SIGURNOST PLAĆANJA

1. Uvod

Ovaj dokument definira mjere i procedure kojima se osigurava sigurnost plaćanja na ***Mémoire – A Niche Perfumery*** *web shopu (on-line trgovini) na sljedećoj mrežnoj adresi:* *https://memoireperfumery.hr/*

[Flowable d.o.o. / Trnsko 42a / 10 010 Zagreb / OIB: 97742618910]

Cilj je zaštititi osjetljive podatke korisnika i osigurati sigurno procesuiranje financijskih transakcija.

2. Ciljevi

- **Zaštita podataka:** Osigurati da su svi osjetljivi podaci (osobni podaci, podaci o plaćanju) zaštićeni od neovlaštenog pristupa.
- **Prevencija prijevara:** Implementirati mjere za sprečavanje prijevara i neovlaštenih transakcija.
- **Sukladnost s propisima:** Osigurati da sustavi i procesi budu u skladu s važećim sigurnosnim standardima (PCI DSS) i zakonima (GDPR).

3. Opseg primjene

Ovaj dokument obuhvaća sve aspekte elektroničkog plaćanja putem web shopa, uključujući:

- Kreditne i debitne kartice
- Bankovne transfere
- Elektroničke novčanike i druge digitalne načine plaćanja (PayPal, Google Pay, Keks Pay, Paycek)

4. Odgovornosti

- **Vlasnik web shopa:** Ukupna odgovornost za sigurnost sustava i usklađenost s propisima.
- **IT tim:** Implementacija, održavanje i nadzor tehničkih sigurnosnih mjera.
- **Sigurnosni tim:** Redovita procjena rizika, provođenje sigurnosnih audita i revizija.
- **Korisnici:** Poštivanje sigurnosnih uputa (čuvanje lozinki, ažuriranje podataka).

5. Tehničke mjere

- **Enkripcija:** Svi podaci koji se prenose između korisnikovog preglednika i poslužitelja moraju biti zaštićeni SSL/TLS enkripcijom.
- **PCI DSS sukladnost:** Sustav za obradu plaćanja mora biti usklađen s PCI DSS standardima.

- **Firewall i IDS/IPS:** Implementacija firewall sustava i sustava za otkrivanje i prevenciju upada.
- **Sigurno pohranjivanje podataka:** Osigurati enkripciju i zaštitu baze podataka koja sadrži osjetljive informacije.
- **Ažuriranja i zakrpe:** Redovito ažurirati softver, operativne sustave i sigurnosne zakrpe kako bi se smanjile ranjivosti.

6. Proceduralne mjere

- **Politika lozinki:** Definirati zahtjeve za kompleksnost i redovitu promjenu lozinki.
- **Dvofaktorska autentifikacija (2FA):** Omogućiti 2FA za pristup administrativnim i osjetljivim dijelovima sustava.
- **Kontrola pristupa:** Implementirati stroge mjere kontrole pristupa prema principu najmanjih privilegija.
- **Obuka zaposlenika:** Redovito provoditi edukacije i treninge zaposlenika o sigurnosnim praksama i prepoznavanju potencijalnih prijetnji.

7. Fizičke mjere

- **Sigurnost poslužitelja:** Osigurati fizičku zaštitu poslužitelja i data centara, uključujući kontrolirani pristup, video nadzor i alarmne sustave.
- **Ograničen pristup:** Pristup prostorijama s osjetljivom opremom smanjiti samo na ovlašteno osoblje.

8. Upravljanje rizicima

- **Procjena rizika:** Redovito provoditi procjene rizika kako bi se identificirale i mitigirale potencijalne prijetnje.
- **Plan za hitne slučajeve:** Razviti i dokumentirati planove oporavka u slučaju sigurnosnih incidenata.
- **Sigurnosni auditi:** Provoditi interne i eksterne sigurnosne audite kako bi se osigurala učinkovitost implementiranih mjera.

9. Sigurnost komunikacija

- **Sigurna komunikacija:** Svi komunikacijski kanali (HTTPS, VPN) moraju biti zaštićeni enkripcijom.
- **Autentifikacija poslužitelja:** Osigurati da svi poslužitelji koriste valjane certifikate i da su pravilno konfigurirani.
- **Sigurno slanje obavijesti:** Koristiti sigurne metode za slanje obavijesti o transakcijama

10. Praćenje i revizija

- **Sustav za bilježenje događaja:** Implementirati sustav za logiranje i nadzor svih pristupa i transakcija.
- **Redoviti pregledi:** Provoditi redovite preglede sigurnosnih logova i analiza kako bi se pravovremeno otkrile sumnjive aktivnosti.
- **Interni i eksterni auditi:** Organizirati periodične audite kako bi se osigurala usklađenost sa sigurnosnim politikama i standardima.

11. Ažuriranje i održavanje dokumenta

- **Periodična revizija:** Dokument se mora pregledavati i ažurirati najmanje jednom godišnje ili nakon značajnih promjena u sustavu.
- **Evidencija promjena:** Sve izmjene dokumenta moraju biti dokumentirane, s navođenjem datuma, opisom promjene i odgovornom osobom.

12. Kontakt informacije

- **IT sigurnosni tim:** [Infocom d.o.o. / Ulica Svetog Mihovila 39 / 40 000 Čakovec, HR / OIB: 69961324765 / Kontakt telefon: +385 98 545 989 / Zoran Martinjak, direktor]
- **Korisnička podrška:** Flowable d.o.o. / Trnsko 42a / 10 010 Zagreb, HR / OIB: 97742618910 / Kontakt telefon: +385 1 2014 062 / Borna Koružnjak, direktor; Kristijan Berić, prokurist

13. Izjava o sukladnosti

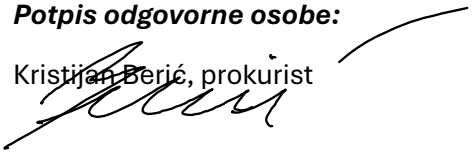
Ovaj dokument je izrađen u skladu sa svim relevantnim sigurnosnim standardima i zakonodavnim zahtjevima (PCI DSS, GDPR). Svi zaposlenici i suradnici obavezni su se pridržavati navedenih mjera i procedura.

14. Potvrda i prihvaćanje

Ovim potvrđujem da sam upoznat/a i prihvaćam sve mjere i procedure navedene u dokumentu.

Potpis odgovorne osobe:

Kristijan Berić, prokurist



Datum: 07. Veljače 2025.