

Beveiligingsrichtlijnen Groenink advies

Annius Groenink

22 december 2010

Groenink advies spant zich in om uitermate zorgvuldig om te gaan met gegevens van derden. Tegelijkertijd wordt erop gelet dat de opdrachtgever het beveiligingsbeleid niet als lastig ervaart. Tenzij anders afgesproken commiteert Groenink advies zich aan onderstaande richtlijnen.

Algemene beveiliging

- Alle computersystemen zijn alleen toegankelijk met gebruik van een sterkwachtwoord van minimaal 8 karakters met minimaal 3 niet-letters en minimaal 1 leesteken.
- Groenink advies gebruikt laptop computers voor werk op locatie.
- Laptopsystemen worden beveiligd middels een BIOS password en drive encryption.
- Laptopsystemen mogen in slaapstand worden gezet, maar kunnen vanuit slaapstand alleen worden geactiveerd door het invoeren van een wachtwoord.
- Laptopsystemen worden niet onbeheerd ingelogd achtergelaten.
- Voor bestandsoverdracht op locatie kan een memory stick worden gebruikt. Bestanden op de memory stick worden na overdracht direct verwijderd.
- Servers, computersystemen en netwerken worden op effectieve wijze beveiligd tegen wederrechtelijke (netwerk-)toegang door onbevoegden.
- Servers en vaste computersystemen van Groenink advies staan op een vaste plaats die alleen voor Groenink advies toegankelijk is.
- Backups van alle gegevens van klanten van GA worden alleen op een vaste plaats bewaard die alleen voor Groenink advies toegankelijk is.

Omgang met privacy-gevoelige gegevens

- Groenink advies treedt op als databewerker en zet alle van opdrachtgevers verkregen gegevens uitsluitend in zover direct nodig voor de met opdrachtgever afgesproken projectdoelen.
- Privacygevoelige gegevens zijn ten minste: gegevens van opdrachtgevers over derden, financiële gegevens, gegevens waarvan redelijkerwijs kan worden begrepen dat deze extra dienen te worden beveiligd, en alle gegevens die expliciet als gevoelig worden aangemerkt.
- Privacygevoelige gegevens worden niet zonder voorafgaande telefonische afstemming verstuurd per e-mail of andere kanalen met beperkte betrouwbaarheid.
- Privacygevoelige gegevens worden maximaal 3 maanden na afloop van een opdracht bewaard en daarna vernietigd.
- Voor klantgegevens die niet zijn aangemerkt als privacygevoelig – bijvoorbeeld het GA extranet - wordt een passende, door Groenink advies afdoende geachte toegangsbeveiliging toegepast. Het niveau van beveiliging moet voor opdrachtgever altijd helder zijn.