# GBS-beleid van Proximus


| | |
|---|---|
| Datum | 21/11/2022 |
| Referentie | GBS-beleid |
| Contact | Rik Beckaert |
| E-mail | rik.beckaert@proximus.com |

## Met zijn geïntegreerd beheerssysteem (GBS) garandeert Proximus duurzame en veilige oplossingen van topkwaliteit voor zijn professionele klanten

Voor zijn professionele klanten hanteert Proximus een geïntegreerd beheerssysteem dat voldoet aan de internationale ISO 9001-, ISO 27001- en ISO 14001-normen, net als aan de regelgeving en alle andere contractuele beveiligingsverplichtingen in het bijzonder. Proximus verbindt er zich toe aan alle vereisten te voldoen die het met zijn klanten is overeengekomen.


## Proximus, betrouwbare zakenpartner op het vlak van kwaliteit, veiligheid en milieu

Het ISO 9001-certificaat garandeert de kwaliteit en betrouwbaarheid van onze producten en diensten. Op zijn beurt staat de ISO 27001-norm borg voor de vertrouwelijkheid, integriteit en beschikbaarheid van informatie. Als maatschappelijk verantwoorde onderneming zijn onze groene ambities in lijn met de vereisten van de ISO 14001-norm voor ons datacenter te Machelen.

**Samen vormen deze ISO-normen de leidraad van het geïntegreerd beheerssysteem.** Dit omvat alle onderdelen van de dienstverlening aan onze professionele klanten en combineert de processen, procedures en controles die binnen Proximus worden gebruikt. Op die manier beoogt Proximus dé leverancier te zijn van intuïtieve end-to-endoplossingen, zodat klanten hun werk- en privéleven kunnen organiseren en verrijken.

**Naast de voortdurende verbetering van onze producten en diensten werken we continu aan de beveiliging van informatie.** Om deze informatie te beschermen tegen onbedoelde of opzettelijke ongeoorloofde bekendmaking, wijziging of vernietiging, dienen intern een aantal richtlijnen op het vlak van Security Governance gevolgd te worden. Medewerkers die toegang wensen tot deze bedrijfsinformatie dienen zelf kennis te nemen van de desbetreffende policy's en ze nauwgezet te respecteren. De beveiligingssystemen, van welke aard ook, moeten zo worden geconfigureerd dat ze permanente en toereikende bescherming garanderen, zelfs in geval van dienstonderbrekingen. Hierbij geldt het 'beschermd door standaardinstellingen'-principe.

**Effectieve informatiebeveiliging is essentieel om onze doelstellingen te bereiken**, de wet na te leven en de verwachtingen van onze aandeelhouders en ons imago te handhaven en te verbeteren.

Deze gecoördineerde activiteiten, waarbij de uitvoering van passende controles en de behandeling van onaanvaardbare informatiebeveiligingsrisico's worden gestuurd (algemeen bekend als elementen van Informatiebeveiligingsbeheer), zijn alleen **effectief door de actieve betrokkenheid en inzet van iedereen binnen onze organisatie**, inclusief het toezicht en de steun op alle managementniveaus.

Door de continue toepassing en het beheer van passende controles pakken we met succes een breed scala aan bedreigingen aan, waardoor het succes en de continuïteit van het bedrijf worden gewaarborgd en de **gevolgen van informatiebeveiligingsincidenten tot een minimum worden beperkt.**

**Verder zetten we ons elke dag in om onze milieudoelstellingen te bereiken.** Dat betekent minder CO2-uitstoot, minder energieverbruik en meer duurzame alternatieven.

**Door regelmatige controles en audits verbeteren we dit geïntegreerde beheerssysteem voortdurend.** De feedback van klanten, partners, medewerkers en stakeholders wordt opgevolgd en geanalyseerd om onze doelstellingen te bereiken. Het management van Proximus zorgt ervoor dat dit beleid wordt gedeeld en begrepen, zowel intern als extern.