Gesloten openheid
Beleid informatiebeveiliging gemeente Leeuwarden 2014-2015

VOORWOORD

In januari 2003 is het eerste informatiebeveiligingsbeleid vastgesteld voor de gemeente Leeuwarden in de nota "Gesloten Openheid". In deze nota werd het beleid ten aanzien van informatiebeveiliging geformuleerd. Het informatiebeveiligingsbeleid biedt richting en ondersteuning aan het management ten behoeve van Informatiebeveiliging.

Het beveiligingsbeleid is gebaseerd op de Code voor Informatiebeveiliging [1], die als internationale standaard voor informatiebeveiliging wordt gezien. Politieke, maatschappelijke, technologische en operationele ontwikkelingen zijn van invloed op het Beveiligingsbeleid. Periodieke evaluatie en aanpassing van het beleid is daarom noodzakelijk. In het beleid is bepaald dat deze actualisatie in een vierjaarlijkse cyclus wordt vastgesteld, hetgeen voor het eerst is gebeurd in 2007.

Dit Informatiebeveiligingsbeleid is ook van toepassing voor het GBA, de BAG en het Suwinet. De afzonderlijke beleidsplannen voor deze applicaties komen met invoering van dit plan te vervallen

Het hierna volgende document is een actualisatie van "Gesloten Openheid" en geeft een invulling aan het informatiebeveiligingsbeleid voor de gemeente Leeuwarden voor 2014-2015. Dit beleidsdocument is geldig voor de gehele organisatie van de gemeente Leeuwarden.

[1] Code voor informatiebeveiliging, Nederlands Normalisatie Instituut, Delft, 2007 : NEN-ISO.IEC 27002.

Inhoud

SAMENVATTING

Dit informatiebeveiligingsbeleid beschrijft hoe binnen de Gemeente Leeuwarden moet worden omgegaan met informatie om de vereiste vertrouwelijkheid, integriteit en beschikbaarheid te kunnen waarborgen.

Het beleid moet bijdragen dat de continuïteit van de bedrijfsprocessen en dienstverlening wordt gegarandeerd en de schade bij beveiligingsincidenten wordt geminimaliseerd.

De gemeentelijke organisatie is in toenemende mate afhankelijk van een ongestoorde werking van haar informatiesystemen. De kwetsbaarheid van de gemeentelijke informatiesystemen is dan ook een groot risico, waarvan de gemeentelijke organisatie nadelige gevolgen kan ondervinden. Het is dus zaak door middel van zowel preventieve als repressieve beveiligingsmaatregelen de risico"s zoveel mogelijk te beperken. Om te bepalen welke maatregelen de gemeente moet nemen voor een optimale beveiliging van de eigen of aan haar toevertrouwde (informatie)systemen wordt een zorgvuldige afweging gemaakt tussen afhankelijkheid en kwetsbaarheid van de processen enerzijds, en de kosten/consequenties van de beveiligingsmaatregelen anderzijds.

Optimaal betekent daarom: op basis van afgewogen risicoanalyses.

Naast de uitkomsten van de risico analyses (kosten/baten) is een belangrijk onderdeel van het niveau van informatiebeveiliging het voldoen aan wet en regelgeving. Door de Wet Bescherming Persoonsgegevens worden eisen gesteld waaraan gemeenten moeten voldoen en die zich richten tegen enige vorm van onrechtmatige verwerking van gegevens. Ook vanuit andere wetgeving, zoals de GBA, BAG en Suwinet worden eisen gesteld aan het niveau van Informatiebeveiliging. Uitgangspunt hierbij is steeds dat er "passende"[2] beveiligings maatregelen worden genomen.

De noodzaak om informatiebeveiliging als vitaal onderdeel op te nemen in de bedrijfsprocessen, continu te monitoren en aan te passen zijn:

- Nieuwe voorschriften en controles vanuit de landelijke overheid;
- Inadequate informatiebeveiliging en vooral incidenten bij het lekken van informatie geven veel imagoschade;
- Technische ontwikkelingen vergen continu aanpassing maatregelen (voorkomen digitale inbraken)
- Uitbreiding van digitale gegevensuitwisseling zowel met burgers als andere externe organisaties;
- Het creëren van voldoende bewustzijn om vertrouwelijk om te gaan met gegevens is een moeizaam proces.

DE RISICOANALYSES EN AUDITS ZIJN ONDERDEEL VAN HET CONTROLEJAARPLAN INFORMATIEBEVEILING.

[2]Passend betekent in dit verband overeenstemming met de stand van de techniek en overeenkomstig de proportionaliteit tussen de maatregelen en de aard van de te beschermen gegevens.

1 INLEIDING

Binnen de gemeente Leeuwarden wordt een grote hoeveelheid gegevens verwerkt, variërend van publieke, vertrouwelijke tot geheime gegevens. Geautomatiseerde gegevensverwerking speelt een steeds grotere rol in vele bedrijfsprocessen binnen de gemeente. De bedrijfsvoering is in toenemende mate afhankelijk van integriteit en beschikbaarheid van informatie en geautomatiseerde informatiesystemen. Er is daarom systematische zorg vereist om de (geautomatiseerde) informatie(systemen) te beveiligen tegen verstoringen die schade kunnen toebrengen aan de bedrijfsvoering van de organisatie. Beveiliging is nodig om onze informatievoorziening te beschermen tegen bedreigingen, kwetsbaarheden en risico"s.

Het Informatiebeveiligingsbeleid is erop gericht de noodzakelijke basisbeveiliging te continueren. Die bestaat uit onder meer het nakomen van wettelijke verplichtingen, afhandeling van beveiligingsincidenten en continuïteitsplanning

Taken, verantwoordelijkheden en bevoegdheden op het gebied van informatiebeveiliging worden in dit beleid beschreven en zijn ingebed in de bestaande structuur van de organisatie.

1.1 Bijlage

Onderdeel van dit document is een bijlage waarin de volgende onderdelen zijn opgenomen:

1. Uitgangspunten van het informatiebeveiligingsbeleid;
2. Normenkader waaraan de gemeente Leeuwarden zich wil conformeren als uitgangspunten van het beleid op basis van de Code van Informatiebeveiliging;
3. Uitwerking van de maatregelen waarin beschreven zijn de basisbeveiligingsmaatregelen die de gemeente Leeuwarden heeft getroffen en de afspraken waaraan de organisatie zich moet houden om het gewenste basis niveau van beveiliging te handhaven;
4. Overzicht van de inhoudsopgave van het Handboek Informatiebeveiliging.

Deze bijlage is vooral bedoeld voor medewerkers die werkzaam zijn in het organisatie & informatie veld en/of medewerkers die het management ondersteunen voor deze taken.

2 ACHTERGRONDEN EN UITGANGSPUNTEN INFORMATIEBEVEILIGING

2.1 Wat is informatiebeveiliging

Informatiebeveiliging is het treffen en onderhouden van een samenhangend pakket maatregelen om de betrouwbaarheid van informatievoorziening te waarborgen. [3] Informatiebeveiliging is in die zin een integraal onderdeel van ieder proces binnen onze organisatie.

2.2 Belang van Informatiebeveiliging

De burger mag van de gemeente (de overheid) verwachten dat zij vertrouwelijk omgaat met gegevens die aan de gemeente wordt toevertrouwd. Dit betekent dat de gemeente een hoge prioriteit moet geven aan informatiebeveiliging. Dit is noodzakelijk om de vertrouwelijkheid en de beschikbaarheid van de gegevens te kunnen garanderen.

2.3 Doel van informatiebeveiliging

Het doel van informatiebeveiliging bij de gemeente Leeuwarden is drieledig [4]:

- Te voldoen aan de eisen die gesteld mogen worden vanuit de wet en regelgeving aan een betrouwbare overheid
- Het waarborgen van de continuïteit van de bedrijfsprocessen en dienstverlening.
- Het minimaliseren van eventuele schade, direct en indirect, die ontstaat uit beveiligingsincidenten.

2.4 Uitgangspunten informatiebeveiliging

```
ERROR: undefined
OFFENDING COMMAND: F1S63YFFFF

STACK:
```