**ТЕХНИЧЕСКА СПЕЦИФИКАЦИЯ**

**„Услуга по тестване на софтуер, сигурност на информацията и натоварване на системата“:**

***Изисквания към изпълнението на предмета:***

Предмета на процедурата включва извършване на услуга по тестване на софтуер, сигурност на информацията и натоварване на системата.

***Минимални изисквания:***

**1) Функционално тестване спрямо техническата спецификация**

Да се потвърди, че всички функционалности, описани в техническата спецификация, са налични и работят коректно, стабилно и предвидимо при реални сценарии на употреба.

**Обхват**

* Всички модули/екрани/работни потоци, дефинирани в спецификацията
* Потребителски роли и права за достъп
* CRUD операции (създаване, редакция, изтриване, търсене, филтрация)
* Валидации на входни данни и обработка на грешки
* Известия/имейли, експорти/импорти
* Административни функционалности
* UI поведение (навигация, форми, съобщения, състояния)

**Минимални изисквания**

* **Покритие:** 100% от изискванията в техническата спецификация да са покрити от тестове
* **Критични потоци:** 100% успешни за поне следните типове сценарии:
  + Регистрация/достъп/вход/изход
  + основни операции по създаване и управление на данни
  + права на достъп според роли
* **Негативни тестове:** за всяка форма/ендпойнт да се покрият:
  + празни/липсващи полета
  + невалидни формати (email, дата, число, дължина)
  + гранични стойности (min/max)
  + неочаквани символи и дълги входове
* **Браузърна съвместимост (минимум):**
  + Chrome, Firefox

**Критерии за приемане**

* Няма блокиращи или критични дефекти по функционалностите от спецификацията

**2) Тестове за информационна сигурност**

Да се открият и минимизират уязвимости в уеб приложението чрез комбинация от ръчни проверки и автоматизирани инструменти, в съответствие с добри практики (OWASP).

**Автоматизирано сканиране – изисквания**

Скенерите следва да покрият минимум:

* OWASP Top 10 категории (напр. XSS, SQL Injection, Broken Access Control)
* Проверка на HTTP security headers (CSP, HSTS, X-Frame-Options и др.)
* Откриване на изтичане на информация (stack traces, версии, debug данни)
* Basic проверки за SSL/TLS конфигурация

**Артефакти:**

* Доклад от скенера със severity, доказателства (URLs, payload) и препоръки.

**Ръчни тестове – минимални сценарии**

* **Authentication / Authorization**
  + директен достъп до защитени ресурси без логин
  + опит за достъп до чужди ресурси (IDOR)
  + проверка за role escalation
* **Session management**
  + изтичане на сесии, logout invalidation
  + cookie flags: HttpOnly / Secure / SameSite
* **Input validation & Injection**
  + XSS (reflected/stored), SQLi, command injection (ако е приложимо)

**Критерии за приемане**

* 0 критични уязвимости
* Приложението не допуска неоторизиран достъп до данни/функции

**3) Анализ и ревюта на имплементацията за откриване на уязвимости**

Да се оцени сигурността на имплементацията и архитектурата чрез:

* статичен анализ
* ревю на ключови компоненти

**Минимални изисквания за анализ**

* Статичен анализ върху backend и frontend код (където е приложимо)
* Проверка за:
  + hardcoded secrets / ключове / токени
  + небезопасни конфигурации (debug mode, unsafe CORS, permissive policies)
  + непроверени входни данни и директни заявки към база
  + липса на централизирана обработка на грешки

**Ревю на критични части (минимум)**

* вход/регистрация/възстановяване на парола
* управление на роли/права
* операции върху чувствителни данни
* механизми за качване/сваляне на файлове (ако има)
* административни функции

**Критерии за приемане**

* Няма открити критични пропуски в сигурността на логиката

**4) Тестове под натоварване и определяне на лимити и хостинг нужди**

Да се установят:

* максимален устойчив брой едновременни потребители
* поведение при пик и деградация
* необходимите ресурси (CPU/RAM/DB/scale)
* стабилност при продължително натоварване

**Минимални изисквания (метрики и сценарии)**

* вход в системата
* основни ключови действия (най-често използваните)
* търсене/филтриране
* създаване/редакция на запис
* качване/генериране на документи

**Хостинг изводи и препоръки**

В резултат да се предостави:

* препоръчителна конфигурация (CPU/RAM) за приложението
* препоръки за база данни (ресурси, индексирование, connection pool)
* нужда от кеширане/CDN
* препоръка за скалиране (вертикално и хоризонтално)