## Bijlage 5: Technische en organisatorische beveiliging gegevens kindcentra Kits Primair

Om te voorkomen dat de persoonsgegevens van Kindcentra Kits Primair worden beschadigd, verloren gaan of onrechtmatig worden verwerkt zijn de volgende maatregelen getroffen:

- Toegang tot het systeem wordt verkregen op basis van persoonlijke inlog (gebruikersnaam/wachtwoord).
- Systeembeheerders krijgen alleen toegang middels twee-weg-verificatie.
- Wachtwoorden moeten telkens binnen 90 dagen vervangen worden. Dit wordt aangegeven via het systeem. Indien hier geen gevolg aan wordt gegeven wordt de toegang automatisch geblokkeerd.
- Rechtenstructuur op basis van groepslidmaatschappen.
- Gegevens worden opgeslagen in de Cloud. Deze gegevens bevinden zich in een datacentrum in Groningen met een Back-up in een Datacentrum in Hoogersmilde. Verwerkers die gegevens van Kits Primair beheren tekenen de verwerkersovereenkomst behorend bij het convenant Digitale onderwijsmiddelen en Privacy.
- Bij het verlaten van de werkplek moeten werknemers hun computer vergrendelen (Windows+L).
- Twee maandelijks vindt er een controle plaats of mensen met toegang tot het systeem van Kits Primair nog wel werkzaam zijn binnen de organisatie. Tevens wordt de systeembeheerder automatisch via het systeem op de hoogte gesteld van de uitdiensttreding, zodat deze de vereiste acties kan ondernemen.
- Mailbeveiliging: ESET Mail Security voor Microsoft Exchange Server.
- Periodiek zullen calamiteiten-oefeningen worden georganiseerd ter controle en bewustwording van de privacy gevoeligheid van de organisatie.
- Via het eigen opleidingscentrum zal periodiek aandacht worden geschonken aan het omgaan met privacygevoelige gegevens van Kindcentra Kits Primair.
- Kindcentra Kits Primair heeft geen verplichting tot het aanstellen van een Functionaris Gegevensbescherming (FG).