Wachtwoordbeleid gemeente Tilburg
Beleidsuitgangspunten voor het gebruik van wachtwoorden

1.1 Doel
Om de beveiliging van (digitale) informatie te waarborgen zijn er maatregelen nodig rondom toegang tot de informatievoorziening van gemeente Tilburg. Dit wachtwoord beleid geeft kaders waaraan de organisatiebrede informatiesystemen moeten voldoen om informatiebeveiliging risico's te beperken.

Wachtwoorden vormen een belangrijk aspect van de informatiebeveiliging. Wachtwoorden zorgen ervoor dat onbevoegden minder gemakkelijk toegang kunnen krijgen tot informatie. Een eenvoudig wachtwoord evenals onduidelijke of niet gevolgde wachtwoord procedures en afspraken zijn een bedreiging voor de vertrouwelijkheid en integriteit van informatie. Dit kan uiteindelijk leiden tot het verlies van informatie en imagoschade van de gemeente.

1.2 Scope
Dit beleid en de uitwerking hiervan is van toepassing op alle informatievoorzieningen waar de gemeente Tilburg eigenaar van is, verantwoordelijke in is en waar de gemeente Tilburg beheerder van is. Dit betreft zowel de eigen omgeving (On Premise) als uitbestede diensten (SAAS).

1.3 Proceseigenaar wachtwoordbeleid
De proceseigenaar (verantwoordelijke) is de Chief Information Security Officer (CISO).

1.4 Verantwoordelijkheid
- De CISO is namens het College van B&W verantwoordelijk voor het beleid en controle op uitvoering hiervan.
- Beheerders van informatiesystemen zijn verantwoordelijk om het beleid te vertalen naar maatregelen binnen deze IT systemen (Security&Privacy by Design).
- Alle in- en externe medewerkers zijn verantwoordelijk voor het veilig omgaan met de eigen authenticatie gegevens.
- Team managers zien toe op naleving van het wachtwoordbeleid en zijn mede verantwoordelijk voor het uitdragen ervan. Bij het niet naleven van de afspraken neemt de teamleider passende maatregelen zoals het aanspreken van medewerkers op hun verantwoording.

1.5 Actualiteit
De CISO is verantwoordelijk voor het actueel houden van dit beleid en de communicatie binnen de organisatie.

1.6 Relatie
Dit beleid is gerelateerd aan het vastgestelde "informatiebeveiligingsbeleid 2017-2020 gemeente Tilburg". Uitgangspunten zijn ontleend aan de Baseline Informatie Beveiliging Gemeenten (BIG).

1.1.1 Algemene regels ten aanzien van wachtwoorden

Ten aanzien van wachtwoorden gelden de volgende regels en maatregelen:

☒	Standaard (leveranciers) wachtwoorden worden voor ingebruikname (productiegang) gewijzigd.
☒	Wachtwoorden worden (binnen systemen, applicaties en databases) nooit in originele vorm (plaintext) opgeslagen of verstuurd, maar altijd beveiligd opgeslagen.
☒	Wachtwoorden worden op een veilige manier uitgegeven (controle identiteit van de medewerker voor uitgifte van het wachtwoord).
☒	Wachtwoorden zijn persoonlijk en alleen bij de medewerker zelf bekend.
☒	Tijdelijke wachtwoorden of wachtwoorden die standaard in software of hardware worden meegegeven worden bij eerste gebruik vervangen door een persoonlijk wachtwoord.
☒	Tijdelijke wachtwoorden (eerste uitgifte) voldoen aan de eisen voor wachtwoord complexiteit (zie hieronder)
☒	Wachtwoorden moeten tekens uit **drie** van de volgende **categorieën** bevatten: Hoofdletters, Kleine letters, Cijfers, Niet-alfanumerieke tekens (!,$,&,#,%) en bestaan uit minimaal 8 karakters.
☒	Wachtwoorden zijn maximaal 60 dagen geldig en mogen niet binnen 24 keer herhaald worden.
☒	Wachtwoorden van beheerders zijn maximaal 42 dagen geldig en mogen niet herhaald worden.
☒	Systeem- en Servicewachtwoorden zijn maximaal 365 dagen geldig en mogen niet herhaald worden.
☒	Nadat een wachtwoord 5 keer foutief ingevoerd is wordt het account minimaal 30 minuten geblokkeerd. Indien er geen lock-out periode ingesteld kan worden, dan wordt het account geblokkeerd totdat de gebruiker verzoekt deze lock-out op te heffen of het wachtwoord te resetten.
	Toegang tot de informatievoorziening wordt verleend op basis van twee-factor authenticatie.[1] (met uitzondering van beheerde, vooraf gedefinieerde en goedgekeurde Mobile Device Management toepassingen voor mobiele apparaten. Reden hiervoor is een uniforme manier van authenticatie (intern- en extern) en een steeds hoger risico op inbreuk waarbij een interne netwerkomgeving niet per definitie als veilig kan worden aangemerkt.

De nog niet genomen maatregelen worden in de jaarlijkse evaluatie opnieuw beoordeeld en eventueel alsnog ingevoerd, waarna het beleid opnieuw zal worden vastgesteld.

1 Met twee-factor authenticatie wordt bedoeld dat je iets weet (je wachtwoord) en iets dat je hebt (bijvoorbeeld een token, key generator of smartphone). Bij drie-factor authenticatie komt daar nog iets bij dat je bent (vingerafdruk, irisscan).

1.1.2 Wachtwoorden voor eindgebruikers

Gebruikers behoren altijd goede beveiligingsgewoonten in acht te nemen zoals bij het kiezen en gebruiken van wachtwoorden. Andere algemene voorwaarden staan in het reglement gebruik kantoor faciliteiten.
Een aantal van de speerpunten worden in bewustwording sessies (iBewust &voorlichting m.b.t. informatiebeveiliging en privacy) meegenomen. Het wachtwoordgebruik is een van die speerpunten.

- Het wachtwoord is strikt persoonlijk en niet overdraagbaar.
- Wachtwoorden worden niet opgeschreven[2].
- Gebruikers delen hun wachtwoord nooit met anderen (geheimhouding is verplicht).
- Wachtwoorden mogen niet opeenvolgend zijn.
- Een wachtwoord wordt onmiddellijk gewijzigd als het vermoeden bestaat dat het bekend is geworden bij een derde.
- Gebruikers- en beheerderswachtwoorden worden niet gebruikt in automatische inlogprocedures (bijvoorbeeld opgeslagen onder een functietoets of in een macro).
- De gebruiker is verantwoordelijk voor het gebruik van de bevoegdheden die aan de combinatie van gebruikersnaam en wachtwoord zijn verbonden. De gebruiker moet dus alle redelijke maatregelen voor de beveiliging en geheimhouding van het wachtwoord hebben getroffen.
- De gebruiker zal bij constatering van misbruik van zijn combinatie van gebruikersnaam en wachtwoord de beheerder en de ISO/CISO hiervan onverwijld in kennis stellen.
- Incidenten (zoals misbruik van authenticatiegegevens) worden via de geldende procedures (incidentenmeldingen) geregistreerd (in Topdesk) en opgevolgd.

1.1.3 Externe toegang tot de informatievoorziening (toegang op afstand)

Externe toegang tot de informatievoorziening van of in beheer van “gemeente Tilburg” wordt zoveel mogelijk beheerst met een beveiligde inlogprocedure. Hierbij wordt gebruik gemaakt van de volgende aanvullende maatregelen:

Onder externe toegang wordt ook verstaan: Interne via draadloos ontsloten (bijv. WIFI) apparaten.

☒	Toegang tot de informatievoorziening wordt verleend op basis van twee-factor authenticatie.[3] (met uitzondering van beheerde, vooraf gedefinieerde en goedgekeurde Mobile Device Management toepassingen voor mobiele apparaten.
☒	Het wachtwoord wordt niet getoond op het scherm tijdens het ingeven. Er wordt geen informatie getoond die herleidbaar is tot de authenticatiegegevens.
	Voorafgaand aan het aanmelden wordt aan de gebruiker een melding getoond dat alleen geautoriseerd gebruik is toegestaan voor expliciet door de organisatie vastgestelde doeleinden.
☒	Voor mobiele apparaten die toegang hebben tot de informatievoorziening van gemeente Tilburg is de Wipe functie geactiveerd.

2 Wachtwoorden mogen wel in een door de vanuit de CISO goedgekeurde en vanuit de gemeente ondersteunde digitale wachtwoordenkluis worden opgeslagen.

2 Met twee-factor authenticatie wordt bedoeld dat je iets weet (je wachtwoord) en iets dat je hebt (bijvoorbeeld een token, key generator of smartphone). Bij drie-factor authenticatie komt daar nog iets bij dat je bent (vingerafdruk, irisscan).

Nog niet genomen maatregelen worden in de jaarlijkse evaluatie opnieuw beoordeeld en eventueel alsnog ingevoerd, waarna het beleid opnieuw zal worden vastgesteld.

1.1.4 Het beheren van wachtwoorden

Systemen voor wachtwoordbeheer behoren interactief te zijn en moeten bewerkstelligen dat wachtwoorden van geschikte kwaliteit worden gekozen.

☒	Er wordt automatisch gecontroleerd op goed gebruik van wachtwoorden (onder andere voldoende sterke wachtwoorden, regelmatige wijziging, directe wijziging van initieel wachtwoord).
☒	Wachtwoorden hebben een geldigheidsduur van maximaal 60 dagen. Na deze periode dient het wachtwoord bij een eerstvolgende inlog te worden gewijzigd.
	Wanneer het wachtwoord langer dan 100 dagen is verlopen, wordt het account geblokkeerd.
	Wachtwoorden die gereset zijn en initiële wachtwoorden zijn maximaal 14 dagen geldig en moeten bij het eerste gebruik worden gewijzigd.
☒	De gebruikers hebben de mogelijkheid hun eigen wachtwoord te kiezen en te wijzigen. Hierbij geldt dat voordat een gebruiker zijn wachtwoord kan wijzigen, de gebruiker opnieuw wordt geauthentiseerd.
☒	Beheerders van de informatievoorziening en (kritische) applicaties moeten een apart beheeraccount gebruiken voor beheerswerkzaamheden (functiescheiding).
☒	Systeem- en Serviceaccounts zijn voorzien van complexe wachtwoorden. Het doel, de toepassing en bijbehorende eigenaar dienen te worden vastgelegd.

Nog niet genomen maatregelen worden in de jaarlijkse evaluatie opnieuw beoordeeld en eventueel alsnog ingevoerd, waarna het beleid opnieuw zal worden vastgesteld.

1.2 Rapportage en controle

Het management controleert minimaal eens per jaar of dit beleid juist is toegepast binnen de informatiesystemen waar zij verantwoordelijk voor zijn.

Beheersmaatregel:	11.2.3
Documentversie:	31 januari 2019
Documentnaam:	11.2.3 Wachtwoordenbeleid.docx