Privacybeleid Cobijt

Datum: 25 juli 2018
Versie: 1.0
Van: Paul Schmitz

1. Algemeen

Het bestuur van COBIJT onderkent dat het toenemende gebruik van datacommunicatiemogelijkheden, de complexiteit van en verwevenheid tussen geautomatiseerde systemen, de massaliteit van de dagelijkse communicatie, de omvang van de bestanden alsmede de toenemende professionalisering van de computercriminaliteit leiden tot een grote afhankelijkheid en kwetsbaarheid van de geautomatiseerde informatievoorziening binnen COBIJT. De risico's die hiermee samenhangen zijn aanzienlijk en kunnen een bedreiging vormen voor de vertrouwelijkheid, integriteit en continuïteit van de informatievoorziening en daarmee indirect voor het imago van COBIJT.

2. Eindverantwoordelijkheid

Er is geen afzonderlijke Functionaris voor de gegevensbescherming (FG) aangesteld.
Gelet op de mogelijke impact van verstoringen op het imago van COBIJT berust de eindverantwoordelijkheid voor het beleid inzake de beveiliging en de interne controle van de geautomatiseerde informatievoorziening bij het bestuur van COBIJT.

3. Doelstelling en doelgroep

Dit document maakt deel uit van het algehele beveiligingsbeleid van COBIJT. De doelstelling van dit document inzake de vertrouwelijkheid, integriteit en continuïteit van de informatievoorziening van COBIJT luidt:
'Het bieden van een raamwerk van beleidsuitgangspunten met betrekking tot de exclusiviteit, integriteit en beschikbaarheid van de informatievoorziening, waarbinnen een evenwichtig (doeltreffend en doelmatig) stelsel van onderling samenhangende maatregelen ontwikkeld wordt, teneinde de informatievoorziening te beschermen tegen interne en externe bedreigingen.'
Bestuur en secretariaat dienen ervoor zorg te dragen, dat aan de in dit document geformuleerde beleidsuitgangspunten wordt voldaan bij de inrichting van de organisatie, procedures, werkwijze en de daarbij gehanteerde informatiesystemen.

4. Beleidsuitgangspunten

De fysieke en logistieke beveiliging van COBIJT is zodanig, dat de vertrouwelijkheid, integriteit en beschikbaarheid van de gegevens en gegevensverwerking gewaarborgd zijn.

Aanschaf, installatie en onderhoud van geautomatiseerde gegevensverwerkende systemen, alsmede inpassing van nieuwe technologieën, mogen geen afbreuk doen aan het niveau van veiligheid van de totale informatievoorziening.
Opdrachten aan derden voor het uitvoeren van werkzaamheden worden zodanig omgeven met maatregelen, dat er geen inbreuk op de vertrouwelijkheid, integriteit en continuïteit van de informatievoorziening kan ontstaan.
Bij de verwerking en het gebruik van gegevens worden maatregelen getroffen om de privacy van de leden en andere stakeholders te waarborgen.
Logische toegangsbeveiliging zorgt ervoor, dat ongeautoriseerde personen of processen geen toegang krijgen tot de geautomatiseerde systemen, gegevensbestanden en programmatuur van COBIJT.
Gegevensverstrekking intern en extern gebeurt op basis van 'need to know'. Medewerkers treffen maatregelen om te voorkomen dat informatie in handen van personen terechtkomt, die deze informatie niet strikt nodig hebben. Ook de toegang tot informatiesystemen wordt volgens dit principe adequaat beveiligd.
Datatransport is zodanig met beveiligingsmaatregelen omkleed, dat geen inbreuk kan worden gepleegd op de vertrouwelijkheid en de integriteit van de gegevens en op de informatievoorziening als geheel.
Teneinde computervirusinfecties te voorkomen wordt er slechts gewerkt met geautoriseerde versies van (legale) programmatuur.
Het beheer en de opslag van gegevens zijn zodanig, dat geen informatie verloren kan gaan.
Er is een proces om incidenten adequaat af te handelen en hier lessen uit te trekken.

5. Overzicht technische beveiligingsmaatregelen

☐ Er worden regelmatig back-ups gemaakt, die ook extern bewaard worden
☐ De schijven waarop de back-ups staan, zijn beveiligd tegen ongeautoriseerde toegang (in voorbereiding)
☐ Updates worden zo snel mogelijk geïnstalleerd
☐ Er zijn up to date virusscanners en firewalls
☐ Bezoekers wordt geen toegang gegeven op het eigen Wifi netwerk (in voorbereiding)
☐ Telefoons van de vaste installatie bevatten geen persoonsgegevens
☐ Mobiele telefoons zijn door middel van toegang via vingerafdruk beschermd tegen ongeautoriseerde toegang
☐ Er worden afgezien van deelnemerslijsten geen persoonsgegevens op laptops en USB-sticks opgeslagen.

6. Overzicht organisatorische beveiligingsmaatregelen

☐ Computers gaan na korte tijd automatisch op lock als de gebruiker niet op zijn plek is
☐ Fysieke post blijft niet onbeheerd achter
☐ Wachtwoorden worden niet rond de werkplekken genoteerd
☐ Clean desk policy
☐ Bij de printer blijven nooit vertrouwelijke documenten liggen

☐ Oude documenten worden op de juiste manier vernietigd.