

Checklist Email

Het is belangrijk om veiligheidsproblemen te voorkomen met persoonsdocumenten of -gegevens. Om een zo hoog mogelijke veiligheid te waarborgen bij gebruik van digitale communicatie is deze checklist opgesteld.

Veiligheidsclassificaties

Security Level 1 (Lage impact)

Lage impact. Informatie waarbij de kans op misbruik gering is.

Security Level 2 (Medium impact)

Medium impact. Informatie die gebruikt kan worden voor bijvoorbeeld illegale online transacties of bestellingen. Versleutelde email wordt aangeraden.

Security Level 3 (Hoge impact)

Hoge impact. De informatie kan gemakkelijk misbruikt worden en de schade kan vrij ernstig zijn. Dit kan bijvoorbeeld identiteitsfraude zijn. Versleutelde email is verplicht.

Security Level 4 (Extreme impact)

Extreme impact. De informatie kan heel makkelijk misbruikt worden en dient niet gedeeld te worden maar mocht dit toch nodig zijn dan is uiterste zorgvuldigheid vereist. Het gebruik van versleutelde email is verplicht en deze moet met een wachtwoord van 32 tekens beveiligd worden, dit wachtwoord wordt los verzonden. Tevens moet er een self-destruct in de mail zitten zodat deze zich binnen 3 dagen vernietigt.

Door overheid uitgegeven documenten

- Bevat volledige geboortenaam
 - **SL3**
- Bevat geboortedatum
 - **SL1**
- Bevat volledige naam, geboortedatum en adres
 - **SL3**
- Bevat burgerservicenummer
 - **SL4**
- Bevat documentnummer
 - **SL2**
- Bevat een combinatie van persoonsgegevens
 - Afhankelijk van het type persoonsgegevens, het hoogste *security level* moet gehandhaafd worden

Bij twijfel dient minimaal SL2 gebruikt te worden.

Financial documents

- Bevat volledige naam en adres
 - **SL2**
- Bevat achterkant inclusief handtekening

- **SL3**
- Bevat vervaldatum, CCV-code, pasnummer of een combinatie van dezen
 - **SL4**

Andere documenten en gegevens

- Bevat (gedeeltelijke) wachtwoorden
 - **SL4**

Revision #8

Created 25 December 2020 13:42:06 by Nicky Hendriks

Updated 8 April 2022 05:24:51 by Nicky Hendriks