Informatie over Veiligheid

YouBasicsCM Contractmanagementsysteem

Informatieveiligheid is van groot (en groeiend) belang bij het inzetten van software. YouBasicsCM draait op het Betty Blocks platform. Servicepartner Ilionx draagt zorg voor doorontwikkeling en service. In dit document geven wij een overzicht van de maatregelen welke genomen zijn om een degelijke, stabiele en bovenal veilige tool te kunnen bieden.

Inhoud

Veiligheidsstandaarden

- Zowel het platform als de datacenters van Betty Blocks zijn ISO27001 gecertificeerd. Wanneer gewenst kan Opdrachtnemer de certificaten en “Statement of Applicability” aanleveren.
- De richtlijnen voor hardening van zowel NIST 800-53 als de CIS Benchmarks worden toegepast, zodat een robuuste en veilige IT-infrastructuur gewaarborgd is.
- Alle verplichte beveiligingsstandaarden van het forum standaardisatie zijn toegepast.
- De web interface is beveiligd tegen de OWASP top-10
- Mail is beveiligd met STARTTLS over ten minste het TLS1.3 protocol, DANE, DNSSEC of gekoppeld met Exchange Online via MS Graph.
- De leverancier past de ICT-beveiligingsrichtlijnen voor webapplicaties toe. Servicepartner Betty Blocks is in het verleden ook met regelmaat geaudit op naleving van de NCSC-richtlijn BWA.
- Vanuit de Cloud Control Matrix zijn overeenkomsten omschreven met de aanwezige TOMS vanuit ISO27001. Een overzicht met genomen maatregelen vanuit CCM is desgewenst beschikbaar.
- De software functioneert voor wat betreft aspecten van beveiliging en privacy volledig conform alle betreffende wet- en regelgeving (ten minste AVG en BIO) en andere van

toepassing zijnde wetgeving. De BIO voldoet uiteraard enkel voor de reikwijdte die redelijkerwijs aan een SaaS-leverancier kan en behoort te worden gesteld.
- Er zijn maatregelen genomen om de applicatie te beschermen tegen DDOS aanvallen.

Gegevensbeheer

- De leverancier heeft een procedure voor het verwijderen van data/ informatie.
- Gegevens en documenten worden opgeslagen en verwerkt in een datacenter/cloudserver binnen de Europese Unie. YouBasicsCM wordt gehost in beveiligde datacenters van Betty Blocks. Deze Microsoft Azure datacenters bevinden zich in Nederland alsmede dus ook de data.
- Bij de leverancier bestaand duidelijke beleidslijnen en procedures voor het beheren van de levenscyclus van gegevens, inclusief creatie, opslag, gebruik, delen, archiveren en vernietigen.
- Gezien binnen YouBasicsCM géén cliëntgegevens worden opgeslagen, is de AVG-wetgeving hierop niet van toepassing.

Autorisatie

- De software heeft een mogelijkheid om vastgelegde autorisaties op alle niveaus inzichtelijk te maken per persoon, per gebruikersgroep en rol. Hiervoor is het toegepaste autorisatieschema te exporteren naar een bestand, dat leesbaar en interpreteer baar is voor derden (zoals toezichthouders zoals bijvoorbeeld de accountant, auditors, etc.).
- Gebruikers krijgen enkel toegang tot de informatie die toebehoort aan de functie en rol.

Authenticatie

- Iedere gebruiker, dus ook van de beheerder en van de aanbieder, heeft een eigen account op naam (en is daarmee herleidbaar).
- YouBasicsCM kan gebruik maken van Multi-Factor Authenticatie (MFA) en Single Sign-On (SSO) indien van toepassing. De software ondersteunt veilig inloggen door SSO door middel van OAuth en SAML en federatie met Azure AD.

Back-up

- Binnen Betty Blocks wordt iedere nacht een back-up gemaakt van alle gegevens. Deze back-up wordt middels een beveiligde verbinding naar een fysiek gescheiden en eveneens streng beveiligde locatie gemaakt. De back-up gegevens worden bovendien middels encryptie onleesbaar voor derden opgeslagen. Opdrachtgever kan deze back-up bij calamiteiten opvragen bij Opdrachtnemer.

Cookie beheer

- Er worden geen vertrouwelijke gegevens in cookies opgeslagen.
- Cookies ten behoeve van authenticatie worden niet persistent opgeslagen.
- YouBasicsCM gebruikte unieke namen, paden en domeinen voor cookies ten behoeve van authenticatie (cookie parameters ‘name’, ‘path’ en ‘domain’).

Export functionaliteit

- In beginsel is voor gebruikers géén mogelijkheid beschikbaar voor het exporteren van gegevens. In overleg met het serviceteam zijn rapportages te reproduceren.
- De mogelijkheid bestaat alle gegevens te exporteren naar een gestandaardiseerd formaat, wanneer daaraan behoefte is, bijvoorbeeld na beëindigen van het contract met YouBasicsCM.

Compatibiliteit

- YouBasicsCM is benaderbaar via een browser userinterface en is compatible met Microsoft, Android en Apple op basis van de laatste én voorlaatste versies van het operating systeem.
- YouBasicsCM werkt cliënt- en platform onafhankelijk.
- Voor gebruik van de applicatie hoeven géén plug-ins te worden geïnstalleerd.

Incident management

- Binnen de Service Level Agreement (SLA) wordt met iedere klant vastgelegd welk serviceniveau op welk moment van toepassing is. Op basis van de urgentie van het incident worden responsetijden afgesproken.

Wachtwoordbeheer

- Er wordt geen gebruik gemaakt van een standaard wachtwoord. Ieder toegekend wachtwoord is willekeurig gegenereerd.
- Voor het beheren van wachtwoorden van speciale accounts (bijv. admin- of serviceaccounts) wordt een passwordmanager gebruikt.
- Geen account heeft hetzelfde wachtwoord. Voor toegang tot de wachtwoordkluis is twee factor-authenticatie nodig
- Wachtwoorden van accounts van diensten (serviceaccounts) dienen complex te zijn en tenminste 20 karakters lang.

Versleuteling

- De gegevens die opgeslagen zijn (zowel in de back-up als in rust) en de gegevens die worden overgedragen, worden gedurende de gehele duur van het contract versleuteld volgens de geldende standaarden. Op dit moment zijn de standaarden voor gegevensoverdracht TLS 1.2 en TLS 1.3, en voor gegevens in rust wordt Advanced Encryption Standard (AES)-256 gebruikt.
- De software ondersteunt TLS 1.3 met betrekking tot de API-koppelingen voor gegevensuitwisselingen.

Sessiebeheer

- Het is mogelijk sessies automatisch te laten beëindigen na 5 of 15 minuten van activiteit, om ongeoorloofde toegang tot gevoelige gegevens te minimaliseren.
- Kritieke en vertrouwelijke sessiewaardes worden niet doorgegeven via een QUERY-string.

Logging

- YouBasicsCM biedt zodanige functionaliteit met betrekking tot logging dat wijzigingen door gebruikers worden opgeslagen. Meer specifieke logging, welke inzicht geven op processen, processtappen en statuswijzigingen, zowel door de gebruikers als de applicatie zelf, wordt ontwikkeld.

Privacy

- Het is mogelijk een DPIA of pre-PIA test uit te voeren wanneer dit nodig is.
- De applicatie ondersteunt passende technische en organisatorische maatregelen om de privacy van persoonlijke gegevens te waarborgen vanaf het ontwerp en de standaardinstellingen.
- YouBasicsCM biedt functionaliteit om individuen in staat te stellen hun rechten uit te oefenen, zoals toegang, rectificatie, verwijdering en dataportabiliteit van hun persoonlijke gegevens.

- De applicatie biedt de mogelijkheid om persoonsgegevens enkel en alleen te verwerken voor specifieke, welomschreven en rechtmatige doeleinden.
- YouBasicsCM bevat een geautomatiseerd proces voor het detecteren, rapporteren en reageren op inbreuken op de beveiliging van persoonsgegevens. Hierbij wordt voldaan aan de meldingsplicht datalekken.

Pentest

- Betty Blocks werkt mee aan audits en pentesten ten behoeve van YouBasicsCM. In overleg tussen klant en implementatiepartner kan bepaald worden waar en wanneer een pentest wordt uitgevoerd, voorafgaand aan de pentest dient Betty Blocks genotificeerd te worden. Daarnaast verwacht Betty Blocks dat voorafgaande aan de test een LoA overlegd wordt (vanuit de klant richting Betty Blocks) en dat pentest resultaten naderhand worden gedeeld.