# Bestuursvoorstel

| | |
|---|---|
| Vergaderdatum | 1 oktober 2025 |
| Afdeling | Control Risk & Audit (CRA) |

## Onderwerp
Strategisch informatiebeveiligings- en privacybeleid

### Voorgesteld besluit
Het Algemeen Bestuur wordt voorgesteld om:

1. Het Strategisch informatiebeveiligings- en privacybeleid vast te stellen.

## Aanleiding
VRBN beschikt over een door het management in 2018 vastgesteld informatiebeveiligingsbeleid.

Dit informatiebeveiligingsbeleid was gebaseerd op de Baseline Informatiebeveiliging Gemeenten (BIG) die per 1 januari 2019 is vervangen door de BIO (Baseline Informatiebeveiliging Overheid). Ook de digitale wereld en omgeving van VRBN is flink veranderd de afgelopen jaren. Een update van het Strategisch informatiebeveiligingsbeleid was daarom noodzakelijk.

Het huidig beleid was enkel gericht op informatiebeveiliging. Gelet op de samenhang tussen informatiebeveiliging en privacy is in het vernieuwde beleid ook privacy opgenomen.

Het management heeft op 3 juli jl. ingestemd met het onderhavige Strategisch informatiebeveiligings- en privacybeleid. Gelet op de vitaalstelling, het toenemende belang van informatiebeveiliging en privacy en draagvlak van het Strategisch informatiebeveiligings- en privacybeleid leggen we dit keer het beleid ter vaststelling aan u voor.

## Doel
Het Strategisch informatiebeveiligings- en privacybeleid van VRBN heeft als doel het waarborgen van de beschikbaarheid, integriteit, vertrouwelijkheid van informatie, informatiemiddelen en bedrijfsprocessen, door middel van preventieve, detectieve, repressieve en correctieve maatregelen. Dit draagt bij aan het minimaliseren van risico's, het voorkomen van reputatieschade, beveiligingsincidenten, datalekken en het waarborgen van de continuïteit van de informatievoorziening die de organisatie levert aan burgers, ketenpartners en de eigen organisatie.

De doelen van het Strategisch informatiebeveiligings- en privacybeleid van VRBN zijn de volgende:

- *Kader:* het beleid biedt een kader om (toekomstige) maatregelen in de informatiebeveiliging en privacy te toetsen aan vastgestelde eisen die door het MTVR zijn gesteld.
- *Normen:* de basis voor de inrichting van het security-management is de ISO 27001 en de Baseline Informatiebeveiliging Overheid (BIO). De basis voor de inrichting van privacy management is de Algemene Verordening Gegevensbescherming (AVG) in combinatie met de Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG).

- *Daadkrachtig:* het beleid dient als basis voor duidelijke keuzes in maatregelen, actieve controle op beleidsregels en de uitvoering daarvan.
- *Helderheid:* het beleid biedt duidelijkheid, is ondubbelzinnig en is voor iedereen binnen VRBN te begrijpen en toe te passen.

Daarnaast wordt tevens voldaan aan wet- en regelgeving omtrent informatiebeveiliging en privacy (BIO, ISO 27001 en AVG).

## Argumenten

1.1. ***Compliance met wetgeving**: De AVG, BIO, ISO 27001 en andere relevante wet- en regelgeving vereisen een robuust kader rondom informatiebeveiliging en privacy.*

1.2. ***Doelen, kaders en uitgangspunten:** Het document zorgt voor heldere doelen, kaders en uitgangspunten op gebied van informatiebeveiliging en privacy.*

## Kanttekeningen en risico's

**Risico's:**

**Compliance zonder effectiviteit**: Wanneer het beleid puur als een formaliteit wordt opgevolgd zonder aandacht voor daadwerkelijke effectiviteit, kan het een schijnveiligheid creëren. In plaats van werkelijke bescherming biedt het slechts kaders en uitgangspunten. Uitvoering geven aan het beleid en het daadwerkelijk inrichten van maatregelen en de controle hierop is essentieel.

**Onvoldoende medewerkersbetrokkenheid**: Wanneer medewerkers niet goed worden meegenomen in het onderwerp informatiebeveiliging en privacy kan het belang hiervan worden onderschat. Dit kan leiden tot niet gedragen maatregelen of onbewust onjuist gedrag van medewerkers wat leidt tot verhoogde risico's voor de organisatie welke kunnen leiden tot incidenten.

## Communicatie

Het Strategisch informatiebeveiligings- en privacybeleid wordt gepubliceerd op de corporate website van VRBN.

## Evaluatie

Het beleid geldt voor een periode van vier jaar. Jaarlijks wordt door de CISO en FG gecontroleerd of er grote of significante wijzigingen hebben plaatsgevonden waardoor het beleid eerder moet worden gewijzigd en opnieuw moet worden vastgesteld dan de termijn van vier jaar.

## Bijlagen

1. Strategisch informatiebeveiligings- en privacybeleid