Informatiebeveiligingsbeleid Scholengroep Holland

1. Verantwoordelijkheid

Het Bestuur van Scholengroep Holland is eindverantwoordelijk.
De schooldirecteur is verantwoordelijk voor het gebruik van de systemen en de beveiliging daarvan.
Administratiekantoor Groenendijk is de verwerker van gegevens waaronder o.a. persoonsgegevens.
Alle medewerkers binnen de Scholengroep Holland, in welke functie dan ook, conformeren zich aan de beleidsuitgangspunten, procedures, werkwijze en de daarbij gehanteerde informatiesystemen.

2. Toepassingsgebied

Dit beleid is van toepassing op alle gegevens die gecreëerd, ontvangen, verzonden of bewaard worden binnen de Scholengroep Holland en de daarmee samenhangende contractuele verplichtingen. Het beleid en de uitwerking hiervan gelden voor alle medewerkers binnen de Scholengroep Holland. Afwijkingen hierop moeten gemeld worden, zodat er continu verbeterd kan worden. Dit beleid geldt ook voor leveranciers en contractanten. Met hen zijn verwerkersovereenkomsten afgesloten dan wel zijn er SAAS-verklaringen afgegeven.

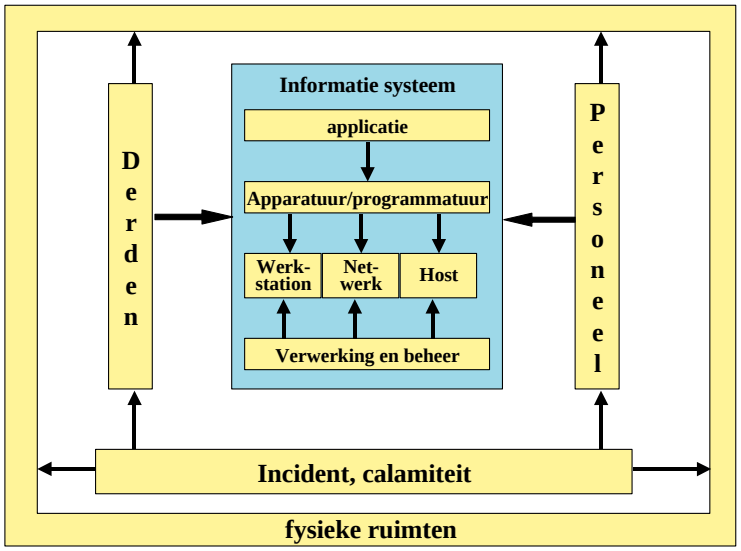
2.1 Houderschap en reikwijdte van het beleid

Het Bestuur van Scholengroep Holland is verantwoordelijk voor het stellen van voorwaarden aan de leverancier die haar dienst beschikbaar stelt met voldoende beveiligingsopties, conform de informatiebeveiligingsnormen en andere wet- en regelgeving. Ook voldoet de hosting en het beheer van de software aan deze eisen.
De leidinggevenden binnen Scholengroep Holland zijn verantwoordelijk voor het creëren van bewustwording bij het personeel met betrekking tot informatiebeveiliging (IB) en het bewaken van privacy gevoelige informatie die zij onder zich hebben.
Het bestuur van Scholengroep Holland is verantwoordelijk voor het inhuren van het betreffende systeem, inclusief:

- het bepalen van bij het systeem te onderkennen risico's,
- het classificeren van het systeem en de daarbij behorende gegevens,
- het (laten) ontwikkelen van adequate beveiligingsmiddelen en interne controlemaatregelen.
- Het ontwikkelen van tools om de bewustwording bij medewerkers te vergroten.

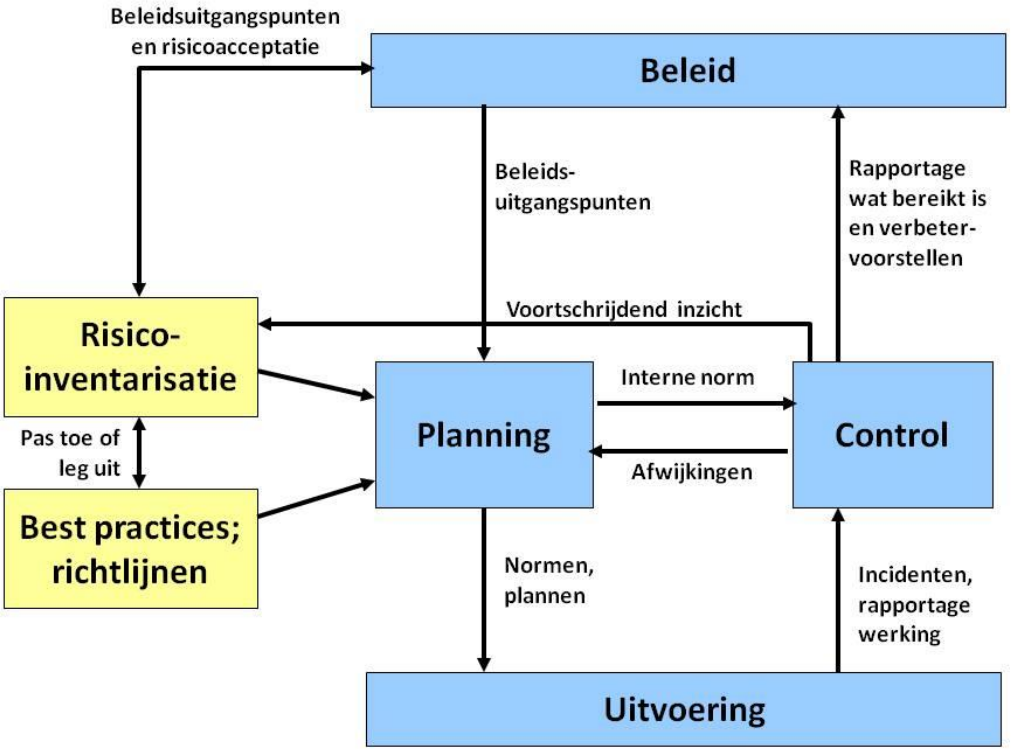
Om incidenten en calamiteiten te voorkomen of af te handelen wordt gestuurd op de juiste inzet van de infrastructurele componenten (werkstations, servers en het interne en externe netwerk), de juiste verwerking, het adequate beheer, het goed functioneren van het personeel, het maken van afspraken met derden, fysieke beveiliging en voorzieningen.

In onderstaand figuur zijn alle genoemde deelgebieden van een informatiesysteem opgenomen. Hierbij wordt niet een maximaal beveiligingsniveau nagestreefd, maar een optimaal niveau.



2.2 Controle werking en naleving van het beleid

Halfjaarlijks wordt de werking en de naleving van het beleid intern geëvalueerd met de leverancier en hierover wordt gerapporteerd aan het bestuur. Onderdeel van deze evaluatie zijn het opnieuw beoordelen van risico's en een impact analyse van nieuwe wet- en regelgeving. Onderdeel van deze rapportage is een plan met verbetervoorstellen. De directie beoordeelt de rapportage, keurt voorstellen al dan niet goed en kent budget toe voor de realisatie van de voorstellen. Onderstaand is dit schematisch weergegeven.



3. Beleidsuitgangspunten

In deze beleidsuitgangspunten is vastgelegd op welke wijze de informatiebeveiliging vorm gegeven wordt zodat deze past bij de Scholengroep Holland. Bij de verdere invulling van dit beleid dienen de volgende uitgangspunten gehanteerd te worden:

1. Informatiebeveiliging is een belangrijk bedrijfsrisico voor Scholengroep Holland. Het Bestuur stelt daarom het beleid vast, beoordeelt de risico's, stelt de maatregelen vast en laat periodiek de werking van het beleid en de naleving van deze maatregelen beoordelen om te borgen, dat het IBsysteem blijvend adequaat werkt en waar nodig verbeterd wordt.
2. Scholengroep Holland conformeert zich m.b.t. de informatiebeveiliging aan de van toepassing zijnde wetgeving.
3. De Algemene Verordening Gegevensverwerking vormt, voor zover zij bijdragen aan informatiebeveiliging, het uitgangspunt voor de te definiëren maatregelen. Dit is vooral een bedrijfseconomische afweging.
4. Scholengroep Holland beschouwt computercriminaliteit als een ongewenst maatschappelijk probleem. Zij ziet het slechts als haar taak passende maatregelen te nemen teneinde schade, ten gevolge van criminele activiteiten, zoveel mogelijk te beperken.
5. Vertrouwen is voor Scholengroep Holland een groot goed en zij hanteert naar medewerkers, klanten, leveranciers en andere stakeholders het wederkerigheidsprincipe. Scholengroep Holland gaat er vanuit, dat zij afspraken nakomen m.b.t. integriteit, vertrouwelijkheid en continuïteit van de informatievoorziening.
6. Het personeelsbeleid is mede gericht op het verbeteren van inzicht in de integriteit, vertrouwelijkheid en continuïteit van de informatievoorziening bij medewerkers. Tijdens een jaarlijkse evaluatie wordt dit aan de orde gesteld.
7. De fysieke en logistieke beveiliging van de gebouwen en de ruimtes daarin zijn zodanig, dat de vertrouwelijkheid, integriteit en beschikbaarheid van de gegevens en gegevensverwerking gewaarborgd zijn.
8. Aanschaf, installatie en onderhoud van informatie- en communicatiesystemen, alsmede inpassing van nieuwe technologieën, worden zo nodig met aanvullende maatregelen uitgevoerd, dat hiermee geen afbreuk wordt gedaan aan de informatiebeveiliging.
9. Opdrachten aan derden voor het uitvoeren van werkzaamheden worden zodanig omgeven met maatregelen, dat er geen inbreuk op de vertrouwelijkheid, integriteit en continuïteit van de informatievoorziening kan ontstaan.
10. Bij de verwerking en het gebruik van gegevens worden maatregelen getroffen om de privacy van ouders, leerlingen, medewerkers en andere betrokkenen te waarborgen.
11. Toegangsbeveiliging zorgt ervoor, dat ongeautoriseerde personen of processen geen toegang krijgen tot de informatiesystemen, gegevensbestanden en programmatuur.
12. Gegevensverstrekking extern gebeurt op basis van 'need to know'. Intern is dit niet altijd wenselijk omdat kennisdeling essentieel is voor een kosteneffectieve dienstverlening aan ouders en leerlingen.
13. Scholengroep Holland en haar medewerkers treffen maatregelen om te voorkomen dat vertrouwelijke informatie in handen van derden terechtkomt.
14. Input van ouders en of leerlingen die vertrouwelijke gegevens bevat, wordt na verwerking gearchiveerd of vernietigd conform het bewaarbeleid.
15. Gegevenstransport is zodanig met beveiligingsmaatregelen omkleed, dat geen inbreuk kan worden gepleegd op de vertrouwelijkheid en de integriteit van deze gegevens.
16. Geautoriseerde medewerkers hebben ook op afstand een beveiligde toegang tot de voor hun relevante productie omgevingen. Er worden geen vertrouwelijke gegevens buiten de productieomgeving opgeslagen. Onder condities kan hiervan afgeweken worden.

17. Productie omgevingen zijn gescheiden van andere omgevingen en hierin kunnen specifiek toegangsrechten worden verleend en is monitoring van de toegang mogelijk.
18. Het beheer en de opslag van gegevens in productie omgevingen zijn zodanig, dat geen informatie verloren kan gaan tenzij er sprake is van overmacht.
19. Er zijn functiescheidingen aangebracht tussen de beheer- en gebruikersorganisatie. Voorts wordt functiescheiding toegepast waar dat mogelijk en wenselijk is.
20. Er is een proces om incidenten adequaat af te handelen en hier 'lessons learned' uit te trekken.
21. Er zijn bij de leverancier calamiteitenplannen en –voorzieningen om de continuïteit van de informatievoorziening te waarborgen.
22. Bij uitbesteding van gegevensverwerking kan de directie besluiten om tijdelijk af te wijken van deze beleidsuitgangspunten en de risico's hiervan tijdelijk te accepteren.
23. Genoemde beleidsuitgangspunten gelden voor die gegevensbewerkingen, waarvoor Scholengroep Holland wettelijk en/of contractueel verantwoordelijk is.