DEA.Amsterdam B.V. hecht grote waarde aan het veilig omgaan met systemen en persoonlijk identificeerbare informatie (PII). Naast dat daartoe een wettelijke verplichting op ons rust is er ons er veel aan gelegen het in ons gestelde vertrouwen hoog te houden en te borgen. Wij streven dit altijd naar laatste stand van technische mogelijkheden uit te voeren. In deze security brief vindt u kort beschreven welke domeinen en onderliggende acties wij in ons security bewustzijn onderscheiden.

Security bewustzijn is een levend onderwerp waardoor dit document telkens zal worden bijgewerkt als voortschrijdend inzicht en ontwikkelingen daartoe aanleiding geven. Voor vragen over dit document kunt contact opnemen met:

Jeffrey Bleijendaal, Security Officer DEA.Amsterdam, 020-2374705

FYSIEKE **VEILIGHEID**

- Op alle computer apparatuur waarop wij werken moet met een gekend account ingelogd worden (gast accounts staan we niet toe);
- Wachtwoordrotatie wordt afgedwongen. Samenstelling en herhaling moeten voldoen aan voorwaarden;
- Er is een actief software update beleid. Zodra security patches beschikbaar zijn worden deze direct uitgerold;
- Gegevens opslag op alle computers is altijd versleuteld (Bitlocker);
- Met regelmaat vinden PEN testen plaats op netwerk & beveiliging;
- Computerapparatuur wordt beveiligd opgeslagen;
- Kantoor locatie is beveiligd met een goedgekeurd alarmsysteem.

ORGANISATORISCHE **VEILIGHEID**

- Een security officer is benoemd. Deze zorgt voor de coördinatie en monitoring van de security & privacy gerelateerde processen en escalaties;
- 2x per jaar wordt Ematters (het netwerk en de systemen) gecontroleerd door een externe ethische hacker. De rapportages en adviezen worden actief geëvalueerd en indien nodig actie ondernomen;
- Actief bewustwordingsbeleid voor security gerelateerde onderwerpen;
- Wachtwoorden van platformen worden versleuteld opgeslagen in een softwarematige wachtwoord kluis;
- Wij werken veel met als PII geclassificeerde gegevens. Voor veel operaties moeten transformaties op deze gegevens worden uitgevoerd. Dat kan gebeuren op workstations: eventueel nog aanwezige PII wordt telkens uiterlijk aan het eind van elke werkdag permanent daarvan zijn verwijderd;
- In geval dat PII moet worden verstuurd wordt deze versleuteld en verzonden via beveiligde systemen We nemen een proactieve rol aan om klanten te informeren over de meest veilige en werkbare wijze van het transport van PII;
- PII en klantdata wordt opgeslagen op systemen binnen de Europese juridische ruimte. Indien data opgeslagen dient te worden in Amerika dan alleen bij partijen die zijn gecertificeerd volgens de Amerikaanse Privacy Shield;
- Processen voor uitvragen, verwerken, transport en opslag van PII zullen altijd naar de laatste stand van de techniek worden ontworpen, gebouwd en uitgevoerd. Indien de toepassing en aard van de gegevens dit vereisen, verzorgen we security audits daarvoor gecertificeerde een erkende partij.

SOCIALE VEILIGHEID **VEILIGHEID**

- Valide identificatie/authenticatie zijn verplicht voor het wijzigen van accountgegevens;
- Verwijderings- of inzageverzoeken worden niet gehonoreerd zonder valide identificatie/authenticatie.