SAEN-IT
laat IT en telecom werken zoals het hoort

Oude Blaauwweg 5
1521 RN WORMERVEER
Tel: +31753030040
E-Mail: info@saen-it.nl
Website: www.saen-it.nl

Wachtwoordbeleid 2023 - 2024

Beheerwachtwoorden:

Voor het beheer van randapparatuur en servers gebruiken we complexe wachtwoorden die voldoen aan strikte beveiligingsrichtlijnen. Deze wachtwoorden worden opgeslagen in de SAEN-IT passportal (wachtwoordenkluis). Ze zijn allemaal verschillend, hebben een minimale lengte van 12 karakters en bevatten hoofdletters, kleine letters, cijfers en speciale tekens. We implementeren altijd Twee-factorauthenticatie (2FA of MFA) waar mogelijk. Alleen geautoriseerde medewerkers van SAEN-IT hebben toegang tot deze beheerwachtwoorden.

Clientwachtwoorden Windows-domein:

Windows-domeinwachtwoorden worden veilig verstuurd via een wachtwoordlink in een e-mail. Deze link is maximaal 3 dagen geldig en vervalt na bekijken. Bij de eerste keer inloggen wordt de gebruiker gevraagd het wachtwoord zelf aan te passen. De frequentie van wachtwoordwijzigingen wordt bepaald door uw bedrijfspolicy. We slaan deze wachtwoorden niet op, behalve die van SAEN-IT Passportal gebruikers.

In geval van een vergeten Windows-domeinwachtwoord, kunnen wij deze alleen resetten. De gebruiker of de ICT-contactpersoon binnen uw bedrijf kan een wachtwoordreset aanvragen via een ticket (helpdesk@saen-it.nl) of via de desktopsnelkoppeling "Maak een nieuwe support ticket". We sturen dan een tijdelijk wachtwoord via de ticket naar het opgegeven e-mailadres, samen met een wachtwoordlink met eventueel instructies. Deze link is maximaal 3 dagen geldig en vervalt na bekijken. Het tijdelijke wachtwoord moet bij de eerste inlog worden aangepast. SAEN-IT Passportal gebruikers kunnen hun (tijdelijke) wachtwoord vinden in hun eigen SAEN-IT Passportal.

SAEN-IT
laat IT en telecom werken zoals het hoort

Oude Blaauwweg 5
1521 RN WORMERVEER
Tel: +31753030040
E-Mail: info@saen-it.nl
Website: www.saen-it.nl

Clientwachtwoorden Microsoft 365:

De initiële Microsoft 365-wachtwoorden worden verzonden via het Microsoft 365 portaal. Voor SAEN-IT Passportal gebruikers wordt het (tijdelijke) wachtwoord in het SAEN-IT Passportal geplaatst en bewaard. Bij ontvangst dient de gebruiker eerst in te loggen op het Microsoft portaal voordat deze in gebruik wordt genomen. Daar kan de gebruiker zijn/haar eigen wachtwoord kiezen en meteen multifactor authenticatie via de Microsoft Authenticator instellen en een (mobiel) telefoonnummer toe te voegen.

Indien u uw Microsoft 365-wachtwoord bent vergeten of niet kent, kunt u dit **zelf** aanpassen via https://login.microsoftonline.com. Log in met uw e-mailadres en klik op **"wachtwoord vergeten"**. Hiervoor moet wel een (mobiel) telefoonnummer bekend zijn in het Microsoft 365 portaal. Als dit niet lukt, kan de gebruiker of de ICT-contactpersoon binnen uw bedrijf een ticket aanmaken (helpdesk@saen-it.nl) of via de desktopsnelkoppeling "Maak een nieuwe support ticket" om het (mobiel) telefoonnummer door te geven en bij welk e-mailadres dit hoort. Wij zullen het (mobiel) telefoonnummer toevoegen aan het e-mailadres, waarna de gebruiker het wachtwoord kan wijzigen volgens de bovenstaande instructies **("wachtwoord vergeten")**. Indien beveiligingsgegevens ontbreken, wordt ook meteen gevraagd om de multifactor authenticatie via de Microsoft Authenticator in te stellen.

NAS systemen (Synology – QNAP) wachtwoorden:

Wachtwoorden voor NAS systemen (Synology – QNAP) worden veilig verstuurd via een wachtwoordlink in een e-mail. Deze link is maximaal 3 dagen geldig en vervalt na bekijken. We slaan deze wachtwoorden niet op, behalve die van SAEN-IT Passportal gebruikers.

Bij vergeten of onbekende wachtwoorden voor NAS systemen (Synology – QNAP) kunnen wij deze alleen resetten. De ICT-contactpersoon binnen uw bedrijf kan een wachtwoordreset aanvragen via een ticket (helpdesk@saen-it.nl) of via de desktopsnelkoppeling "Maak een nieuwe support ticket". We sturen dan een wachtwoord via de ticket naar het opgegeven e-mailadres, samen met een wachtwoordlink met instructies. Deze link is maximaal 3 dagen geldig en vervalt na bekijken. Gebruikers die gebruik maken van SAEN-IT Passportal kunnen hun wachtwoord vinden in hun eigen SAEN-IT Passportal.

SAEN-IT
laat IT en telecom werken zoals het hoort

Oude Blaauwweg 5
1521 RN WORMERVEER
Tel: +31753030040
E-Mail: info@saen-it.nl
Website: www.saen-it.nl

Webhosting en WordPress wachtwoorden:

Wachtwoorden voor webhosting en WordPress worden veilig verstuurd via een wachtwoordlink in een e-mail. Deze link is maximaal 3 dagen geldig en vervalt na bekijken. We slaan deze wachtwoorden niet op, behalve die van SAEN-IT Passportal gebruikers.

Bij vergeten of onbekende wachtwoorden voor webhosting of WordPress kunnen wij deze alleen resetten. De ICT-contactpersoon binnen uw bedrijf kan een wachtwoordreset aanvragen via een ticket (helpdesk@saen-it.nl) of via de desktopsnelkoppeling "Maak een nieuwe support ticket". We sturen dan een wachtwoord via de ticket naar het opgegeven e-mailadres, samen met een wachtwoordlink met instructies. Deze link is maximaal 3 dagen geldig en vervalt na bekijken. Gebruikers die gebruik maken van SAEN-IT Passportal kunnen hun wachtwoord vinden in hun eigen SAEN-IT Passportal.

Bij Saen-it nemen we de privacy en beveiliging van onze gebruikers/cliënten zeer serieus. Om deze reden bewaren wij geen wachtwoorden van onze gebruikers/cliënten. Dit geldt als standaardpraktijk. Er is echter één uitzondering op deze regel: gebruikers van SAEN-IT Passportal.

Voor de wachtwoorden die wij verstrekken via de link, geldt dat deze altijd voldoen aan de hoogste mate van complexiteit. Dit betekent dat simpele wachtwoorden niet worden ondersteund en evenmin worden verstrekt.

SAEN-IT
laat IT en telecom werken zoals het hoort

Oude Blaauwweg 5
1521 RN WORMERVEER
Tel: +31753030040
E-Mail: info@saen-it.nl
Website: www.saen-it.nl

Wachtwoorden tips

Complexiteit: Wachtwoorden moeten minimaal 12 tekens lang zijn en moeten een combinatie bevatten van hoofdletters, kleine letters, cijfers en speciale tekens.

Regelmatige Wijziging: Wachtwoorden moeten elke 90 dagen worden gewijzigd. Gebruikers worden aangemoedigd om nooit hetzelfde wachtwoord twee keer te gebruiken.

Geen Hergebruik van Wachtwoorden: Een nieuw wachtwoord mag niet overeenkomen met een van de laatste 5 gebruikte wachtwoorden.

Geen Persoonlijke Informatie: Wachtwoorden mogen geen persoonlijke informatie bevatten, zoals namen, geboortedata of gebruikersnamen.

Geen Woorden uit het Woordenboek: Wachtwoorden mogen geen bestaande woorden uit het woordenboek bevatten.

Gebruik van Een Wachtwoordmanager als SAEN-IT Passportal: Het gebruik van een betrouwbare wachtwoordmanager wordt sterk aangeraden om unieke en sterke wachtwoorden te genereren en op te slaan.

Vermijd Openbare Computers: Gebruik geen openbare computers of netwerken om in te loggen op accounts waar gevoelige informatie wordt opgeslagen.

Tweestapsverificatie (2FA/MFA): Schakel waar mogelijk tweestapsverificatie in om een extra beveiligingslaag toe te voegen aan je accounts.

Wachtwoordvoorbeelden (niet toegestaan):
- "Wachtwoord123"
- "Gebruikersnaam2023"
- "123456"
- "Welkom123"

Goed Wachtwoordvoorbeeld (aanbevolen):
- "SOc!@IM3d!@ROck$"

Dit beleid bevat nu duidelijke richtlijnen om sterke en veilige wachtwoorden te waarborgen. Zorg ervoor dat dit beleid wordt gecommuniceerd aan alle gebruikers en dat er bewustwordingstraining wordt gegeven over het belang van veilige wachtwoorden.