1. Saugumo antraštės (Security Headers)

Reikia užtikrinti nemažesni nei **A** lygį pagal saugumą SecurityHeaders.com, rekomenduojama konfigūruoti šias antraštes:

- **Content-Security-Policy (CSP)** – riboti resursus tik patvirtintiems šaltiniams.
- **X-Frame-Options** – SAMEORIGIN arba DENY (apsauga nuo clickjacking atakų).
- **X-Content-Type-Options** – nosniff (užkerta kelią MIME sniffing atakoms).
- **Strict-Transport-Security (HSTS)** – priversti naudoti tik HTTPS.
- **Referrer-Policy** – no-referrer-when-downgrade arba strict-origin-when-cross-origin.
- **Permissions-Policy** – valdyti prieigą prie kameros, mikrofono, GPS ir kt.

2. Apsauga nuo duomenų įvedimo atakų (Injection & Spam)

Jei svetainėje yra formos ar el. pašto paslaugos, reikia laikytis **OWASP** rekomendacijų:

- **SQL Injection prevencija:** Naudoti **paruoštas užklausas (prepared statements)** arba ORM (pvz., Eloquent, SQLAlchemy).
- **Cross-Site Scripting (XSS) prevencija:** Naudoti **HTMLEncode** funkcijas visiems įvesties laukams.
- **CSRF apsauga:** Naudoti **CSRF token'us** visoms formoms.
- **Rate Limiting & CAPTCHA:** Naudoti Google reCAPTCHA arba kitą metodą, riboti užklausų dažnumą.

3. Bendri serverio saugumo patarimai

Serveriai.lt sistemoje OS atnaujinimai vyksta automatiškai tačiau svarbu užtikrinti tiek teisiu tiek įkeliamų failų saugumą:

- Failų leidimų apribojimai – vengti 777 leidimų, svarbiems failams naudoti 640 arba 600.
- Atsarginės kopijos – nustatyti automatinius backup'us.
- DDoS apsauga – naudoti Cloudflare arba kitą WAF (Web Application Firewall) (Naudojant VMSA domeną ar subdomeną bus užtikrinta).
- Failų įkėlimų apribojimai – leisti tik tam tikrus formatus (pvz., .jpg, .png, .pdf) ir tikrinti MIME tipą.
- Blokuoti neleistinus IP – jei įmanoma, riboti admin panele prieigą pagal IP adresus.

4. Wordpress saugumo patarimai

- **Naudoti „Limit Login Attempts“** – riboti prisijungimų skaičių.
- **Admin paskyroms turi būti įjungtas 2FA (dviejų faktorių autentifikavimas)**.
- **Visi naudojami plėtiniai turi būti iš patikimų šaltinių ir laiku atnaujinami**.
- **Slėpti WordPress versiją** – kad būtų sunkiau nustatyti galimas saugumo spragas.

5. Kodo versijavimas per Git

- Slaptų duomenų neįtraukimas į repozitorijų istoriją
- Saugaus prisijungimo prie nuotolinio serverio užtikrinimas, Naudoti saugius protokolus, tokius kaip SSH, prisijungdami prie nuotolinio Git serverio
- **Prieigos kontrolės ir teisių valdymas:** Įsitikinti, kad prieiga prie Git repozitorijų ir serverio yra apribota
- **Kodo peržiūra ir statinė analizė prieš diegiant,** prieš keliant kodą į gamybos serverį, atlikii kruopščią kodo peržiūrą (code review)

6. Naudoti PAM (Privileged Access Management) privilegijuotų prisijungimų įrankį.

- **Centralizuotas valdymas ir auditas:** Visus privilegijuotus prisijungimus rekomenduoajma fiksuoti per centrinę PAM sistemą. (prisijungimo laikas, trukme, pagal poreiki atllikti veiksmai).
- **Mažiausios privilegijos principo taikymas:** Suteikite vartotojams tik tas būtinas privilegijas, kurių reikia konkrečioms užduotims atlikti.
- **Slaptažodžių valdymas ir saugus saugojimas:** PAM sistemoje saugiai saugoti visų privilegiuotų paskyrų slaptažodžius. Vartotojai neturėtų tiesiogiai žinoti ar valdyti šių slaptažodžių.

7. Užduočių užsakymo ir vykdymo procesas:

- Visi su užsakymais ir jų valdymu susiję procesai turi būti vykdomi ir dokumentuojami Kliento užduočių valdymo sistemoje (toliau – UVS), pvz. darbų sąrašas (angl. Backlog), vartotojo istorijos (angl. User Story), užsakymai – užduotys (angl. Tasks), laiko planavimas kt. Kitais klausimais ar tikslinant informaciją privalomas bendravimo kanalas yra MS „Teams“. Neskubiais klausimais galima bendrauti ir kitais, su Klientu suderintais, kanalais, pvz. el. paštu.

- **Užduoties pateikimas.** Atsiradus paslaugų užsakymo poreikiui, Klientas pateikia užsakymą (toliau – Užduotis) UVS sistemoje. Klientas užduotyje nurodo savo poreikius, reikalavimus ir kitą informaciją reikalingą paslaugų vykdymui. Atlikus šiuos veiksmus, Klientas pakeičia užduoties būseną į „Priskirtas“ ir paskiria užduotį reikiamam Paslaugų teikėjo specialistui.
- **Užduoties peržiūra (Paslaugų teikėjo).** Paslaugų teikėjas detaliai išnagrinėja ir įvertina gautą užduotį:

  a) **Jei turima klausimų –** Jei Paslaugų teikėjui kyla neaiškumų, kuriuos reikia įvertinti prieš įvertinant ir pradedant vykdyti užduotį, Paslaugų teikėjas nurodo savo klausimus užduotyje ir ją grąžina Klientui. Užduotis grąžinama pakeičiant jos būseną į „Priskirtas“ arba „Trūksta informacijos“ bei paskiriant užduotį ją pateikusiam Kliento specialistui. Esant poreikiui, organizuojamas susitikimas klausimams aptarti.

  b) **Jei užduotis aiški –** Paslaugų teikėjas nurodo planuojamas darbų apimtis ir jas suderinęs su Klientu (Klientui patvirtinus) pradeda vykdyti užduotį. Pradėjus vykdyti užsakymą užduoties būsena pakeičiama į „Vykdoma“. Paslaugų teikėjas įsipareigoja pradėti vykdyti užsakymą ne vėliau nei kitą darbo dieną nuo Kliento patvirtinimo, kad užduoties realizavimo sprendimas ir valandų trukmė tinkama.

- **Užduoties vykdymas.** Užduoties vykdymo metu esminiai užsakymo klausimai ar pakeitimai fiksuojami UVS sistemoje. Bendraujant tarpusavyje ir perduodant užduotį su klausimais, patikslinimais, pakeičiama užduoties būsena ir paskirtas specialistas. Galimos užduoties būsenos: Naujas, Priskirtas, Trūksta informacijos, Grąžinta vykdymui, Vykdoma, Testuojama, Įvykdyta.

- **Užduočių vykdymui keliami šie papildomi reikalavimai:**
  - Visi programinio kodo pakeitimai turi būti atliekami iš UVS registruotų užduočių.
  - Užduotys vykdomos pagal eilę, kaip surikiuota UVS.
  - Pradėjus vykdyti užduotį, UVS užduoties statusas pakeičiamas į „Vykdoma“, o ją pabaigus – į „Įvykdyta“.
  - Užduotis turi būti suskaidyta į sub-užduotis, jei jos planuojamas atlikimo laikas (estimate) > 8 val.
  - Sub-užduotis pagrindinei užduočiai atlikti kuria pats programuotojas, o jas atlikus statusas keičiamas į „Uždaryta“.
  - Prie užduoties turi būti fiksuojamas praleistas laikas.

- Darbo dienos pabaigoje visi atlikti pakeitimai darbinėje aplinkoje turi būti įkeliami į GIT plaformą.

- **Užduoties užbaigimas.** Galutinai atlikus užduotį, Paslaugų teikėjas pakeičia užduoties būseną į „Įvykdyta“ ir paskiria ją Kliento specialistui.

8. Programinio kodo atnaujinimo procesas

- Pradėjus vykdyti užduotį Darbinėje programuotojo aplinkoje turi būti sukuriama šaka (angl. branch) su užduoties numeriu (pvz. feature-56213) nuo pagrindinės MAIN šakos.
- Atlikus programinio kodo pakeitimus, užduoties šaka įkeliama į atitinkamą Gitlab projektą. Pakeitimų žinutė (angl. commit message) turi būti suformuota anglų kalba ir aiškiai nusakanti kokie pakeitimai buvo atlikti (pvz.: #56213. Added birthday column to user table).
- Sukuriamas naujas užduoties šakos suliejimo prašymas (angl. merge request/pull request) su TEST šaka.
- Į TEST šaką programinis kodas gali būti suliejamas tik tada, kai yra pilnai sukurtas funkcionalumas (angl. feature).
- Suliejimo prašymas turi būti peržiūrimas kitų programuotojų (angl. code review).
- Nesant pastabų arba atlikus reikiamus pataisymus, programinis kodas suliejamas su TEST šaka.
- Gitlab CI/CD įrankis atnaujina TEST aplinką.
- Ištestavus IS, veikiančios TEST šakoje, funkcionalumus, kuriems turėjo įtakos programinio kodo pakeitimai, užduoties šaka suliejama su MAIN šaka.
- Gitlab CI/CD įrankis atnaujina produkcinę aplinką.