



Grip op informatieveilig gedrag

Hulpmiddel 1: Vijf succesfactoren voor het bestuurlijke gesprek

Het goede bestuurlijke gesprek over informatieveiligheid: Vijf succesfactoren



1: Maak het overleg integraal



Betrek diverse collega's bij het gesprek met jullie directeur/(praktijk)eigenaar, dus bijvoorbeeld ook mensen die met innovatie en kwaliteit bezig zijn. Een diverse samenstelling voorkomt een eenzijdige focus.



Koppel informatieveiligheid aan jullie bredere veiligheidscultuur. Link het dus bijvoorbeeld aan veiligheid van zorg of zelfs brandveiligheid. Dit voorkomt versnippering en vergroot de efficiëntie en effectiviteit van interventies.

2: Regelmaat en directe, korte lijnen



Organiseer elke 4 tot 8 weken een voortgangsoverleg voor continuïteit en opvolging. Wanneer er ook overleg is zonder de directeur/(praktijk)eigenaar, kan de frequentie met hem/haar naar eens per kwartaal.



Werk met een herkenbare voortgangsrapportage en vaste gespreksonderwerpen voor overzicht en focus.



Zoek elkaar tussentijds op bij incidenten of urgente dilemma's. Investeer dus in directe korte lijnen met de directeur/(praktijk)eigenaar.

3: Expliciet aandacht voor gedrag



Sta bewust stil bij gedrag om te voorkomen dat informatieveiligheid enkel een technische of papieren werkelijkheid is.



Sta stil bij wat gedrag verklaart. Het onderscheid tussen 'willen', 'kunnen' en 'gelegenheid' helpt hierbij. Pas als je een verklaring voor gedrag hebt, kun je passende interventies bedenken.



Maak in de voortgangsrapportage onderscheid tussen mens (gedrag), proces en techniek. Werk met verschillende vormen van sturingsinformatie.



Hulpmiddel: Bestuurlijke dialoogkaarten



Hulpmiddel: Bestuurlijke voortgangsrapportage



4: Agendeer kansen en dialoog



Maak bewust ruimte voor dialoog over visie, strategie en rolverdeling. Dit helpt om buiten de hectiek van alledag te werken aan een gezamenlijk kompas voor de besturing op informatieveiligheid.



Kijk bewust ook naar kansen voor een win-win op veiligheid en vernieuwing. Eenzijdige sturing op het voorkomen van incidenten en minimaliseren van informatieveiligheidsrisico's remt innovatie.

5: Intelligent omgaan met risico's



Weeg informatieveiligheid als waarde in relatie tot andere waarden zoals efficiëntie, werkgelek en kwaliteit van zorg.



Maak risico's concreet met scenario's en praktijkvoorbeelden. Dit maakt besluiten beter uitlegbaar en het gesprek concreter en relevanter.



Prioriteer risico's samen en bespreek welke risico's acceptabel zijn. Leg bewuste risico's of uitzonderingen op beleid vast.

Het goede bestuurlijke gesprek over informatieveiligheid: Vijf succesfactoren



1: Maak het overleg integraal



Betrek diverse 'chefs' (CISO, CIO, CMIO, CHIO, directeur bedrijfsvoering) en het hoofd kwaliteit bij het bestuurlijk voortgangsoverleg. Maak eventueel een onderscheid tussen een directieoverleg en een bestuurlijk overleg. Dit voorkomt een te eenzijdige focus op informatieveiligheid.



Maak informatieveiligheid onderdeel van de besturing van de bredere veiligheidscultuur in de organisatie. Dit voorkomt versnippering en vergroot de efficiëntie en effectiviteit van interventies.

2: Regelmaat en directe, korte lijnen



Organiseer elke 4 tot 8 weken een bestuurlijk voortgangsoverleg voor continuïteit en opvolging. Wanneer er apart overleg is met de directie kan de frequentie met bestuurder naar eens per kwartaal.



Werk met een herkenbare voortgangsrapportage en vaste gespreksonderwerpen voor overzicht en focus.



Zoek elkaar tussendoor op bij incidenten of urgente dilemma's. Investeer dus in directe korte lijnen met de bestuurder en een werkplek dicht bij de bestuurskamer.

3: Expliciet aandacht voor gedrag



Sta bewust stil bij gedrag om te voorkomen dat informatieveiligheid enkel een technische of papieren werkelijkheid is.



Sta stil bij wat gedrag verklaart. Het onderscheid tussen 'willen', 'kunnen' en 'gelegenheid' helpt hierbij. Pas als je een verklaring voor gedrag hebt, kun je passende interventies bedenken.



Maak in de voortgangsrapportage onderscheid tussen mens (gedrag), proces en techniek. Werk met verschillende vormen van sturingsinformatie.



Hulpmiddel: Bestuurlijke dialoogkaarten



Hulpmiddel: Bestuurlijke voortgangsrapportage



4: Agendeer kansen en dialoog



Maak bewust ruimte voor dialoog over visie, strategie en rolverdeling. Dit helpt om buiten de hectiek van alledag te werken aan een gezamenlijk kompas voor de besturing op informatieveiligheid.



Kijk bewust ook naar kansen voor een win-win op veiligheid en vernieuwing. Eenzijdige sturing op het voorkomen van incidenten en minimaliseren van informatieveiligheidsrisico's remt innovatie.

5: Intelligent omgaan met risico's



Weeg informatieveiligheid als waarde in relatie tot andere waarden zoals efficiëntie, werkgeuk en kwaliteit van zorg.



Maak risico's concreet met scenario's en praktijkvoorbeelden. Dit maakt besluiten beter uitlegbaar en het gesprek concreter en relevanter.



Prioriteer risico's samen en bespreek welke risico's acceptabel zijn. Leg bewuste risico's of uitzonderingen op beleid vast.