

BERICHT VAN GO m.b.t. de informatiebeveiliging voor de GO-vergaderen app.

Dames en heer,

GO geeft m.b.t. de informatiebeveiliging voor de GO-vergaderen app. aan dat er een drietal wijzigingen aankomen:

- 1) wachtwoorden nog maar 60 dagen geldig i.p.v. een jaar;
- 2) de optie om ingelogd te blijven kunnen we binnenkort uitzetten: daar ben ik voor, dan kan een ander er niet in komen als ze hun iPad verliezen of als die gestolen wordt. Zijn jullie het daar mee eens?
- 3) Mogelijkheid tot 2-factor authenticatie komt eraan (als een nieuwe dienst = module die apart gekocht moet worden?). Dat betekent dat nadat je met inlognaam en ww begint in te loggen, je een SMS-bericht krijgt met een code die je in moet typen om helemaal in te loggen.

Dat laatste punt wil ik graag jullie ideeën over horen.

Pro:

Het versterkt de beveiliging op de toegang tot de besloten en soms erg (privacy)gevoelige informatie die in de GO-app ontsloten wordt voor de digitale vergaderingen (denk dan met name aan de bezwarencommissies en de besloten B&W).

Contra:

Aan de andere kant vergt het van de college- en commissie-/raadsleden bij elke keer dat ze de app willen gebruiken een paar extra handelingen; èn dat ze allemaal de beschikking hebben over een telefoon waarmee ze SMS berichten kunnen ontvangen en lezen op het moment dat ze hun digitale vergaderstukken willen gaan lezen of digitale vergaderagenda willen controleren.

Vragen:

Zijn jullie gebruikers daartoe in staat en bereid?

Is dit iets waar wij als gemeente ze toe willen gaan verplichten, uit informatiebeveiligings-oogpunt? Zo ja, wie beslist dat?

Met vriendelijke groeten,
Hanneke Nieuwenhuijzen

Werkzaam op dinsdag, woensdag, donderdag en vrijdag

Voor Corsa-helpdesk: maak een zelfservice-melding aan op Hugo! Topdesk-meldingen krijgen voorrang boven vragen via de mail!

[Gemeente Heerhugowaard, Afd.I&A](#)