Beleid Informatiebeveiliging
Coöperatie ParkeerService

Naam document	Beleid Informatiebeveiliging CPS
Classificatie	Openbaar
Eigenaar	Femke Santema
Versienummer	1.3
Datum wijziging	28 augustus 2023

Inhoud

1 Beleid Informatiebeveiliging

1.1 Inleiding

Coöperatie ParkeerService ziet de bescherming van informatievoorziening als een essentieel onderdeel van haar bedrijfsvoering. Publiekrechtelijke informatie en privacygevoelige gegevens worden dagelijks gecreëerd, gedeeld of verwerkt. De leden van de coöperatie werken volgens een gemeenschappelijk normenkader Baseline Informatiebeveiliging Overheid (BIO), wat aangeeft dat er een groot belang is bij het borgen van beveiliging van de informatie die in opdracht van de leden wordt verwerkt.

Informatie is één van de voornaamste bedrijfsmiddelen van Coöperatie ParkeerService. Het verlies van gegevens, uitval van ICT, of het door onbevoegden kennisnemen of manipuleren van bepaalde informatie kan ernstige gevolgen hebben voor de bedrijfsvoering maar ook leiden tot imagoschade. Ernstige incidenten hebben mogelijk negatieve gevolgen voor burgers, bedrijven, partners en de eigen organisatie met waarschijnlijk ook politieke consequenties. Informatieveiligheid is daarom van groot belang. Informatiebeveiliging (IB) is het proces dat dit belang dient. Coöperatie ParkeerService wil structureel aantoonbaar een samenhangend pakket aan maatregelen treffen en onderhouden.

2 Verantwoordelijkheid, doelstelling en doelgroep

Gelet op de mogelijke impact van verstoringen op de bedrijfsvoering en continuïteit van coöperatie ParkeerService en haar klanten, berust eindverantwoordelijkheid voor het beleid voor informatiebeveiliging bij de directie.

Het Beleid Informatiebeveiliging (hierna te noemen beleid IB) heeft als doel de risico's m.b.t. de volgende drie onderdelen van de informatievoorziening binnen Coöperatie ParkeerService te beheersen.

- Beschikbaarheid: zekerstellen dat informatie op de juiste momenten aanwezig is.
- Integriteit: waarborgen dat informatie correct en volledig is.
- Vertrouwelijkheid: beschermen van gevoelige informatie tegen onbevoegde kennisname.

Bij Coöperatie ParkeerService definiëren we dit als volgt:

> 'Een raamwerk van beleidsuitgangspunten met betrekking tot de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de informatievoorziening, waarbinnen een evenwichtig (doeltreffend en doelmatig) stelsel van onderling samenhangende maatregelen ontwikkeld wordt, om de informatievoorziening te beschermen tegen interne en externe bedreigingen'.

Bovenstaande is als zodanig ook vastgelegd in de missie en visie van het Informatiebeveiligings- en Privacybeleid ParkeerService (20181018 ParkeerService IPB v1.0.docx). Het IPB beleid is onlosmakelijk verbonden als onderdeel van het ISMS voor ISO 27001.

Alle betrokkenen moeten zorgen, dat aan de in dit beleid IB geformuleerde beleidsuitgangspunten wordt voldaan bij de inrichting van de organisatie, procedures, werkwijze en de daarbij gehanteerde informatiesystemen.

3 Toepassingsgebied

Dit beleid is van toepassing op alle informatie die gecreëerd, ontvangen, verzonden of bewaard wordt in de dienstverlening van Coöperatie ParkeerService aan klanten en de daarmee samenhangende contractuele verplichtingen en ondersteunende processen. Het beleid en de uitwerking hiervan gelden voor alle medewerkers van Coöperatie ParkeerService. Afwijkingen hierop moeten gemeld worden, zodat het managementsysteem continu verbeterd wordt. Daarnaast geldt het beleid ook voor contractanten, die Coöperatie ParkeerService ondersteunen bij haar dienstverlening aan klanten.

Onlosmakelijk onderdeel van dit beleid zijn de '**Protocollen' (**Protocollen Coöperatie ParkeerService, zoals gepubliceerd op Afas Insite), waaraan ook alle medewerkers, contractanten en stagiaires zich moeten houden. Dit bevat ook de ethische code. Er wordt zoveel mogelijk gestreefd naar beveiligingsmaatregelen die gebaseerd zijn op logische principes, omdat deze kosteneffectief en duurzaam zijn. Deze principes zijn:

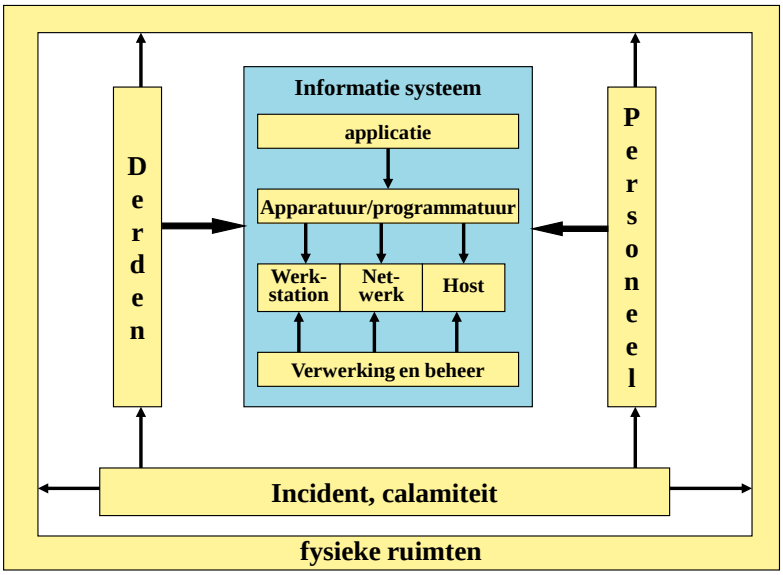
1. Vertrouwelijke gegevens die je niet hebt, hoef je ook niet te beveiligen;
2. Niet slepen met vertrouwelijke gegevens;
3. Scheiden van gegevens.
4. Security by design: vanaf het ontwerpproces wordt rekening gehouden met informatiebeveiliging.

Alle medewerkers worden geacht deze principes in de praktijk te brengen.

3.1 Houderschap en reikwijdte van het beleid

Coöperatie ParkeerService is dus verantwoordelijk voor het beschikbaar stellen van haar dienst met voldoende beveiligingsopties, zodat haar klanten kunnen voldoen aan de voor haar geldende IB-normen en andere wet- en regelgeving. Ook voldoet de hosting en het beheer van de software aan deze eisen. Dit ontslaat echter de klant niet van de eindverantwoordelijkheid voor de beveiliging van haar informatievoorziening.

Van elk informatiesysteem, inclusief de daarbij behorende gegevens, moet expliciet één houder zijn benoemd. Het houderschap impliceert de eindverantwoordelijkheid voor het betreffende systeem, inclusief het bepalen van de bij het systeem te onderkennen risico's, het classificeren van het systeem en de daarbij behorende gegevens en het (laten) ontwikkelen van adequate beveiligingsmiddelen en interne controlemaatregelen. Naast de applicatie betreft dit ook 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 om incidenten en calamiteiten te voorkomen of af te handelen. In onderstaande figuur zijn alle genoemde deelgebieden van een informatiesysteem opgenomen.



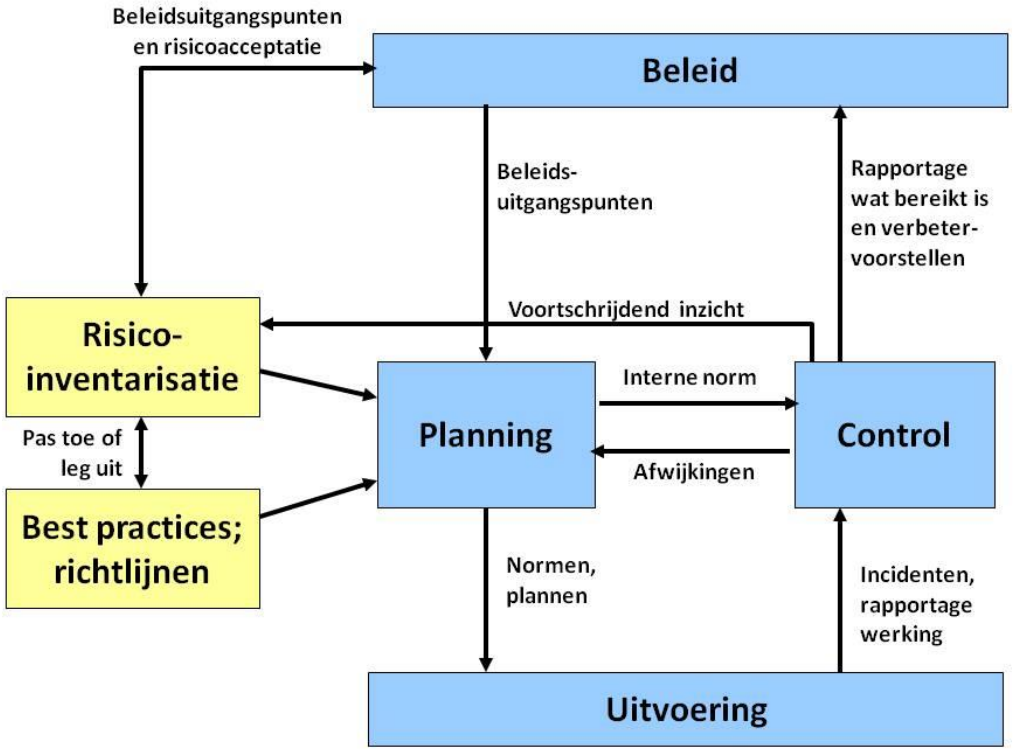
3.2 Uitwerking van dit beleid

Op basis van dit beleid worden risicoanalyses uitgevoerd en wordt een set van maatregelen gedefinieerd als interne norm, die geldt als minimumniveau van beveiliging voor de dienstverlening aan klanten. In overleg kan een hoger niveau met een klant worden afgesproken.

3.3 Controle werking en naleving van het beleid

In de management review wordt de werking en de naleving van het beleid intern geëvalueerd en zo nodig aangepast.

Jaarlijks wordt een interne audit gehouden. Onderdeel van deze interne audit zijn het opnieuw beoordelen van risico's en een beoordeling van nieuwe contracten en wet- en regelgeving. Onderdeel van deze rapportage is ook 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.



Daarnaast wordt jaarlijks een externe audit uitgevoerd op de werking van het IB-managementsysteem door een onafhankelijke derde partij, die hiertoe bevoegd en deskundig is. De rapportage hiervan is beschikbaar voor (potentiële) klanten.

4 Beleidsuitgangspunten

Met onderstaande kwalitatieve beleidsuitgangspunten verwacht coöperatie ParkeerService haar informatiebeveiligingsrisico's te beheersen en tegelijk haar flexibiliteit en efficiency bij het uitvoeren van haar werkzaamheden te behouden.

De beleidsuitgangspunten bieden bovendien het kader voor de directie, op welke wijze zij wil dat de informatiebeveiligingsdoelstellingen worden vormgegeven, die passend zijn voor coöperatie ParkeerService.

Genoemde beleidsuitgangspunten gelden voor die gegevensbewerkingen, waarvoor coöperatie ParkeerService wettelijk en/of contractueel verantwoordelijk is.

Bij de verdere invulling van dit beleid gelden de volgende uitgangspunten:

1. Informatiebeveiliging is een belangrijk bedrijfsrisico voor coöperatie ParkeerService. De directie stelt daarom het beleid vast, beoordeelt de risico's, stelt de maatregelen vast, stelt voldoende middelen ter beschikking en laat periodiek de werking van het beleid en de naleving van deze maatregelen intern en extern beoordelen om te borgen dat het IB-managementsysteem blijvend adequaat werkt en waar nodig verbeterd wordt.
2. Coöperatie ParkeerService conformeert zich m.b.t. de informatiebeveiliging aan de relevante wetgeving en de contractuele afspraken met klanten en business partners.

3. Coöperatie ParkeerService streeft ernaar om haar dienstverlening aan klanten continu te verbeteren.
4. De beheersdoelstellingen en beheersmaatregelen van de norm NEN-ISO/IEC 27001 en de privacyrichtlijnen van de Autoriteit Persoonsgegevens (AP) vormen, voor zover zij bijdragen aan de informatiebeveiliging van coöperatie ParkeerService en handhaafbaar zijn, het uitgangspunt voor de te definiëren maatregelen. Dit is vooral een bedrijfseconomische afweging.
5. Coöperatie ParkeerService beschouwt computercriminaliteit als een ongewenst maatschappelijk probleem en ziet het slechts als haar taak om passende maatregelen te nemen om schade ten gevolge van criminele activiteiten zoveel mogelijk te beperken.
6. Vertrouwen is voor Coöperatie ParkeerService een groot goed en zij hanteert naar medewerkers, klanten, leveranciers en andere stakeholders het wederkerigheidsprincipe. Coöperatie ParkeerService gaat ervan uit, dat zij afspraken nakomen m.b.t. beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening.
7. Het HRM-beleid is mede gericht op het verbeteren van de beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening bij medewerkers. Tijdens een jaarlijkse evaluatie wordt dit aan de orde gesteld.
8. De fysieke en logistieke beveiliging van de gebouwen en de ruimtes daarin zijn zodanig, dat de beschikbaarheid, integriteit en vertrouwelijkheid van de gegevens en gegevensverwerking inclusief de bedrijfsmiddelen gewaarborgd zijn.
9. Ontwikkeling of aanschaf, installatie en onderhoud van informatie- en communicatiesystemen, alsmede inpassing van nieuwe technologieën, moeten zo nodig met aanvullende maatregelen worden uitgevoerd, dat hiermee geen afbreuk wordt gedaan aan de informatiebeveiliging.
10. Opdrachten aan derden voor het uitvoeren van werkzaamheden worden zodanig omgeven met maatregelen, dat er geen inbreuk op de beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening kan ontstaan.
11. Bij de verwerking en het gebruik van gegevens worden maatregelen getroffen om de privacy van klanten, medewerkers en andere betrokkenen te waarborgen.
12. Toegangsbeveiliging zorgt ervoor, dat ongeautoriseerde personen of processen geen toegang krijgen tot de informatiesystemen, gegevensbestanden en programmatuur van coöperatie ParkeerService.
13. Gegevensverstrekking extern gebeurt op basis van 'need to know'. Intern is dit niet altijd wenselijk omdat kennisdeling essentieel is voor een kosteneffectieve dienstverlening aan klanten.
14. Coöperatie ParkeerService en haar medewerkers treffen maatregelen om te voorkomen dat vertrouwelijke informatie in handen van derden terechtkomt.
15. Input van klanten die vertrouwelijke data bevat, wordt na verwerking binnen de wettelijke termijnen gearchiveerd of vernietigd.
16. Datatransport is zodanig met beveiligingsmaatregelen omkleed, dat geen inbreuk kan worden gepleegd op de vertrouwelijkheid en de integriteit van deze gegevens.
17. Geautoriseerde medewerkers moeten ook op afstand een beveiligde toegang hebben tot de voor hun relevante productie omgevingen. Er worden geen vertrouwelijke gegevens buiten de productieomgeving opgeslagen. Onder condities kan hiervan afgeweken worden.
18. Productie omgevingen zijn gescheiden van andere omgevingen en hierin kunnen specifiek toegangsrechten worden verleend en is monitoring van de toegang mogelijk.

19. Het beheer en de opslag van gegevens in productieomgevingen zijn zodanig, dat geen informatie verloren kan gaan tenzij er sprake is van overmacht.
20. Er zijn functiescheidingen aangebracht tussen de ontwikkel-, beheer- en gebruikersorganisatie. Verder wordt functiescheiding toegepast waar dat mogelijk en wenselijk is.
21. Er is een proces om incidenten adequaat af te handelen en hier 'lessons learned' uit te trekken.
22. Er zijn calamiteitenplannen en -voorzieningen om de beschikbaarheid van de informatievoorziening te waarborgen.
23. Bij uitbesteding van gegevensverwerking kan de directie besluiten om tijdelijk af te wijken van deze beleidsuitgangspunten en de risico's hiervan tijdelijk te accepteren.
24. Bij conflicten prevaleert de missie van coöperatie ParkeerService boven de eisen die gesteld worden door IB en of privacy.
25. Informatiebeveiliging is onderdeel van het ontwerpen, ontwikkelen en beheren van software, ook als die door derden wordt ontwikkeld. Security by design en privacy by design en default vormen hierbij de voornaamste uitgangspunten.
26. Coöperatie ParkeerService en haar medewerkers realiseren zich de privacy gevoeligheid van de (bijzondere) persoonsgegevens die zij verwerken en waarborgen te allen tijde de afscherming, corrigeerbaarheid en transparantie van deze gegevens ter bescherming van de persoonlijke levenssfeer van de betrokkenen.
27. Het gebruik van verwijderbare media zoals USB-sticks en externe harde schijven zijn niet toegestaan, tenzij dit expliciet (schriftelijk) is vastgelegd met toestemming van de leidinggevende.