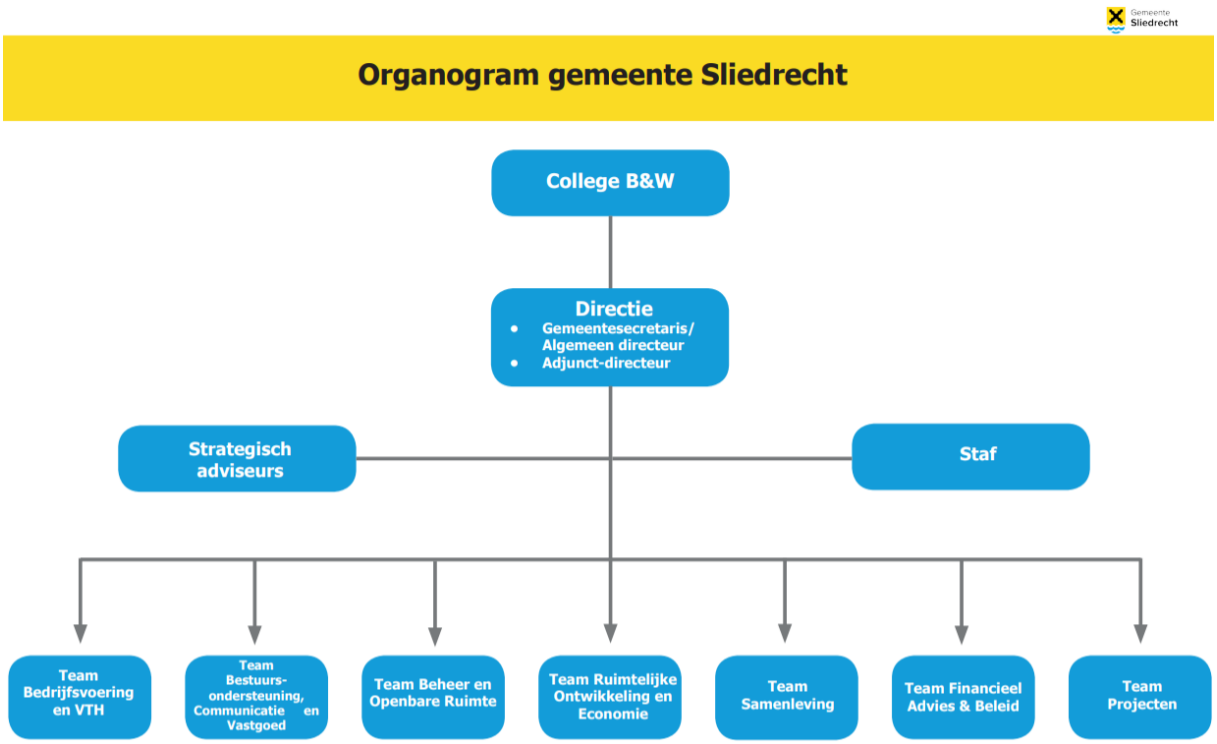
Bijlage: Addendum Sliedrecht

In dit addendum is voor de gemeente Sliedrecht aangegeven op welke wijze er op het regionale informatiebeveiligingsbeleid wordt afgeweken of wordt aangevuld. Bij wijzigingen in de organisatiestructuur die invloed hebben op de uitvoering van het informatiebeveiligingsbeleid kan een herziene versie van het addendum worden vastgesteld door het College.

Afwijkingen

Binnen Sliedrecht heeft ieder team een manager. Waar in het informatiebeveiligingsbeleid wordt gesproken over lijnmanagement, spreken wij binnen Sliedrecht over teammanagers.



Aanvullingen

<u>Strategische doelstellingen</u>

Ieder jaar wordt een regionaal informatiebeveiligingsplan opgesteld. Binnen Sliedrecht is het belangrijk ook te monitoren op de lokale ontwikkelingen. Vandaar dat Sliedrecht aanvullend op het regionale beveiligingsplan ook een lokaal plan heeft. Dit plan wordt ieder jaar geëvalueerd. Wanneer nodig, stelt de beveiligingsadviseur met ondersteuning of advies van de CISO wijzigingen aan het lokale informatiebeveiligingsplan op. Als deze wijzigingen financiële gevolgen hebben, dient het College van Burgemeester en Wethouders het herziene plan vast te stellen. Als deze wijzigingen geen financiële gevolgen hebben, stelt de directie het herziene plan vast.

<u>Uitgangspunten</u>

Binnen Sliedrecht is informatieveiligheid niet de verantwoordelijkheid van een individu.

- Het management bepaalt, op basis van de uitgangspunten van dit beleid, de prioriteiten voor de organisatie op het gebied van informatieveiligheid.
- Iedereen binnen de organisatie is bekend met de verantwoordelijkheden die bij zijn of haar rol horen.

Rollen en verantwoordelijkheden

Vanuit strategisch en tactisch oogpunt zijn er voor Sliedrecht verschillende rollen belegd met bijbehorende verantwoordelijkheden. Zij zorgen ervoor dat het veilig omgaan met informatie door de gehele organisatie heen wordt nagestreefd en dat verantwoordelijkheden bij de juiste personen binnen de organisatie belegd zijn. In dit addendum worden verantwoordelijkheden benoemd die aanvullend zijn op de verantwoordelijkheden die in het informatiebeveiligingsbeleid staan beschreven.

De regionale Chief Information Security Officers zijn verantwoordelijk voor het adviseren op en controleren van de toepassing van informatiebeveiliging binnen de gemeente. De gemeente heeft de coördinatie van lokale taken voor informatieveiligheid binnen Sliedrecht bij een adviseur belegd. De adviseur voor informatieveiligheid wordt in staat gesteld onafhankelijk advies te geven aan het management, de directie en het College. De Chief Information Security Officers gebruiken deze adviseur als aanspreekpunt voor het communiceren over regionale initiatieven met lokale impact. Verder bieden zij de lokale adviseur ondersteuning en advies bij lokale initiatieven.

De directie is verantwoordelijk voor het vaststellen van het gewenste niveau van continuïteit en vertrouwelijkheid. De directie draagt zorg voor het uitwerken van tactische informatiebeveiligingsbeleidsonderwerpen en laat zich hierin bijstaan door de CISO van de gemeente.

De directie zorgt dat alle processen en systemen en de daarbij behorende middelen altijd onder de verantwoordelijkheid van een teammanager vallen. De directie zorgt dat de teammanagers zich, wanneer hierom wordt gevraagd, verantwoorden over de beveiliging van de informatie die onder hen valt. De directie zorgt dat de eindverantwoordelijke portefeuillehouders binnen het college gevraagd en ongevraagd geïnformeerd worden over de mate waarin informatiebeveiliging een onderdeel is van het handelen van de bedrijfsvoering. Op die manier kan het college zich ook verantwoorden naar de raad.

Teammanager zorgen ervoor dat voor informatiesystemen en applicaties die enkel binnen de gemeente Sliedrecht in gebruik zijn, functioneel beheerders zijn aangesteld. Zij zijn verantwoordelijk voor het treffen van de juiste maatregelen rondom de autorisaties van het systeem of de applicatie. Dit doen zij vanaf de beginfase: bij het aanschaffen van een nieuw systeem of applicatie dient rekening te worden gehouden met aspecten van informatiebeveiliging. Bij geconstateerde gebreken aan informatiesystemen of applicaties zijn de functioneel beheerders verantwoordelijk voor het zoeken naar de oorzaak en mogelijke oplossingen. Wanneer dit niet binnen het kenniskader van de beheerder ligt, zijn zij verantwoordelijk voor het ondersteunen van of adviseren in een regionaal of extern onderzoek.

Iedere medewerker draagt verantwoordelijkheid voor het toepassen van opgestelde beveiligingsmaatregelen. Wanneer een medewerker constateert onvoldoende kennis te hebben over het implementeren van maatregelen of uitvoeren van acties binnen processen, is de teammanager het aanspreekpunt. Bij het zien van onvolledigheden, gebreken of incidenten op het gebied van informatieveiligheid zijn medewerkers geïnstrueerd een melding te doen.