

PvE Gemeente Westerkwartier - ICT v2.0 - Nieuwe software

Systeemvereisten

De oplossing is volledig SAAS. De applicatie beschikt over een volledige schaalbare webbased userinterface die zonder beperking van functionaliteit, benaderbaar is op elk willekeurig device, door de laatste twee versies van de meest gangbare en ondersteunde webbrowsers (Microsoft Edge, Mozilla Firefox, Google Chrome, Apple Safari), zonder gebruik te maken van plug-ins (zoals Flash, Silverlight, ActiveX of soortgelijke).

Alle activiteiten in het systeem moeten in het kader van een audit-trail worden gelogd in een logboek. De beheerder mag niet in staat zijn dit log te muteren.

Minimaal de homepage is te personaliseren conform de huisstijl van de organisatie.

Het systeem vereist geen installatie van additionele programmatuur op de desktop van de gebruiker.

Informatiebeveiliging

Versleuteling van het verkeer tussen browser en SAAS-oplossing is minimaal A+. (ssllabs)

Het systeem heeft een functie om inloggen en registreren tijdelijk te deactiveren.

Het is mogelijk om gebruikersaccounts tijdelijk toegang te geven met een verlooptdatum.

Inlogpogingen moeten worden gelogd met minimaal een IP-adres.

Registraties van accounts met een vreemd domein moeten worden goedgekeurd door de beheerder.

De SAAS-oplossing moet gelocaliseerd zijn in de EU en bij voorkeur in Nederland.

Het systeem legt geen bijzondere persoonsgegevens vast volgens de definitie van artikel 16 Wbp.

Het datacenter waar de SAAS-oplossing is gelocaliseerd is ISO-27001 gecertificeerd.

De informatiebeveiliging vindt plaats volgens een algemeen erkend normenstelsel zoals NEN7510, NEN/ISO-27001, PCI/DSS of een overheidsnorm zoals BIG, BIR of BIO.

Two-Factor authentication is mogelijk met de Microsoft authenticator, SMS of met E-mail voor autorisatie van service accounts.

Er moet een sterk wachtwoordbeleid zijn geïmplementeerd indien geen gebruik wordt gemaakt van MFA. Plus 2 keer per jaar het wachtwoord vernieuwen

Er wordt periodiek een pentest en kwetsbaarhedescan uitgevoerd op de dienst. TPM verklaring

Bewaking en detectie van inbraakpogingen + incidentrespons

Wordt een eventuele inbraak of datalek gemeld?

De dienst wordt gemonitord door een SIEM en/of SOC middels detectie voorzieningen.

In en uitgaand netwerkverkeer wordt bewaakt (geanalyseerd op kwaadaardige elementen)

Heeft de saas provider een "responsible disclosure policy"

Versleuteling van de data in opslag (database, etc)

Security patches worden zo snel mogelijk geïnstalleerd.

Blijft Westerkwartier eigenaar van de opgeslagen data in de saas omgeving. Dit in geval bij een eventueel faillissement van de SaaS provider

De applicatie moet voldoen aan de internetstandaarden volgens de site 'internet.nl' en moet hier 100% score behalen. Hierop kan getoetst worden.

Onderhoud, Support, Releasebeleid

Leverancier heeft een telefonische helpdesk tijdens kantooruren.

Leverancier heeft een online helpdesk en online handleiding.

Leverancier biedt een persoonlijk aanspreekpunt en directe communicatielijnen.

Leverancier heeft een Service Level Agreement. Voeg een bijlage toe met de responstijden per 'severity'.

Leverancier heeft een releasebeleid. Voeg een bijlage toe met het releasebeleid.

Systeemkoppelingen

De Applicatie (Saas) koppelt aan Microsoft Azure-AD voor SAML authenticatie t.b.v. toegang

Indien de applicatie beschikt over een mailvoorziening, dan moet doormiddel van mail relay naar de omgeving van de Opdrachtgever gerouteerd worden met een herkenbare domeinnaam van de betreffende organisatie.

De applicatie ondersteunt een directe databaseconnectie al dan niet via een API zodat de gegevens in een dataplatform als PowerBI gebruikt kunnen worden.