Informatiebeveiligingsbeleid Kempengemeenten, GRSK en KempenPlus 2020;
Bijlage webapplicaties

1. Classificatie van gegevens
Voor een effectieve bescherming van de informatie is vereist dat de waarde van de informatie voor de onderneming bekend is. Classificatie van informatie in termen van vereiste vertrouwelijkheid, integriteit en beschikbaarheid:

- informeert het management en medewerkers over wat moet worden beschermd en hoe informatiemiddelen op een standaard manier kunnen worden beschermd;
- toont de waarde van middelen aan medewerkers, zodat het bewustzijn van beveiliging binnen hun dagelijkse werkzaamheden wordt gestimuleerd;
- stelt de gemeenten in staat te voldoen aan eventuele wettelijke en contractuele verplichtingen.

De eigenaar van de informatie blijft verantwoordelijk voor het up-to-date houden van de identificatie van informatiemiddelen en de toegekende waarde van elk van de geïdentificeerde middelen.

2. Toegangsvoorziening
De gemeenten hebben maatregelen getroffen om ongeoorloofde toegang (zowel fysiek als logisch) tot haar pand en informatieverwerkende faciliteiten te voorkomen. De expliciete maatregelen die getroffen zijn hiervoor, zijn opgenomen en beschreven in relevantie documentatie. Toegang geschiedt bij de gemeenten te allen tijde op basis van ‘need-to-access’. Dit betreft interne systemen en faciliteiten, maar wordt ook toegepast binnen producten die de gemeenten ontwikkelen.

3. Kwetsbaarhedenbeheer
De gemeenten werken vanuit een veilige IT-omgeving en ontwikkelt producten die voldoen aan de hoogste eisen van informatiebeveiliging. Wanneer er kwetsbaarheden worden gedetecteerd, nemen de gemeenten hier via diverse fora, specialisten en koppelingen (RSS-feeds) notie van. Het dichten van deze kwetsbaarheden zal op basis van een risico-analyse in de tijd weggezet worden. De gemeenten laten zowel op de fysieke locatie als op haar producten met regelmaat pentests uitvoeren