

DZIAŁ 2: WYBRANE METODY OCHRONY DANYCH I STANDARDY CYFROWE

1. Szyfrowanie i Bezpieczeństwo Transmisji

Miejsca logowania oraz wprowadzania danych osobowych (formularz rezerwacji) są chronione w warstwie transmisji za pomocą certyfikatu SSL (Secure Socket Layer) o wysokim standardzie szyfrowania. Dzięki temu dane osobowe i parametry płatności zostają zaszyfrowane w komputerze użytkownika i mogą być odczytane jedynie na docelowym, autoryzowanym serwerze.

2. Standardy Bankowe i Rezerwacyjne (Operator płatności elektronicznych / Zewnętrzny system rezerwacyjny online)

W celu maksymalnego zabezpieczenia środków i danych finansowych Gości, Operator stosuje infrastrukturę renomowanych partnerów:

- **Zewnętrzny system rezerwacyjny online:** Wszystkie dane rezerwacyjne procesowane są w środowisku spełniającym rygorystyczne wymogi ochrony danych osobowych.
- **Standard Operatora płatności elektronicznych:** Rozliczenia realizowane są w oparciu o infrastrukturę Instytucji płatniczych, co zapewnia bezpieczeństwo transakcji kartowych zgodnie z wymogami PCI DSS.
- **Organizacja oraz Procesy fakturowania:** Nadzór nad płatnościami (w tym obsługa kaucji) jest w pełni zautomatyzowany, co minimalizuje ryzyko błędów ludzkich i nieuprawnionego dostępu do dokumentacji finansowej.

3. Procedury Wewnętrzne i Kopie Zapasowe

- **Kopie Bezpieczeństwa:** Operator regularnie wykonuje zaszyfrowane kopie bezpieczeństwa (backup), co gwarantuje ciągłość danych i możliwość ich odzyskania w przypadku awarii systemów zewnętrznych.
- **Zarządzanie Dostępem:** Operator stosuje rygorystyczną politykę haseł administracyjnych, które są okresowo zmieniane oraz chronione przez mechanizmy wieloskładnikowego uwierzytelniania.
- **Aktualizacje Systemowe:** Kluczowym elementem ochrony jest regularna aktualizacja oprogramowania i komponentów programistycznych, co pozwala na bieżące eliminowanie podatności systemowych.

4. Bezpieczeństwo Fizyczne i Monitoring

Teren obiektu Natural Mielno jest monitorowany, a dostęp do urządzeń

przetwarzających dane jest ograniczony wyłącznie do osób upoważnionych, co zapobiega fizycznemu dostępowi osób trzecich do serwerów i dokumentacji.