen, aanpassen en verwijderen.

De Cybersecurity-officer OT geeft persoonlijke toegang tot de Beveiligde Omgeving aan een Betrokkene, nadat de Betrokkene de Vertrouwelijkheidsverklaring heeft ondertekend en overhandigd aan de Cybersecurity Officer.

De Cybersecurity-officer OT slaat de getekende Vertrouwelijkheidsverklaring op de Beveiligde Omgeving en deelt met (groepen van) Betrokkenen, welke andere Betrokkenen ook toegang hebben tot die delen van de Vertrouwelijke informatie.

De volgende beveiligingseisen worden gesteld aan Beveiligde Omgeving:

□ de cybersecurity officer beheert de toegang van de Betrokkenen

□ maakt persoonlijke toegang mogelijk over de organisatorische grenzen van de betrokken partijen heen, zoals leveranciers en GVB, teneinde een beveiligde samenwerking tussen Betrokkenen te realiseren

□ kent indelingsmechanismen om delen van de cybersecurity-informatie af te scher-
men (need-to-know) om de kans op (onbewuste) inbreuken te minimaliseren, door
middel van groepen van Betrokkenen voor het delen van de Vertrouwelijke informa-
tie. Dit betreft het toegang krijgen, hebben en beëindigen tot informatie.

□ de Betrokkenen kunnen zien wie de andere Betrokkenen zijn binnen de Groep.

□ stimuleert (centrale) enkelvoudige opslag en belemmert (decentrale) meervoudige
opslag, teneinde de kans fors te reduceren op (onbewuste) inbreuken van de ver-
trouwelijkheid en integriteit.

□ kent stringente technische en organisatorische informatiebeveiligingsmaatregelen
die minstens voldoen aan of vergelijkbaar zijn met ISO27001, inclusief de vigerende
normatieve kaders, die juist ook gelden voor de applicatie-ontwikkelaar en hosting

□ heeft een beveiligd meldpunt (postbus) om De (operationele) Actoren van de ope-
rationele MET-systemen cybersecurity Incidenten op een beveiligde manier te kun-
nen laten melden en daarna te kunnen laten opvolgen (afhandelen) door Betrokke-
nen.

□ heeft functies om beveiligingszaken te kunnen bespreken en af te handelen met
Betrokkenen: bespreking, prioritering, selectie, filtering, sortering, acties en work-
flow; inclusief het formeel nemen van besluiten; maakt het mogelijk te kunnen vol-
doen aan ISO15489.

□ maakt het mogelijk een oefen/educatie-omgeving in te richten voor Betrokkenen