
# Przegląd bezpieczeństwa

Ostatnia aktualizacja: Luty 2020

# Spis treści

## 1. Nasza firma i produkt

Jesteśmy firmą informatyczną z Krakowa, która rozpoczęła działalność w 2017 roku. Stworzyliśmy innowacyjny system QRmaint CMMS i udoskonalamy go nieprzerwanie do dzisiaj, korzystając z praktycznych wskazówek wielu naszych klientów.

Naszą misją jest upowszechnianie systemów CMMS w zakładach produkcyjnych i szeroko rozumianym utrzymaniu technicznym. Stawiamy na proste i skuteczne rozwiązania dostępne dla wszystkich.

Produkt QRmaint CMMS jest oferowany w modelu Software-as-a-Service (SaaS). Rozwiązanie te jest dostępne dla naszych klientów za pośrednictwem aplikacji internetowej, aplikacji mobilnej lub application programming interfaces (API).

## 2. Bezpieczeństwo QRmaint i zarządzanie ryzykiem

Głównym celem QRmaint w zakresie bezpieczeństwa jest ochrona danych naszych klientów i użytkowników. Jest to jeden z powodów, dla których nasza firma zainwestowała w odpowiednią infrastrukturę i inne zasoby, które pozwolą zapewnić poziom bezpieczeństwa na najwyższym poziomie. Skupiamy się na definiowaniu nowych i udoskonalaniu już istniejących mechanizmów kontroli, zarządzaniu strukturą bezpieczeństwa QRmaint, a także ciągłym jej rozwijaniu.

## 3. Nasze cele dot. bezpieczeństwa i zarządzania ryzykiem

Opracowaliśmy nasze ramy bezpieczeństwa, korzystając z najlepszych praktyk w branży SaaS. Nasze główne cele to:

- Zaufanie klientów - konsekwentnie dostarczamy naszym klientom najwyższej jakości produkty i usługi, jednocześnie chroniąc prywatność i poufność ich informacji.
- Dostępność i ciągłość działania - doskonale wiemy jak ważna dla naszych klientów jest stała dostępność do naszej aplikacji i innych usług, dlatego cały czas minimalizujemy zagrożenia bezpieczeństwa zagrażające ciągłości usług.
- Zgodność ze standardami - wdrażamy procesy i kontrole, aby dostosować się do aktualnych międzynarodowych przepisów i wytycznych dotyczących najlepszych praktyk branżowych. Zaprojektowaliśmy nasz program bezpieczeństwa zgodnie z najlepszymi wytycznymi dotyczącymi bezpieczeństwa w chmurze.

## 4. Kontrola bezpieczeństwa

W celu zapewnienia ochrony powierzonych nam danych wdrożyliśmy szereg zabezpieczeń. W poniższych sekcjach wymieniamy najważniejsze z nich.

## 4.1 Infrastruktura QRmaint

### 4.1.1 Bezpieczeństwo centrum danych

QRmaint zleca hosting infrastruktury swoich produktów wiodącemu dostawcy infrastruktury chmurowej. Jest to Amazon Web Services (AWS). Rozwiązanie te zapewnia najwyższy poziom bezpieczeństwa fizycznego i sieciowego. Obecnie instancję serwerów chmurowych QRmaint znajdują się w Niemczech. Centrum danych spełnia poziom zgodny z normami SOC 2 oraz ISO 27001. O jakości bezpieczeństwa centrum danych AWS świadczy fakt, że największe banki USA przenoszą swoje centra danych do Amazon AWS, gdyż nie są w stanie osiągnąć tak wysokiego poziomu bezpieczeństwa.

Ten światowej klasy dostawca infrastruktury wykorzystuje najbardziej zaawansowane technologie infrastruktury obiektów w zakresie zasilania, sieci i bezpieczeństwa fizycznego. Czas działania jest gwarantowany na poziomie od 99,95% do 100%, a obiekty zapewniają minimum N+1 nadwyżki dla zasilania, sieci, oraz infrastruktury HVAC. Dostęp do centrów danych jest ściśle ograniczony zarówno do dostępu fizycznego, jak i elektronicznego za pośrednictwem sieci publicznych (internet) jak i sieci prywatnych(intranet) w celu wyeliminowania wszelkich niepożądanych przerw w świadczeniu usług.

Zabezpieczenia fizyczne, środowiskowe i infrastrukturalne, w tym plany ciągłości i odtwarzania, zostały zatwierdzone w ramach certyfikacji SOC 2 typu II i ISO 27001. Certyfikaty są dostępne na stronie: AWS Cloud Compliance

### 4.1.2 Bezpieczeństwo sieci

Infrastruktura produktu QRmaint jest zbudowana z myślą o zabezpieczeniach na skalę udostępnienia usług w sieci internet. W szczególności zabezpieczenia sieci mają na celu zapobieganie nieautoryzowanemu dostępowi do sieci z zewnątrz i wewnątrz wewnętrznej infrastruktury produktu. Te mechanizmy zabezpieczeń obejmują routing klasy enterprise i zabezpieczenie dostępu do sieci firewall (zapora). Te technologie domyślnie blokują niezamierzony ruch, a cały ruch sieciowy jest rejestrowany i używany do informowania naszych systemów monitorowania. Reguły dostępu do sieci umożliwiają precyzyjną kontrolę ruchu sieciowego z sieci publicznej. W ramach infrastruktury ograniczenia sieci wewnętrznej pozwalają na wielopoziomowe podejście do zapewnienia komunikacji tylko odpowiednich typów urządzeń.

### 4.1.3 Zarządzanie konfiguracją

Infrastruktura QRmaint pozwala na skalowanie zgodnie z potrzebami naszych klientów. Infrastruktura produktu to środowisko, które w razie potrzeby elastycznie zwiększa pojemność i możliwości.

### 4.1.4 Dostęp do infrastruktury

Dobrze zaprojektowany model kontroli dostępu zapobiega potencjalnym zdarzeniom związanym z bezpieczeństwem. W związku z tym dostęp do systemów QRmaint jest ściśle

kontrolowany. Pracownicy QRmaint uzyskują dostęp do usług firmowych infrastruktury produktowej w oparciu o ich pracę, z wykorzystaniem modelu kontroli dostępu opartego na rolach. Dostęp do narzędzi infrastruktury, serwerów i podobnych usług, dostęp jest ograniczony tylko do osób, których praca tego wymaga.

## 4.2 Ochrona aplikacji

### 4.2.1 Ochrona aplikacji webowej i mobilnej

Wszystkie treści klientów hostowane na platformie są automatycznie chronione. Reguły używane do wykrywania i blokowania złośliwego ruchu są zgodne z wytycznymi dotyczącymi najlepszych praktyk udokumentowanych w projekcie Open Web Application Security Project (OWASP). Włączono również zabezpieczenia przed atakami typu Distributed Denial of Service (DDoS), które mają pomagać zapewnić ciągłą dostępność usług i produktów QRmaint. Narzędzia te aktywnie monitorują ruch w warstwie aplikacji w czasie rzeczywistym, umożliwiając ostrzeganie lub odrzucanie złośliwego zachowania na podstawie typu i częstotliwości zachowania.

Ochrona danych naszych klientów jest dla nas najwyższym priorytetem, dlatego zabezpieczenie naszego serwisu jest kluczowe. Zespół ds. bezpieczeństwa nieustannie pracuje nad udoskonaleniem mechanizmów bezpieczeństwa, m.in CSRF, XSS, SQLi, zarządzanie sesją, przekierowywanie URL oraz clickjacking.

### 4.2.2 Zarządzanie nową wersją

Jedną z największych zalet QRmaint jest szybko rozwijający się zestaw funkcji i stale ulepszany produkt dzięki nowoczesnemu podejściu do ciągłego dostarczania oprogramowania. Nowy kod jest testowany, zatwierdzany, scalany i wdrażany wiele razy. Przeglądy kodu w celu zapewnienia jakości są przeprowadzane przez wyspecjalizowane zespoły inżynierów, posiadających dogłębną wiedzę na temat platformy QRmaint. Po zatwierdzeniu kod jest automatycznie przesyłany do środowiska QRmaint, gdzie następuje kompilacja, pakowanie i testowanie. Jeśli wszystkie przejdą pomyślnie, nowy kod zostanie wdrożony automatycznie w warstwie aplikacji.

## 4.3 Ochrona danych klientów

### 4.3.1 Informacje poufne

QRmaint to produkt, który wspiera procesy utrzymania technicznego obiektów oraz urządzeń w firmach. Zgodnie z regulaminem oraz polityką prywatności klienci zapewniają, że przechowują tylko odpowiednie informację w celu wsparcia ich procesów związanych z utrzymaniem. Produkty QRmaint nie są używane do zbieranie, ani przechowywania danych wrażliwych, takich jak numery kart płatniczych, informacji o osobistym koncie bankowym, numery PESEL, numery paszportów, numery prawa jazdy lub podobne dokumenty ani informacji dotyczących zatrudnienia, finansów lub zdrowia.

### 4.3.2 Ochrona danych kart kredytowych

Wielu klientów QRmaint płaci za usługę kartą kredytową. QRmaint nie przechowuje, nie przetwarza ani nie zbiera informacji o kartach kredytowych przekazanych nam przez klientów. Korzystamy z usług zaufanych i zgodnych z PCI dostawców usług płatniczych (DotPay), aby zapewnić, że dane kart kredytowych klientów są przetwarzane w bezpieczny sposób oraz zgodnie z odpowiednimi przepisami i standardami branżowymi.

### 4.3.3 Szyfrowanie

Wszystkie interakcje z produktami QRmaint (np. wywołania API, logowanie, uwierzytelnione sesje do portalu klienta itp.) są szyfrowane podczas przesyłania za pomocą kluczy TLS 1.0, 1.1, 1.2 lub 1.3 i 2048 bitowych lub lepszych.

QRmaint wykorzystuje kilka technologii, aby zapewnić szyfrowanie przechowywanych danych. Fizyczne i zwirtualizowane dyski twarde używane przez instancje serwera produktu QRmaint, a także rozwiązania do długoterminowego przechowywania danych, takie jak AWS S3, używają szyfrowania AES-256.

## 4.4 Prywatność

Prywatność danych naszych klientów jest jednym z głównych aspektów, na których koncentrujemy się w QRmaint. Jak opisano w naszej Polityce prywatności, nigdy nie udostępniamy Twoich danych osobowych osobom trzecim. Zabezpieczenia opisane w tym dokumencie i inne zabezpieczenia, które wdrożyliśmy, mają na celu zapewnienie, że Twoje dane pozostaną prywatne i niezmienione. QRmaint jest projektowany i budowany z myślą o potrzebach klientów i ochronie prywatności. Nasz program ochrony prywatności obejmuje sprawdzone metody, potrzeby klientów i ich kontaktów, a także wymagania prawne.

### 4.4.1 Polityka przechowywania danych

Dane klienta są przechowywane tak długo, jak długo pozostajesz aktywnym klientem. Platforma QRmaint zapewnia aktywnym klientom narzędzia do usuwania ich danych według własnego uznania. Dane byłych klientów są usuwane z aktywnych baz danych na pisemny lub elektroniczny wniosek klienta lub po ustalonym okresie po wygaśnięciu wszystkich umów. Dane klientów Free trial (testowych) są usuwane, gdy portal nie jest już aktywnie używany, a dane byłych płacących klientów są usuwane 90 dni po rozwiązaniu wszystkich relacji. Informacje przechowywane w replikach, snapshotach i kopiach zapasowych nie są aktywnie usuwane, ale zamiast tego naturalnie starzeją się w repozytoriów w miarę cyklu życia danych.

## 4.5 Ciągłość procesów biznesowych i odzyskiwanie danych

QRmaint dba oraz rozwija procesy dbające o ciągłość działania i plany odtwarzania po awarii, koncentrując się zarówno na zapobieganiu przestojom, jak i na strategiach szybkiego przywracania w przypadku problemów z dostępnością lub wydajnością. Zawsze, gdy pojawiają się sytuacje wpływające na klientów, celem QRmaint jest szybkie i przejrzyste odizolowanie i rozwiązanie problemu.

#### 4.5.1 Kopie zapasowe (backupy)

Kopie bezpieczeństwa danych naszych klientów o wykonujemy codziennie i przechowujemy na osobnych serwerach. Okres przechowywania kopii zapasowych zależy od charakteru tych danych.

## 5. Zakres i zastosowanie dokumentu

QRmaint ceni transparentność w sposobach dostarczania rozwiązań naszym klientom. Ten dokument został zaprojektowany z myślą o przejrzystości. Stale ulepszamy zabezpieczenia, które zostały już wdrożone. Dane w tym dokumencie nie mają na celu stworzenia wiążącego lub umownego zobowiązania między QRmaint, a innymi stronami,  a także nie zmieniają jakiekolwiek istniejące umowy między stronami.