Polityka bezpieczeństwa i prywatności serwisu MJ-viewer

1. Zaufanie i prywatność danych

- Prywatność danych klientów jest traktowana jako fundament działalności.
- Dane użytkowników są przetwarzane zgodnie z zasadami minimalizacji i przejrzystości.

2. Przechowywanie i kopie zapasowe

- Bazy danych: każda zmiana w bazie jest zapisywana w logach zapisu (write-ahead logs), które są przesyłane do redundantnych, rozproszonych centrów danych. Umożliwia to szybkie odtworzenie stanu bazy w razie awarii.
- Konfiguracja i metadane aplikacji: backup wykonywany codziennie i przechowywany w wysokodostępnej infrastrukturze.
- Infrastruktura platformy: wszystkie elementy (obrazy instancji, bazy danych itd.) są zabezpieczone i przechowywane w redundantnych systemach, co umożliwia przywrócenie stanu do sekund po awarii.

3. Odzyskiwanie po awarii (Disaster Recovery)

- Aplikacje i bazy danych klientów: automatyczne przywracanie w razie awarii — platforma dynamicznie uruchamia aplikacje i ponownie wznawia elementy infrastruktury.
- Platforma: zaprojektowana z myślą o redundancji i odporności, działa w wielu centrach danych. Po awarii odtwarza się działanie z backupów i obrazów systemu. Każdy incydent podlega analizie przyczyn i wdrażane są usprawnienia.
- Retencja danych i usuwanie: użytkownik decyduje, co przechowywać lub usuwać. Po usunięciu aplikacji i bazy danych — informacje przechowywane są jeszcze tydzień, a następnie automatycznie niszczone. Fizyczne nośniki danych są niszczone zgodnie ze standardami DoD 5220.22-M lub NIST 800-88.

4. Prywatność i ochrona danych

- Stosowana jest jasna polityka prywatności określająca, jakie dane są zbierane i w jaki sposób wykorzystywane.

- Mechanizmy ochrony obejmują: uwierzytelnianie i kontrolę dostępu, szyfrowanie danych (HTTPS/SSL)

5. Dostęp pracowników do danych klientów

- Pracownicy nie mają dostępu do danych klientów w codziennych operacjach.
- Jeśli dostęp jest konieczny — wymagana jest zgoda klienta lub nakaz prawny.
- Każde takie działanie jest rejestrowane (czas, powód, zakres dostępu).

6. Bezpieczeństwo wewnętrzne (pracownicy i polityki)

- Wszyscy pracownicy przechodzą weryfikację przed zatrudnieniem.
- Obowiązuje przestrzeganie polityk bezpieczeństwa i zasad użytkowania.
- Funkcjonuje dedykowany zespół ds. bezpieczeństwa, współpracujący z całą organizacją w celu minimalizacji ryzyka.

7. Standardy bezpieczeństwa oferowane przez AWS S3 (zdjęcia, faktury, wszelkie dane statyczne)

- Szyfrowanie danych w spoczynku: Amazon S3 wspiera szyfrowanie po stronie serwera (SSE) z wykorzystaniem kluczy zarządzanych przez AWS (SSE-S3), kluczy zarządzanych przez AWS KMS (SSE-KMS) oraz kluczy dostarczanych przez klienta (SSE-C).
- Wszystkie dane przesyłane do i z S3 mogą być szyfrowane przy użyciu protokołu HTTPS (TLS).
- Kontrola dostępu: dostęp do zasobów S3 jest zarządzany poprzez polityki IAM, polityki bucketów oraz listy kontroli dostępu (ACL).
- Blokowanie publicznego dostępu: domyślne ustawienia pozwalają na blokowanie wszelkiego publicznego dostępu do bucketów i obiektów.
- Rejestrowanie i audyt: AWS S3 umożliwia rejestrowanie żądań poprzez AWS CloudTrail oraz dostęp do logów dostępu w celu monitorowania i audytu.
- Odporność i dostępność: dane w S3 są przechowywane redundantnie w wielu lokalizacjach w ramach regionu AWS, co zapewnia wysoką dostępność i trwałość (99.999999999%).

8. Centra danych AWS i certyfikaty bezpieczeństwa

- Infrastruktura: globalna sieć centrów danych AWS o wysokiej dostępności.

- Bezpieczeństwo fizyczne: kontrola dostępu, monitoring, ochrona 24/7.
- Zgodność z normami: ISO 27001, ISO 27017, ISO 27018, SOC 1/2/3, PCI DSS, HIPAA, FedRAMP.
- Audyt i zgodność: regularne audyty niezależnych podmiotów.
- Odpowiedzialność współdzielona: AWS odpowiada za infrastrukturę, klient za aplikacje i dane.