الهيئة الوطنية لخدمات تقانة المعلومات
National Authority for IT Services

الإصدار الثالث
التصنيف :عام

دليل الإجراءات الاسترشادية
لتطوير مواقع ومنصات الويب الحكومية

الهيئة الوطنية لخدمات تقانة المعلومات

National Authority for IT Services

دليل الإجراءات الاسترشادية لتطوير مواقع ومنصات الويب الحكومية

إعداد:

- الهيئة الوطنية لخدمات تقانة المعلومات
- فريق الأمن السيبراني الاستشاري

جدول المحتويات

ا- مقدمة

ا-ا- المرجع

في إطار ممارسة الصلاحيات والواجبات الممنوحة للهيئة الوطنية لخدمات تقانة المعلومات بموجب القانون رقم /7/ لعام 2023، تصدر الهيئة المعايير والأدلة الاسترشادية التالية لبناء المواقع الإلكترونية الحكومية.

ا-2- نطاق التطبيق

الهدف من هذه الوثيقة هو توفير المعايير والأدلة الاسترشادية لتطوير وإدارة المواقع الإلكترونية الحكومية وبالتالي تحسين الجودة والموثوقية والدقة وإمكانية الوصول إلى معلومات الجهات الحكومية والتفاعل معها عبر شبكة الإنترنت وضمان تجربة متسقة لجميع المستخدمين.

وتشمل أهداف الوثيقة ما يلي:

1. ضمان امن مواقع الجهات الحكومية، وحماية البيانات الموجودة على الموقع، وبيانات المواطنين.
2. ضمان تحديث مواقع الجهات الحكومية والحفاظ على محتواها دقيق وصحيح وأن تكون متاح للاستخدام العام بشكل مستمر.
3. التأكد من أن المواقع الحكومية قابلة للاستخدام ويسهل الوصول إليها من قبل المواطنين.
4. لضمان الاتساق في التصميم وتسمية أسماء النطاقات لجميع مواقع الجهات الحكومية.
5. لتوجيه ومساعدة العاملين في مجال تقانة المعلومات في تصميم وتطوير وإدارة وتأمين المواقع الإلكترونية الخاصة بجهاتهم.
6. لتمكين مستخدمي المواقع الحكومية من الوصول إلى معلومات موثوقة بطريقة تتفق مع أفضل الممارسات العالمية.

ا-3- مبادئ

يجب على جميع الجهات الحكومية مراعاة احتياجات مجموعة واسعة من الزوار، بما في ذلك عامة الناس والمتخصصين والأشخاص ذوي الهمم، وأولئك الذين ليس لديهم إمكانية الوصول إلى التقنيات المتقدمة، وذوي الكفاءة المحدودة في اللغة الإنجليزية ومهارات تكنولوجيا المعلومات والاتصالات.

ا-4- تعاريف ومصطلحات

الهيئة: في سياق هذه الوثيقة، يقصد بها الهيئة الوطنية لخدمات تقانة المعلومات التابعة لوزارة الاتصالات والتقانة.

المعرفات البصرية (Visual Identification): هي مجموعة من العناصر التصميمية التي تُستخدم لتعريف وتمييز هوية كيانٍ أو جهة معينة، وتشمل، على سبيل المثال لا الحصر: الشعار الرسمي، لوحة الألوان المعتمدة (النظام اللوني)، الأيقونات، الخطوط الطباعية والمستخدمة، وأنماط التصميم البصرية. تهدف هذه العناصر إلى خلق صورة ذهنية متسقة وسهلة التعرّف عليها لدى الجمهور، وتعزيز التميّز والاحترافية في التواصل البصري، بالإضافة إلى تمييز الجهة عن غيرها والتعريف بها بسرعة.

الموقع الإلكتروني (Website): هو منصة رقمية تتكوّن من مجموعة من صفحات الويب المترابطة، متاحة للزوار عبر شبكة الإنترنت وتعمل تحت اسم نطاق موحّد. يُستخدم الموقع الإلكتروني كوسيلة تعريف رسمية للجهة على الإنترنت، ويُركّز على تقديم محتوى إعلامي مثل عرض الأخبار والمستجدات، نبذة عن الجهة وآلية عملها، الأدلة الخاصة بها (سواء كانت تجارية، خدمية أو صناعية)، وطرق الاستفادة من خدماتها، بالإضافة إلى معلومات الاتصال وقنوات التواصل الرسمية.

الموقع الإلكتروني الحكومي (Government Website): هو منصة رقمية أو موقع إلكتروني يتبع لجهة عامة، تتولى هذه الجهة مسؤولية إدارته وتحديث محتواه وتحديد أهدافه. يُصمَّم الموقع وفق هوية بصرية تعبّر عن طبيعة عمل الجهة وتُبرز تميّزها عن غيرها، ويُستخدم كواجهة رسمية لعرض المعلومات، الأخبار، والخدمات ذات الصلة بنطاق اختصاصها.

المنصة الرقمية (Digital Platform): هي بيئة تقنية متكاملة تتكوّن من مجموعة من الحلول والأنظمة التي تُبنى عليها الخدمات الرقمية، ويتم من خلالها تقديم هذه الخدمات للمستفيدين عبر قنوات رقمية متنوعة، مثل تطبيقات الويب، تطبيقات الهاتف المحمول، والبوابات الإلكترونية. تمتاز المنصة الرقمية بقدرتها على التكامل والتواصل مع أنظمة وخدمات خارجية، وتتيح التفاعل مع العديد من الجهات والأشخاص.

عرض الحزمة (Bandwidth): هو الحد الأقصى لمعدل نقل البيانات عبر شبكة أو اتصال إنترنت، ويُقاس عادةً بمقدار البيانات التي يمكن نقلها خلال فترة زمنية محددة، غالبًا في الثانية الواحدة.

المتصفح (Web Browser): و تطبيق برمجي (أداة) يتيح للمستخدمين تصفح الإنترنت من خلال عرض صفحات الويب والتفاعل معها، والوصول إلى المحتوى المتاح عبر الشبكة العالمية، مثل النصوص والصور والفيديو والخدمات الإلكترونية. من أشهر متصفحات الإنترنت: Google Chrome، Mozilla Firefox ، و Microsoft Edge.

اسم النطاق (Domain Name): هو العنوان الفريد الذي يُستخدم للوصول إلى الموقع الإلكتروني على شبكة الإنترنت، ويكتبه المستخدمون عادة في شريط العنوان داخل المتصفح (مثل: www.example.com). يُعد اسم النطاق جزءًا أساسيًا من هوية الموقع الرقمية، ويتميّز بأنه غير قابل للتكرار أو المشاركة بين مواقع مختلفة، مما يضمن تميّز كل موقع عن غيره على الإنترنت.

تحميل الملفات (File Download): هو عملية نقل البيانات من خادم (Server) على الشبكة أو الإنترنت إلى جهاز المستخدم، حيث يتم تخزين هذه البيانات على القرص الصلب أو أي وسيلة تخزين محلية أخرى. تتيح هذه العملية للمستخدم الوصول إلى الملفات والمحتوى الرقمي واستخدامها دون الحاجة إلى اتصال دائم بالإنترنت.

نماذج العمل (Forms): في سياق هذه الوثيقة، تشير نماذج العمل إلى النماذج الإلكترونية التي يتم توفيرها عبر المنصات الرقمية، والتي يمكن للمستخدمين ملؤها لأغراض متنوعة مثل تسجيل البيانات، تقديم الملاحظات، التسجيل في الخدمات، أو طلب معلومات محددة. وتُعد هذه النماذج وسيلة فعّالة لتسهيل التفاعل بين الجهة والمستفيدين بطريقة منظمة وسهلة الاستخدام.

الصفحة الرئيسية (Homepage): هي الواجهة الأساسية للموقع الإلكتروني وتُعد أول صفحة تظهر عند زيارة الموقع. تحتوي عادةً على نظرة عامة عن محتوى الموقع وروابط توجّه الزوار إلى الصفحات الداخلية الأخرى، مثل الأخبار، الخدمات، أو معلومات الاتصال. وتُشكّل الصفحة الرئيسية نقطة الدخول الأساسية التي تعكس هوية الموقع وتنظّم تجربة التصفّح للمستخدمين.

مزود خدمة الاستضافة (Web Hosting Provider): هو جهة متخصصة توفّر البنية التحتية والتقنيات اللازمة لاستضافة المواقع الإلكترونية، وتشمل هذه البنية الخوادم، وأنظمة التشغيل، ووحدات التخزين،

وشبكات الاتصال، بالإضافة إلى تجهيزات وأنظمة الحماية. يتولى مزود الخدمة إدارة هذه الموارد وتشغيلها لضمان عمل المواقع بكفاءة وأمان، وتمكين الوصول إليها عبر شبكة الإنترنت على مدار الساعة.

ملف السجل (Log File): هو ملف يُستخدم لتسجيل وتوثيق الأنشطة والأحداث التي تحدث ضمن موقع الويب أو على الخادم (Server). يتضمن هذا الملف معلومات مثل أوقات الدخول، عناوين IP، الصفحات التي تم الوصول إليها، الأخطاء، والعمليات التي تتم على النظام أو الموقع. تُعد ملفات السجل أداة مهمة في مراقبة الأداء، وتحليل الاستخدام، واكتشاف المشكلات الأمنية والفنية، كما تساعد في تتبع سلوك المستخدمين وتحسين كفاءة وموثوقية الأنظمة.

الخدمات عبر الإنترنت (Online Services): هي خدمات رقمية يتم الوصول إليها وتقديمها للمستخدمين من خلال شبكة الإنترنت، وتشمل مجموعة واسعة من الوظائف مثل التقديم على الطلبات، الدفع الإلكتروني، الوصول إلى المعلومات، التواصل، أو استخدام تطبيقات الويب وتطبيقات الهاتف المحمول المختلفة. تتيح هذه الخدمات التفاعل السريع والفعّال دون الحاجة إلى الحضور الفعلي أو التعاملات الورقية.

المستخدمون/الزوار: في سياق هذه الوثيقة، يُقصد بهم جميع الأفراد الذين يزورون مواقع الويب أو يتفاعلون مع الخدمات المقدّمة عبر الإنترنت، سواء بهدف الاستفادة من المحتوى، أو استخدام النماذج، أو الحصول على خدمات رقمية، أو الاطلاع على المعلومات المتاحة.

محدد موقع المعلومات(URL – Uniform Resource Locator) : هو العنوان الفريد الذي يُستخدم لتحديد موقع أي مورد على شبكة الويب العالمية، مثل صفحة ويب أو ملف أو صورة أو خدمة إلكترونية. يُكتب بصيغة قياسية تتيح للمتصفحات الوصول إلى هذا المورد من خلال بروتوكولات محددة مثل HTTP أو HTTPS.

روبوتات مسح المواقع (Crawlers): هي برامج أو أدوات برمجية تعمل بشكل آلي على تصفّح مواقع الويب واكتشاف محتواها، بما في ذلك الصفحات، الروابط، المجلدات، والملفات، بهدف جمع المعلومات وفهرستها تلقائيًا عبر الإنترنت. تُستخدم هذه الروبوتات بشكل رئيسي من قِبل محركات البحث مثل Google وBing لتحليل المواقع وإدراجها ضمن نتائج البحث، مما يسهّل على المستخدمين العثور على المحتوى

المطلوب. كما يمكن التحكم في وصول هذه الروبوتات إلى أجزاء معينة من الموقع باستخدام ملف robots.txt الذي يحدد قواعد السماح أو المنع لكل روبوت زاحف.

تحسين نتائج الظهور على محرك البحث (SEO – Search Engine Optimization): هو عملية تحسين محتوى وبنية موقع الويب بهدف زيادة فرص ظهوره في نتائج البحث (بشكل طبيعي وبدون اعلانات) على محركات البحث مثل Google و Bing. تشمل هذه العملية مجموعة من التقنيات والممارسات التي تهدف إلى رفع ترتيب الموقع، جذب المزيد من الزوار، وتحسين تجربة المستخدم بما يتوافق مع معايير وأسس محركات البحث.

2- أمان الموقع والخصوصية

2-1- معلومات عامة

يجب على الجهات الحكومية اتخاذ تدابير وضوابط تضمن سرية وسلامة وتوافر مواردها على الإنترنت.

2-2- أدلة استرشادية لأمن الموقع وسياسة الخصوصية

يجب الامتثال لجميع المعايير والقوانين والضوابط الناظمة لحماية المواقع الحكومية وضمان الخصوصية الشخصية على الإنترنت، ومن أبرزها:

- السياسة الوطنية لأمن المعلومات واللوائح التنظيمية المرتبطة بها.
- قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية.
- قانون حماية البيانات الشخصية.
- قانون المعاملات الإلكترونية.

ولتعزيز أمن الموقع، يجب أيضًا اتباع أفضل الممارسات التقنية، وأهمها:

1. التأكد من تحديث نظام التشغيل، ومخدمات الويب وقواعد البيانات، ونظام إدارة المحتوى بشكل مستمر.
2. منع الاتصال المباشر بقاعدة البيانات عبر الإنترنت، واقتصار الوصول عليها من خلال العنوان الداخلي للخادم فقط.
3. استخدام قواعد صلاحيات (Privileges) لحسابات قواعد البيانات، بحيث يُمنح كل حساب أقل قدر من الصلاحيات اللازمة لأداء مهامه. ولا يتم استخدام نفس الحساب على أكثر من قاعدة بيانات.

4. متابعة الثغرات الأمنية المعروفة للبرمجيات والأنظمة المستخدمة، وتحديثها بشكل فوري عند اكتشاف أي ثغرة حرجة.

5. فعّل المصادقة الثنائية (FA2) لجميع حسابات لوحة التحكم لرفع درجات الأمان وحماية الحسابات من محاولات الاختراق. واستخدم تطبيقات موثوقة أو عبر حسابات البريد الإلكتروني، حيث توفر هذه الأدوات طبقة حماية إضافية تتطلب إدخال رمز تحقق مؤقت عند كل تسجيل دخول، بالإضافة إلى كلمة المرور.

6. استخدام ترويسات بروتوكول Http المتعلقة بالحماية الأمنية (Security Headers):

a. يجب تطبيق سياسة أمان صارمة للمحتوى للحد من تنفيذ الأكواد الضارة وحماية الموقع من هجمات XSS وحقن الكود، يمكن استخدام ادوات عبر الانترنت مثل https://securityheaders.com لفحص الموقع

b. تفعيل (X-XSS-Protection) في الخادم لتفعيل آلية الحماية من هجمات XSS في المتصفحات الداعمة.

c. تفعيل (X-Frame-Options) لمنع تضمين الموقع ضمن إطارات (iframes) في مواقع أخرى، ما يحمي من هجمات النقر الخادع (Clickjacking).

7. حماية النماذج (Forms) من هجمات CSRF: يجب تفعيل رموز CSRF لجميع النماذج، وذلك بإضافة رموز تحقق فريدة، مع التحقق منها في الخادم قبل تنفيذ النموذج.

8. في حال كانت الطلبات تمر عبر تطبيقات الطرف الثالث باستخدام واجهة برمجية (API) مثل تطبيقات الجوال أو برمجيات الواجهات Front-end يجب إجراء ما يلي:

a. للبيانات العامة وضع رمز سماح بالوصول auth-code ثابت يتم تغييره عند كل تحديث برمجي في الترويسة للتحقق من أن هذا الطلب يأتي من برمجية مخول لها طلب البيانات ولا تخدم هذه البرمجية الطلب من برمجية غير مخولة.

b. للبيانات الخاصة التي يتم تسجيل الدخول من خلالها يجب استخدام أليات تحقق من الدخول مثل (basic auth, bearer, JWT) ترسل مع كل طلب.

c. في بعض البيئات يتوجب إضافة طبقة حماية أخرى بالسماح لعناوين محددة لطلب الواجهة البرمجية ضمن سياسة CORS.

2-3-البيانات المنقولة:

1. يجب تثبيت شهادة اتصال آمن وموثوق (TLS) لضمان تشفير البيانات المتبادلة مع المستخدمين، مع التأكد من استخدام شهادة اتصال تحتوي سلسلة الشهادات الكاملة (Full Certificate Chain) لتفادي ظهور تحذيرات في المتصفحات.
2. يُشترط استخدام بروتوكول TLS V 1.2 أو أعلى، بما يتوافق مع السياسة الوطنية للتشفير، حيث توفر هذه البروتوكولات تشفيرًا قويًا وتدعم خوارزميات حديثة مثل ECDSA و SHA-256.
3. يجب الاقتصار على استخدام البروتوكولات المشفرة في جميع الاتصالات، مثل: HTTPS للاتصال الآمن عبر الويب و SFTP لنقل الملفات بشكل آمن.

2-4- البيانات المخزنة

2-4-1- أمن قواعد البيانات:

1. يجب عند الحاجة إلى حفظ كلمات مرور المستخدمين أو أي بيانات حساسة في قاعدة البيانات، استخدام خوارزمية تجزئة مخصصة لكلمات المرور مثل Argon2 أو bcrypt أو scrypt، مع تطبيق Salt، يجب ألا تتجاوز عدد محاولات تسجيل الدخول ال5 مرات خلال 5 دقائق بما يقلل فرص نجاح هجمات التخمين أو القوة الغاشمة. ويُمنع تماماً تخزين كلمات المرور كنص عادي أو باستخدام خوارزميات تجزئة سريعة غير مخصصة لهذا الغرض مثل md5 فقط.
2. يجب فصل قواعد البيانات عن خادم الويب، خاصة بالنسبة للمنصات أو التطبيقات التي تقدم خدمات حساسة أو ذات طلب مرتفع، وذلك للحد من مخاطر الاختراق.
3. يُمنع الوصول إلى قواعد البيانات من خلال تطبيقات أو برمجيات الطرف الثالث (مثل phpMyAdmin) بشكل مباشر عبر الإنترنت، ويجب الاعتماد على طرق اتصال آمنة (مثلا: الاتصال عبر لوحة التحكم في الاستضافات المشتركة، أو أن يتم الاتصال بالمخدم عبر SSH ومن ثم يتم الاتصال بقاعدة البيانات من داخل المخدم، يمكن استخدام خاصية tunnel في برمجية Putty لتنفيذ هذه التوصية. كما يمكن استخدام العديد من برمجيات إدارة قواعد البيانات التي تدعم مثل هذه الخاصية).
4. يجب حماية ملف الربط مع قاعدة البيانات (الذي يحتوي على إعدادات وحسابات الدخول) بحيث لا يُمنح صلاحية القراءة أو التحميل أو الكتابة سوى للمستخدم المخول.
5. يجب أن يكون حساب قاعدة البيانات المستخدم في ملف الربط مخصصاً لهذا الغرض فقط، وألا يُستخدم لأي غرض آخر من قبل أشخاص أو برامج أو أدوات أخرى.

6. يُمنع تخزين الملفات الكبيرة أو المرفقات ضمن قاعدة البيانات نفسها؛ بل يجب استخدام مسار آمن مخصص لتخزين هذه الملفات مع ضبط الصلاحيات حسب الحاجة.
7. يُمنع استخدام الحسابات الافتراضية وكلمات المرور الافتراضية لقواعد البيانات، ويجب دائماً تعيين كلمات مرور قوية وفريدة.
8. يجب تشغيل خاصية تتبع الأحداث والسجلات (Logging/Auditing) إن أمكن، لمراقبة الأنشطة وتسجيلها.
9. يجب عدم الثقة بأي مدخل من المستخدم (User Input)، مع ضرورة تنظيف البيانات والتحقق منها قبل عرضها أو استخدامها، ويفضل الاعتماد على مكتبات تحقق (Validation Libraries) معروفة وموثوقة.
10. يُنصح باستخدام أنظمة كشف التسلل (IDS) مثل Snort أو Suricata، أو جدران حماية التطبيقات (WAF) مثل ModSecurity، بالإضافة إلى تقنيات Honeypots لتسجيل محاولات الاستغلال ومراقبة السلوكيات المشبوهة.
11. يمنع حفظ ملفات قواعد البيانات او النسخ الاحتياطية ضمن مسارات يمكن الوصول لها عبر طلب رابط مباشر (URL).

2-4-2- النسخ الاحتياطي:

يجب أخذ نسخ احتياطية بشكل دوري لجميع المحتويات المستضافة، بما في ذلك قواعد البيانات وملفات ومجلدات الويب، لضمان استمرارية الأعمال في حالة الفشل أو الكوارث.

1. على الجهات الحكومية تطوير خطة شاملة لضمان استمرارية الأعمال والتعافي من الكوارث، تتضمن تحديد البيانات الحيوية، وتوثيق إجراءات النسخ والاسترجاع، وتحديد المسؤوليات بوضوح.
2. يجب التأكد من سلامة النسخ الاحتياطية وقابليتها للاسترجاع من خلال إجراء اختبارات دورية، مثل اختبار الاسترجاع الفعلي، ومقارنة البيانات المسترجعة بالأصلية للتأكد من عدم وجود تلف أو فقدان.
3. يُوصى بتطبيق قاعدة "3-2-1" للنسخ الاحتياطي: الاحتفاظ بثلاث نسخ من البيانات، على نوعين مختلفين من الوسائط (نسخة على HDD ونسخة على المخدم نفسه)، مع نسخة واحدة على الأقل خارج الموقع، يجب أن يتم منع الوصول (Public Access) لجميع اماكن تخزين النسخ الاحتياطية، وأن تكون جميع النسخ الاحتياطية مشفرة. يفضل أن تكون نسخة غير قابلة للتعديل (immutable) أو مفصولة عن الشبكة.

a. يمكن ايضاً تطبيق قاعدة "3-2-1-1-0" وتعني – بالإضافة إلى ما سبق- صفر أخطاء عند التحقق من النسخ الاحتياطية – أي أنها صالحة ويمكن استعادتها.

4. يجب تشفير النسخ الاحتياطية لحماية البيانات من الوصول غير المصرح به، مع الالتزام بمعايير التشفير الوطنية والدولية.

5. يجب إجراء اختبارات منتظمة لكفاءة نظام التعافي من الكوارث (Disaster Recovery)، بما يشمل محاكاة سيناريوهات مختلفة (مثل اختراق الموقع، فقدان البيانات، أو هجمات الفدية)، وتوثيق نتائج الاختبارات وتحديث الخطط بناءً عليها.

6. يجب مراقبة سجلات النسخ الاحتياطي والتأكد من نجاح العمليات، مع الاحتفاظ بسجلات مفصلة لعمليات النسخ والاسترجاع.

7. يوصى بأتمتة إنشاء نسخ احتياطية تزايدية يومية ونسخ كاملة أسبوعية للأنظمة والبيانات الحساسة، مع مراجعة دورية لسياسات النسخ الاحتياطي وتحديثها حسب الحاجة.

2-5- البيانات قيد الاستخدام:

1. يجب اتخاذ الإجراءات الفنية والإدارية المناسبة لمنع بقاء جلسات العمل (Sessions) مفتوحة لفترات طويلة بعد توقف المستخدم عن التفاعل معها. يمكن تحقيق ذلك من خلال الحرص على تسجيل الخروج عند الانتهاء من العمل، وضبط إعدادات الجلسات بحيث يتم إغلاقها تلقائيًا بعد فترة قصيرة من الدخول في وضع السكون (Idle).

2. ينبغي اتخاذ التدابير اللازمة لمنع ظهور او كشف شاشات الأجهزة المستخدمة في إدارة الموقع أو إدخال البيانات أو عرضها أمام أشخاص غير مخولين، أو حتى أمام كاميرات المراقبة أو النوافذ والأبواب، وذلك للحد من مخاطر هجمات الهندسة الاجتماعية.

2-6- أمن تطبيقات الويب:

1. يجب إدارة رسائل الخطأ (Debug) بحيث لا تظهر أي معلومات حساسة عن التطبيق أو بيئة التشغيل للمستخدم النهائي، مع تسجيل التفاصيل الفنية في سجلات داخلية للتحليل فقط.

2. يجب تفعيل المصادقة الثنائية (FA2) لجميع أدوار المشرفين، بحسب حساسية التطبيق أو الخدمة، واستخدام تطبيقات موثوقة مثل Google Authenticator أو YubiKey.

3. يجب اعتماد آليات حماية من هجمات تخمين كلمات المرور أو رموز المصادقة المؤقتة، مثل تعطيل الحساب مؤقتًا أو حظر محاولات الدخول من عنوان IP معين عند تكرار الفشل خلال فترة زمنية قصيرة.

4. عند وجود صفحات لإدخال البيانات من المستخدمين، يجب التأكد من صحة وصلاحية القيم المدخلة عبر التحقق على الطرفين: العميل (المستعرض) والخادم، مع اعتماد مكتبات تحقق معروفة وتنظيف البيانات قبل المعالجة أو العرض.
5. يجب استخدام الطلب بطريقة POST في عمليات إدخال البيانات للمستخدمين مثل التسجيل وتسجيل الدخول ورفع الملفات سواء عبر صفحات الويب أو الواجهات البرمجية (APIs)، وإبطال منهجيات مثل OPTIONS وTRACE وDELETE.
6. يجب تغيير الإعدادات والتكوينات الافتراضية، ومسميات ومسارات الملفات والمجلدات الافتراضية وعناوين صفحات الدخول والإدارة، وعدم استخدامها مطلقًا.
7. يجب تعطيل جميع المزايا غير المستخدمة في الموقع مثل التسجيل أو التعليقات، وتعطيل الخدمات والمكتبات البرمجية والخيارات غير الضرورية (مثل Directory Indexes) على الخادم للوقاية من ثغرة Directory Listing.
8. يجب فرض إعادة المصادقة عند التعامل مع الميزات الحساسة (مثل تغيير كلمة المرور أو إجراء عمليات دفع).
9. يجب استخدام أحدث إصدارات بيئات البرمجة ومكوناتها والمكتبات البرمجية (Backend-Frontend) بتاريخ التصميم، مع الحرص على تحديثها باستمرار.
10. يجب حماية ميزة رفع الملفات من خلال: فحص الملفات قبل رفعها، تدقيق الامتدادات، فلترة وتغيير أسماء الملفات، حفظها في مجلدات محمية خارج مجلد الجذر، ومنع الصلاحيات التنفيذية لها.
11. يجب التحقق من صلاحيات الملفات والمجلدات، ومنع منح صلاحيات كاملة لأي ملف أو مجلد، ومنع الوصول إلى الملفات المصدرية أو ملفات الإعدادات البرمجية من جهة المستخدم.
12. يجب عدم حفظ ملفات أو مجلدات الأرشفة أو النسخ الاحتياطية ضمن مجلد الجذر أو أي مجلد فرعي، بل حفظها خارج المسار التخزيني المخصص لتطبيق الويب ويفضل خارج الخادم.
13. يجب التأكد من حذف جميع الملفات أو الصفحات التجريبية وغير الضرورية من بيئة الإنتاج.
14. يجب تجنب عرض روابط أو مسارات ملفات أو مجلدات التطبيق للمستخدم النهائي في روابط التطبيق (URL)، خاصة مسارات رفع الملفات أو الأكواد البرمجية.
15. يجب تقييد الوصول لصفحات الدخول الإدارية من عناوين IP محددة، أو من خلال شبكة Zero Trust فقط مع ربطها بعناوين موثوقة داخل الشبكة.
16. يجب منع تنفيذ طلبات مسارات تتضمن الرموز (../) لتجنب هجمات Path Traversal.

17. يجب التأكد من عدم إمكانية تنفيذ أوامر نظام التشغيل عبر حقول الإدخال (للوقاية من هجمات Remote Command Execution).
18. يجب تقليل عدد المستخدمين ذوي الامتيازات إلى الحد الأدنى، وتطبيق مبدأ أقل صلاحية (Least Privilege).
19. يجب إدارة صلاحيات المستخدمين بحيث تُمنح الصلاحية حسب المهام فقط.
20. يجب التأكد من أن كل دور في نظام إدارة المحتوى (CMS) لا يملك صلاحيات أكثر من اللازم، خاصة حسابات "الناشرين" و"المديرين"، مع تفعيل سياسة Least Privilege.
21. يجب مراجعة الصلاحيات الممنوحة بشكل دوري (كل 6 أشهر على الأكثر)، وإلغاء الصلاحيات فور انتهاء المهمة.
22. يجب تطبيق سياسة صارمة في إنشاء وإدارة كلمات المرور، ومنع استخدام كلمات مرور ضعيفة أو متكررة.
23. يجب إجراء فحص دوري لملفات الموقع بحثًا عن البرمجيات الخبيثة باستخدام أدوات مخصصة للخوادم.
24. يجب تغيير كلمات مرور الحسابات الإدارية بشكل دوري (كل ثلاثة أشهر على الأقل)، وتعطيل أو حذف الحسابات غير المستخدمة خلال شهر من آخر استخدام.
25. يجب حماية ملفات البيئة البرمجية (env/config)، ومنع إتاحتها للتحميل أو العرض عبر المتصفح.
26. يجب تأمين واجهات البرمجة (APIs) باستخدام نظام مصادقة معتمد على الرموز (مثل JWT) مع تحديد صلاحية زمنية للرموز.
27. يجب تفعيل جدار حماية (Firewall/WAF) على جميع نقاط الوصول الحساسة مثل لوحات التحكم وقواعد البيانات.
28. يجب تغيير روابط الدخول الإدارية لتكون غير مألوفة وتجنب المسارات الشائعة مثل /admin أو /login.
29. يجب الحماية من الروبوتات عبر تفعيل CAPTCHA في أماكن تسجيل الدخول ورفع الملفات.
30. يجب مراقبة الثغرات الأمنية باستمرار وإجراء فحوصات دورية لأمن المعلومات وقابلية الاختراق.
31. يجب تفعيل قوائم الحظر الديناميكي والتلقائي (Auto-Ban) لعناوين IP المشبوهة بناءً على السلوك.
32. يجب إخفاء ملفات ومجلدات الموقع (Hardening Directory & File Access) ومنع الوصول غير المصرح به.

33. يجب فحص وتحليل User-Agent وتقييد الفحص من الخارج (Geo-IP Blocking/VPN Detection) عند الحاجة.

34. يجب تطبيق سياسة (CSP Content Security Policy) لمنع تحميل شيفرات برمجية من مصادر غير مصرح بها، وحماية من هجمات XSS.

35. يجب تفعيل ترويسات حماية HTTP Security Headers مثل:

- Content-Security-Policy (CSP)
- X-Frame-Options لمنع التضمين داخل إطارات (Clickjacking Protection)
- X-Content-Type-Options: nosniff
- Referrer-Policy لتقليل التسريب غير المقصود للمعلومات
- Strict-Transport-Security لإجبار استخدام HTTPS

2-7- إرشادات أمن خادم الويب والبيئة المحيطة

2-7-1- الاستضافة الآمنة:

1. يُمنع استضافة المواقع والتطبيقات الحكومية خارج أراضي الجمهورية العربية السورية، وذلك وفق بلاغ رئاسة مجلس الوزراء رقم 15/7944 تاريخ 2012/6/7، وبما يتوافق مع دليل الهيئة الوطنية لخدمات الشبكة. يجب أخذ موافقة من وزارة الاتصالات لاستضافة اي موقع او تطبيق حكومي على خادمات غير مملوكة من وزارة الإتصالات.

2. يجب على المؤسسات الحكومية تنفيذ اتفاقية مستوى الخدمة (SLA) واتفاقية عدم الإفشاء (NDA) مع مزود خدمة الاستضافة، لضمان السرية والنزاهة والتوافر لجميع تطبيقات الويب الحكومية المستضافة.

3. يجب اختيار خطة استضافة آمنة في بيئة معيارية تحقق متطلبات أمن المعلومات واستمرارية الخدمة، بما يشمل توفير حماية مادية ومنطقية للخوادم، وتطبيق أحدث معايير الحماية السيبرانية الوطنية.

4. ينبغي أن يوفر مزود خدمة الاستضافة آليات تسهّل اختبار موقع الويب الحكومي قبل الاستضافة الفعلية، بما في ذلك بيئة اختبار منفصلة وآمنة لفحص الأداء والأمان والتوافقية قبل الإطلاق.

5. على الجهات العامة التي تتطلب طبيعة عملها استضافة تطبيقاتها ومنصاتها الإلكترونية محليا أو ضمن مراكز معطياتها الخاصة، الالتزام التام بمتطلبات أمن المعلومات الخاصة بمراكز البيانات الصادرة عن الهيئة الوطنية لخدمات الشبكة، بما في ذلك ضوابط الحماية، النسخ الاحتياطي، واستمرارية الأعمال.

6. يُفضل أن تكون الاستضافة ضمن مراكز البيانات الحكومية المعتمدة، مثل مركز المعطيات الوطني أو مركز الحوسبة السحابية، لضمان أعلى درجات الحماية والإشراف الفني والقانوني.

2-7-2- إرشادات أمن الخادم المضيف:

1. تحديث نظام تشغيل البيئة المضيفة بشكل مستمر، بعد أن يتم التأكد من أن هذه التحديثات لن تؤثر على عمل الموقع أو التطبيق.
2. ينصح بالاعتماد على أحدث الإصدارات المستقرة من خوادم الويب.
3. يجب مراجعة حسابات المستخدمين وصلاحياتهم، خاصة تلك التي تم إنشاؤها أثناء تنصيب وإعداد نظام التشغيل، مع الإبقاء فقط على الحسابات الضرورية على النظام.
4. يجب إغلاق جميع المنافذ المفتوحة غير الضرورية لتشغيل التطبيق على الخادم، وتعطيل الخدمات والبروتوكولات المرتبطة بها، مثل SMB وNetBIOS، ما لم تكن هناك حاجة فعلية لاستخدامها.
5. يجب استخدام البروتوكولات المشفرة فقط عند الوصول إلى نظام التشغيل، مثل بروتوكول SSH، مع تجنب استخدام بروتوكول سطح المكتب البعيد (RDP) أو أدوات خارجية مثل AnyDesk، ويمكن الوصول عبر RDP في حال طلب ذلك عبر الاتصال المشفر الأمن باستخدام VPN
6. تضمين التدقيق وتسجيل الأحداث (Auditing & Logging) على الخادم، وحفظ السجلات لمدة لا تقل عن /6/ أشهر.
7. يجب ربط الخادم شبكياً ضمن شبكة آمنة معزولة عن أي شبكات أخرى.
8. يجب ضمان تطبيق الحماية الفيزيائية للخادمات وتقييد الوصول إليها من خلال سياسة تحكم بالدخول، بحيث يُسمح بالتواجد الفيزيائي بالقرب من هذه الخوادم للأشخاص المخولين فقط.
9. يجب على الجهات الحكومية إجراء اختبارات ضغط (Stress Test) دورية للتأكد من قدرة مواقعها على تحمل الزيادات المفاجئة في عدد المستخدمين أو الطلبات، مع توثيق النتائج ومعالجتها فنياً. كما يجب تطبيق أنظمة حماية متقدمة ضد هجمات حجب الخدمة الموزعة (DDoS)، ومراقبة حركة الشبكة بشكل مستمر، بالإضافة إلى إعداد خطط استجابة للطوارئ تتضمن التواصل مع مزود الخدمة وتفعيل الحلول التقنية اللازمة. يُوصى أيضًا بإجراء اختبارات محاكاة دورية لهجمات DDoS لضمان جهوزية الموقع وكفاءة أنظمة الحماية.

2-7-3- جدار حماية تطبيقات الويب (WAF)

1. يعمل WAF على مراقبة حركة المرور الواردة إلى التطبيقات وحجب الطلبات المشبوهة أو الضارة قبل وصولها إلى الخوادم، مما يوفّر طبقة دفاع متقدمة ضد هجمات OWASP Top 10، هجمات DDoS، ومحاولات استغلال الثغرات البرمجية.

2. يجب مراجعة إعدادات WAF وتحديث قواعده بشكل دوري، خاصة بعد أي تغيير في التطبيق، لضمان فعالية الحماية ومواكبة التهديدات الحديثة.

3. يوصى بتفعيل تسجيل الأحداث (Logging) على WAF، وتحليل السجلات باستمرار لرصد الأنشطة غير الاعتيادية والاستجابة السريعة للحوادث.

2-7-4- تفعيل التقييد الجغرافي (Geo-Restriction)

1. يتيح التقييد الجغرافي حصر الوصول إلى المواقع والخدمات الحكومية من مناطق جغرافية محددة فقط، وحجب الطلبات الواردة من مناطق عالية الخطورة أو غير مصرح بها.

2. يمكن تطبيق سياسات دقيقة بناءً على عناوين IP، رموز الدول، أو خصائص الشبكة، مع إمكانية استثناء عناوين أو نطاقات محددة عند الحاجة.

3. يساهم التقييد الجغرافي في تقليل مخاطر الهجمات العابرة للحدود، مثل هجمات DDoS أو محاولات الاختراق من جهات خارجية، ويلبي متطلبات السيادة الرقمية وحماية البيانات الوطنية.

4. يفضل تقييد الوصول إلى لوحات الإدارة والبوابات الحساسة جغرافيًا، بحيث لا يمكن الدخول إليها إلا من مواقع أو شبكات محددة داخل الدولة أو من خلال قنوات اتصال آمنة ومعتمدة.

2-8- متطلبات أخرى:

1. يجب على الجهات الحكومية إبلاغ الهيئة الوطنية لخدمات تقانة المعلومات (مركز أمن المعلومات) عن أي حدث طارئ أو اختراق أو هجوم سيبراني تتعرض له التطبيقات أو المنصات الإلكترونية خلال مدة لا تزيد عن ٧٢ ساعة من وقت اكتشاف الاختراق، وذلك عبر القنوات الرسمية مثل البريد الإلكتروني infosec@naits.gov.sy أو الفاكس أو الهاتف.

2. في حال التعرض للقرصنة أو الاختراق، يجب الاحتفاظ بنسخة احتياطية من الموقع المخترق كدليل رقمي قبل استعادة نسخة احتياطية سليمة من الموقع، لضمان توثيق الأدلة الرقمية وتحليل أسباب الحادث.

3. يجب رصد موازنات سنوية مخصصة لتطوير التطبيق، الموقع أو المنصة بهدف إصلاح الثغرات الأمنية التي تكتشف أثناء المسح الدوري الذي تقوم به الهيئة الوطنية لخدمات تقانة المعلومات.

4. تلتزم الجهة العامة بمعالجة جميع الثغرات الأمنية التي تبلغها بها الهيئة من خلال الاختبارات الأمنية، وتقديم التعاون والتنسيق الكامل مع الهيئة، وتسهيل جميع المتطلبات اللازمة للاختبارات الأمنية والاستجابة للحالات الطارئة.

5. يجب توفير الكوادر المؤهلة، والتوعية والتدريب المستمر للكوادر المسؤولة عن إدارة الموقع والنشر عليه، وذلك قبل إطلاق الخدمة، لضمان الجاهزية الفنية والأمنية.

6. يجب إجراء مراجعات أمنية واختبارات اختراق دورية للمواقع والمنصات الإلكترونية، لاسيما الحكومية منها، من قبل جهات معتمدة من الهيئة الوطنية لخدمات تقانة المعلومات، وذلك على الأقل مرة سنويًا أو عند كل تغيير رئيسي في البنية أو إطلاق خدمات جديدة .ويجب توثيق نتائج الفحص والإجراءات التصحيحية المتخذة، لضمان خلو المنصة من الثغرات الأمنية..

7. عند مغادرة أي موظف للعمل لأي سبب (نقل، ندب، استقالة، تقاعد...إلخ)، يجب التأكد من إلغاء جميع الصلاحيات والامتيازات التي كانت بحوزته بشكل فوري في نهاية عمله، وذلك لضمان عدم بقاء أي وصول غير مصرح به.

8. يجب على جميع الجهات الحكومية تحديد جهة اتصال رسمية (بريد إلكتروني، رقم هاتف وتحديد أوقات عمل الهاتف) للإبلاغ عن أي حادثة أمنية أو خلل فني طارئ في الموقع الإلكتروني، ونشر هذه المعلومات بشكل واضح في صفحة التواصل أو ترويسة الموقع، مع التأكيد على سرعة التواصل مع مركز أمن المعلومات عند حدوث أي اختراق أو عطل مفاجئ. مثال: "في حال اكتشاف أي ثغرة أمنية أو تعرض الموقع لهجوم أو عطل، يرجى التواصل فوراً مع مركز أمن المعلومات عبر البريد الإلكتروني *[infosec@naits.gov.sy]*أو رقم الهاتف 0113937032 من التاسعة صباحاً حتى الرابعة مساءً."

2-9- متطلبات عقدية:

1. يجب تجنب التعاقد مع مطورين مستقلين (أفراد)، والالتزام بالتعاقد مع شركات ذات خبرة وسمعة جيدة من القطاعين العام أو الخاص، لضمان استمرارية التطوير وإغلاق الثغرات الأمنية المستجدة وتوفير الدعم الفني. يعود ذلك إلى أن أغلب الجهات العامة تواجه صعوبة في التواصل مع المطورين الأفراد عند الحاجة لمعالجة الثغرات الأمنية المكتشفة من قبل مركز أمن المعلومات في الهيئة الوطنية لخدمات تقانة المعلومات.

2. إذا كانت المنصة الإلكترونية تتضمن خدمات معاملات إلكترونية، يجب التأكد من حصول المنصة على وثيقة اعتمادية من الهيئة الوطنية لخدمات تقانة المعلومات قبل توقيع عقد التوريد أو التطوير.

3. لا يجوز استلام الموقع أو المنصة أو التطبيق دون إجراء الاختبارات الأمنية اللازمة لدى الهيئة الوطنية لخدمات تقانة المعلومات، مع إلزام الشركة المطورة بمعالجة جميع الثغرات الأمنية التي يتم اكتشافها أثناء الفحص الأمني الرسمي.

4. يجب إلزام الشركة المطورة بتسليم الكود المصدري (Source Code) الكامل غير مشفر، مع دليل كامل لهيكلية الموقع، كيفية إدارة الموقع، وتحديثه وتطويره، وتوقيع اتفاقية عدم إفشاء (NDA) لضمان سرية المعلومات ومعالجة الثغرات الأمنية متى دعت الحاجة، ووفق شروط وأحكام القوانين النافذة في التعاقد.

5. يجب إلزام الشركة المطورة بتسليم كافة الحسابات التي تم استخدامها أثناء التطوير، وعلى الجهة العامة التأكد من استلامها وتغيير كلمات المرور فورًا، مع الاحتفاظ بها بطريقة آمنة في مديرية المعلوماتية أو الوحدة التنظيمية المعنية.

6. عند تغيير الفريق التقني أو انتهاء التعاقد مع أي شركة تطوير، يجب توثيق وتسليم جميع الحسابات وكلمات المرور ونسخ احتياطية حديثة من قواعد البيانات والكود المصدري، مع تغيير جميع كلمات المرور فورًا وحصر الصلاحيات بالأشخاص المخولين فقط، وتوثيق عملية الاستلام والتسليم بشكل رسمي.

7. يجب تضمين بند صريح في العقد يلزم الشركة المطورة بمعالجة أي ثغرات أمنية يتم اكتشافها خلال فترة الضمان أو الدعم الفني، وبما يتوافق مع تعليمات الهيئة الوطنية لخدمات تقانة المعلومات.

8. يُنصح أن تتضمن العقود بندًا يحدد آلية التعاون مع الهيئة الوطنية لخدمات تقانة المعلومات في كل ما يتعلق بالاعتمادية، الفحص الأمني، تسليم الكود المصدري، وإدارة الثغرات، بما يضمن الامتثال الكامل للضوابط الوطنية.

اتفاقية مستوى الخدمة

اتفاقية مستوى الخدمة (SLA) هي عقد يُبرم بين الجهة الحكومية والجهة المطورة أو المشغلة للموقع الحكومي، تهدف إلى تحديد مستوى الخدمة المتوقع من حيث التوافرية والموثوقية.

تدعم اتفاقية مستوى الخدمة توافرية الموقع بشكل كبير من خلال تحديد بنود واضحة مثل:

وقت التشغيل :(Uptime) النسبة المئوية للوقت الذي يكون فيه الموقع متاحًا للعمل.

وقت التسليم :المدة الزمنية المتفق عليها لتسليم الخدمات أو التحديثات.

وقت الاستجابة للمشكلات الطارئة :المدة التي تستغرقها الجهة المشغلة للرد على المشكلات.

3- تطوير الموقع

3-1- خطوات إنشاء المواقع الإلكترونية الحكومية

يجب على الجهات الحكومية مراعاة الخطوات التالية عند إنشاء مواقعها الإلكترونية.

3-1-1- تعريف الأهداف وتحليل الأعمال

يجب تحديد النتائج المرجوة للجمهور منذ البداية ، مصدر التمويل اللازم لتشغيل وصيانة الموقع، ومستوى جودة التصميم المتوقع.

3-1-2- تعريف المتطلبات

يجب التصريح بوضوح بما هو مطلوب لتحقيق الأهداف، مثل تحديد المستفيدين، والموارد المطلوبة، والجهة المسؤولة عن تأمين هذه الموارد، والجدول الزمني لذلك.

3-1-3- التخطيط للمشروع

يجب تحديد كيفية تلبية احتياجات مستخدمي الموقع، مثل: بنية الموقع الإلكتروني، وفريق الإشراف والإدارة، وآليات التمويل والتسويق، والمواصفات الفنية والوظيفية وغير الوظيفية، بالإضافة إلى حجز اسم النطاق في حال لم يكن محجوزًا مسبقًا.

3-1-4- التصميم والتنفيذ

1. يجب أن تتضمن مرحلة التصميم تطوير واجهة المستخدم (UI) بشكل احترافي، مع ضمان توافق جميع عناصر الواجهة مع التوصيات والمعايير الواردة في قسم التصميم من الدليل المعتمد.
2. ينبغي كتابة الكود المصدري للموقع الإلكتروني وفقًا للمعايير البرمجية وأفضل الممارسات، مع الالتزام بمبادئ التصميم الآمن (secure by design principles)، لضمان سهولة قراءة الكود المصدري وقابليته للتعديل والصيانة مستقبلاً.
3. يُفضّل بناء المواقع باستخدام لغات البرمجة والمنصات الشائعة والمعتمدة مثل .NET أو PHP أو JAVA، لما توفره من دعم فني واسع، وتحديثات أمنية مستمرة، ومرونة في التطوير والتكامل مع الأنظمة الأخرى.
4. يجب أن تمتلك الجهة الحكومية الكود المصدري الكامل للموقع، بما في ذلك جميع الملفات البرمجية وقواعد البيانات والوثائق التقنية، لضمان القدرة على الصيانة والتطوير المستقبلي دون الاعتماد على جهة خارجية.

3-I-5- اختبارات الموقع

يجب إجراء اختبارات للتأكد من أن المنتج النهائي يلبي الأهداف المطلوبة. وتُعد الاختبارات التالية الحد الأدنى المطلوب لضمان السلامة الفنية للموقع، ويجب تضمينها ضمن مرحلة الاختبار:

1. اختبار الوظائف
2. اختبار قابلية الاستخدام
3. اختبار الواجهة
4. اختبار التوافقية
5. اختبار الأداء
6. اختبار الأمان واختبار قابلية الاختراق (Penetration Testing)

يجب أن تتم جميع هذه الاختبارات بواسطة جهة موثوقة ومعتمدة من قبل الهيئة الوطنية لخدمات تقانة المعلومات التابعة لوزارة الاتصالات والتقانة، والتي تملك الصلاحية للموافقة النهائية على إطلاق الموقع.
يضمن هذا الإجراء التحقق من سلامة الموقع من الناحية الفنية والأمنية، وامتثاله للمعايير الوطنية والدولية ذات الصلة، ويعزز ثقة المستخدمين في الخدمات الحكومية الرقمية.

كما أن الاعتماد على جهات معتمدة يضمن جودة عمليات الاختبار، وفعالية اكتشاف ومعالجة الثغرات والمشكلات التقنية قبل الإطلاق الرسمي للموقع.

3-I-6- الصيانة ومراقبة الجودة والمراجعة

1. يجب إجراء ما يلي للمحافظة على موقع الويب وضمان جودته:
2. إجراء فحوصات منتظمة للتأكد من سلامة جميع الروابط.
3. مراقبة إحصائيات الموقع بشكل دوري.
4. مراقبة البريد الإلكتروني المرتبط بالموقع.
5. التحقق من جاهزية خطط التعافي من الكوارث.
6. التدريب المستمر لفريق العمل على إدارة المحتوى.
7. تقييم الموقع كمشروع ومراجعته بشكل دوري.
8. المحافظة على جاهزية بيئة الاستضافة وتجديدها عند الحاجة.
9. مراقبة التوافر (Availability) من خارج نطاق الخوادم والشبكة للتأكد من استمرارية عمل الموقع.

10. التأكد من إجراء النسخ الاحتياطي بشكل دوري، مع اختبار استرجاع النسخ الاحتياطية مرتين سنويًا على الأقل.
11. اختبار خطة التعافي من الكوارث مرة واحدة سنويًا على الأقل، مع تحديثها عند حدوث تغييرات جوهرية في البنية أو الأنظمة.
12. مراقبة الهجمات الإلكترونية بشكل مستمر، باستخدام أدوات وتقنيات المراقبة اللحظية.
13. تقييم الثغرات الأمنية بشكل دوري، على الأقل مرة شهريًا، مع إعداد تقارير تحليلية لمعالجة نقاط الضعف المكتشفة.

جرت العادة أن تتضمن لوحة إدارة الموقع البيانات الإحصائية والتنبيهات المطلوبة من قبل القائمين على الموقع.

4- إدارة الموقع

على الجهات الحكومية أن تتولى المهام التالية:

1. تحديد الأهداف المتوخاة من نشر الموقع، ومراجعة هذه الأهداف بشكل دوري بهدف تحسينها وتوسيع نطاقها.
2. التأكد من أن الموقع مزود بما يكفي من الموارد البشرية والتقنية والمالية لضمان استمرارية العمل وجودة الأداء.
3. تزويد الموقع بالخدمات ومصادر المعلومات اللازمة لتلبية احتياجات المستفيدين وضمان جودة المحتوى الرقمي.
4. إجراء مراجعات دورية تتعلق بقابلية الاستخدام وجودة المحتوى والخدمات المقدمة عبر الموقع، مع الاستفادة من مؤشرات الأداء ونتائج التقييم لتحسين تجربة المستخدم ورفع مستوى رضا المستفيدين.

4-1- الخطة التشغيلية لإدارة المواقع الإلكترونية

يجب أن تتضمن الخطة التشغيلية تطويرًا ومراجعة دورية لجميع الخطط المتعلقة بالموقع الإلكتروني، بما في ذلك خطط توفير الخدمات عبر الإنترنت، والخطط المالية، وإدارة المخاطر، وإدارة المعلومات، وحتى التسويق عند الحاجة.

ينبغي أن تنص الخطة على ضرورة مراجعتها بشكل دوري، مع تحديد جداول زمنية واضحة لتطبيقها وتحديثها.

4-2- مراجعة الخطة بشكل دوري

تتطلب الخطة التشغيلية إجراء مراجعة منتظمة بهدف:

1. مقارنة الفوائد المتوقعة مع النتائج الفعلية.
2. وضع خطط طوارئ للتعامل مع الأحداث غير المتوقعة، مثل التكاليف الإضافية أو تغيّر الكادر المسؤول عن المشروع، واقتراح حلول مناسبة لها.
3. دراسة فرص تحسين الخدمات المقدمة وتوسيع نطاقها باستمرار، بما يواكب احتياجات المستخدمين وتطور التقنيات.
4. تحديد ومراجعة أجور الخدمات المقدمة.
5. تطبيق التعديلات اللازمة على المحتوى لضمان جودته وملاءمته لاحتياجات المستخدمين.
6. تشمل مراجعات الخطط معالجة مجموعة متنوعة من القضايا الرئيسية، مثل:

7. المراقبة المستمرة للنشاطات الجارية على الموقع.
8. تعديل الموقع لمواكبة احتياجات المستخدمين والتقنيات الحديثة.
9. تعديل وتوسعة أنظمة تخزين واسترجاع البيانات ذات الصلة.
10. تحديث الأجهزة والبرمجيات المستخدمة في تشغيل الموقع.
11. تلبية متطلبات تدريب الموظفين الجدد لضمان استمرارية العمل بكفاءة.

بالإضافة للمحافظة على صلاحية وحيوية الموقع وتحسينها، فإن عملية المراجعة قد تبرز بعض المشاكل المحتملة و/أو أي تغييرات جديدة مطلوبة لتلبية احتياجات الجمهور والجهة بشكل أفضل.

4-3- مراقبة وتقييم الموقع

4-3-1- ملاحظات الموقع

يجب على الجهات الحكومية توفير آلية لتقديم الملاحظات التغذية الراجعة لإتاحة الفرصة لمستخدمي الموقع إرسال أي تعليقات وملاحظات على الموقع إلى مسؤولي الموقع، ويجب تعيين موظف مسؤول لمراجعة التعليقات والرد عليها في غضون 72 ساعة على الأكثر من وقت وصولها.

4-3-2- التدقيق الذاتي

يفضّل إجراء عمليات تدقيق ذاتي استباقية لإدارة الموقع، على أن تشمل هذه المراجعة الداخلية، على الأقل، ما يلي:

1. مراقبة المشكلات المُبلّغ عنها واستفسارات العملاء خلال فترة زمنية سابقة، مع ملاحظة أن عدد هذه البلاغات يجب أن يتناقص مع اتخاذ الإجراءات التصحيحية المناسبة.
2. مراقبة موثوقية الموقع وجدارته، ومدى استخدامه واعتماده من قبل المستخدمين.
3. مراقبة دقة المعلومات المعروضة على الموقع، واتساقها، واكتمالها.
4. مراجعة الموقع للتأكد من توافقه مع السياسات والإرشادات المعتمدة.

4-4- صيانة الموقع

4-4-1- سلامة المعلومات

يجب أن تتضمن خطة إدارة المعلومات تدابير مختلفة للحفاظ على سلامة المعلومات وأهمها ما يلي:

1. إجراء فحوصات دورية على دقة المعلومات المنشورة، وتحديثها عند اللزوم.

2. إزالة الأقسام التي لم تعد مفيدة، مع مراعاة الضوابط الخاصة بالأرشفة وحفظ السجلات. مع ضرورة الالتزام بعدم إزالة أو نقل أي صفحة دون تأمين رابط من موقعها الأصلي إلى مكانها الجديد أو مكان أرشفتها.
3. التحقق بشكل دوري من صلاحية الروابط إلى مواقع الويب الخارجية وأن محتواها لا يزال مناسباً. يفضل استخدام برامج للتحقق الآلي من كافة الروابط.
4. التأكد من وفاء موقع الويب بأي وعود تم اعطاءها للمستخدمين للحصول على معلومات أو خدمات جديدة.

4-4-2- إيقاف تشغيل المواقع الإلكترونية

يجب مراجعة مواقع الويب بانتظام للتأكد من أنها لا تزال مفيدة وذات صلة، ويجب إيقاف الموقع إذا تبين أنه:

1. لا يخدم وظيفة أو هدف محدداً للحكومة.
2. تم تطويره لمشروع أو استراتيجية معينة لم تعد صالحة أو قائمة.
3. تم إطلاقه كجزء من حملة ترويجية برعاية الحكومة وانتهت هذه الحملة، وخصوصاً إذا تبين أنها لم تكن ضرورية وتظهر إحصائيات حركة البيانات أنه لم يتم استخدام الموقع.

عند إيقاف تشغيل مواقع الويب:

1. يجب أرشفة المحتوى بشكل مناسب.
2. حذف أو تعطيل جميع الحسابات الإدارية وصلاحيات المستخدمين المتعلقة بالموقع.
3. أرشفة جميع المراسلات والمحتوى الرسمي بطريقة آمنة، مع التأكد من عدم بقاء أي حساب نشط أو إمكانية دخول غير مصرح بها.
4. حفظ نسخة كاملة من الموقع، بما في ذلك قاعدة البيانات وجميع الملفات، في نظام إدارة الأرشيف المعتمد لدى الجهة الحكومية.
5. التأكد من أن الأرشيف يتضمن جميع الإجراءات والشروحات البيانات الوصفية (metadata) اللازمة لإعادة إنشاء الموقع أو الرجوع إلى محتواه في أي وقت مستقبلاً.
6. إذا تم الإبقاء على المحتوى المؤرشف متاحًا عبر الإنترنت، يجب توضيح أنه محتوى أرشيفي لم يعد يُحدّث، مع بيان تاريخ الأرشفة واستخدامه للأغراض المرجعية فقط.

7. اتخاذ جميع الإجراءات الأمنية اللازمة عند حذف الموقع، مثل إلغاء الشهادات الرقمية، حذف النطاق، إزالة قواعد البيانات، وتحديث إعدادات الجدار الناري.

8. تحديث سجلات الجهة الحكومية لتوثيق عملية الإيقاف والأرشفة، وضمان إمكانية استرجاع المحتوى عند الحاجة، أو تلبية أي طلب رسمي يتعلق بالمعلومات المؤرشفة.

5- توفير المعلومات

تُعد شبكة الإنترنت إحدى أكثر الوسائل شيوعًا للوصول إلى المعلومات وطلب الخدمات الحكومية؛ لذلك يجب على الجهات الحكومية التأكد من أن المعلومات المنشورة على مواقعها دقيقة، وأن تتم مراجعتها وتحديثها بشكل دوري وعند الحاجة.

5-1- متطلبات توفير المعلومات

يجب أن تكون المعلومات المقدمة على المواقع الحكومية متسقة مع السياسات والتوجهات الحكومية، لضمان دقتها وموثوقيتها وتجنب تقديم معلومات مضللة سواء للحكومة أو للمستفيدين. كما ينبغي مراجعة هذه المعلومات وتحديثها بشكل دوري، والالتزام بالمعايير والسياسات التنظيمية المعتمدة لنشر البيانات والمحتوى الرقمي.

5-2- مستوى توفير المعلومات

يجب على الجهات الحكومية نشر نسخ من الوثائق الموجهة للمواطنين وغيرها من المعلومات المصنفة بدرجة تصنيف عادي على مواقعها الإلكترونية. وإذا تعذّر ذلك، مثل في حال كانت البيانات كبيرة الحجم، أو مكلفة على الشبكة، أو الطلب عليها قليل جدًا، أو يتطلب نشرها إجراءات معقدة، فيجب توفير آلية واضحة للحصول على هذه المعلومات.

5-2-1- الصفحة الرئيسية:

يجب أن تتضمن الصفحات الرئيسية للمواقع الحكومية المكونات الأساسية التالية:

1. اسم الجهة
2. بالنسبة للمواقع الإلكترونية للوزارات، يُستخدم شعار الجمهورية العربية السورية (العقاب الذهبي). بالنسبة لبقية الجهات، يُستخدم الشعار المعتمد للجهة، وفي حال عدم وجود شعار خاص، يُستخدم شعار الجمهورية العربية السورية (العقاب الذهبي).
3. رابط لصفحة تعرض معلومات الاتصال بالجهة، متضمنة رقم هاتف فعّال، عنوان بريد إلكتروني يُتابع بشكل دائم، العنوان التفصيلي للجهة، ونموذج مراسلة (form) يحتوي على الحقول التالية:
   - اسم الزائر
   - عنوان الزائر
   - عنوان الرسالة
   - نص الرسالة

- اختيار الإدارة أو القسم المختص داخل الجهة الحكومية الذي يرغب المرسل في توجيه رسالته إليه.

4. يجب أن يوفر الموقع وسيلة فعّالة للبحث عن محتوى معين ضمن الموقع، وأن تكون متاحة في جميع صفحات الموقع.
5. يجب أن يوفر الموقع خريطة توضح هيكلية الموقع (site map)، ما يسهم في سهولة التنقل وتحسين تجربة المستخدم، كما تُعد خريطة الموقع من المتطلبات الأساسية لتحسين ظهور الموقع في محركات البحث.

5-2-2- دليل الخدمات والهيكل التنظيمي

يتعين على المؤسسات الحكومية تقديم دليل خدمات وهيكل تنظيمي واضح ومتكامل، يشمل ما يلي:

1. توفير تفاصيل الاتصال الكاملة، بما في ذلك الموقع الجغرافي لتقديم الخدمة، وأرقام الهواتف، وعناوين البريد الإلكتروني الخاصة بالقسم أو الوحدة التنظيمية المسؤولة عن العلاقات العامة أو تقديم الخدمة المطلوبة.
2. عرض الهيكل التنظيمي للجهة بشكل واضح، بحيث يوضح تقسيم الوحدات الإدارية والأقسام ومسمياتها واختصاصاتها، مما يسهل على المستفيدين معرفة الجهة أو القسم المسؤول عن كل خدمة.
3. توثيق إجراءات العمل التنظيمية لكل وحدة إدارية، مع تحديد نقاط الاتصال ومسؤوليات كل قسم، وذلك بهدف تسهيل التواصل الداخلي والخارجي، وضمان تقديم الخدمات بكفاءة وشفافية.
4. تحديث دليل الخدمات بشكل دوري ليشمل جميع الخدمات المقدمة، مع توضيح اشتراطات وضوابط الحصول عليها، وطرق التواصل والاستعلام، بما في ذلك القنوات الإلكترونية والخرائط التفاعلية عند توفرها.
5. يُعد هذا النهج من أفضل الممارسات التنظيمية، حيث يعزز الشفافية، ويُسهّل على المواطنين والمستفيدين الوصول إلى المعلومات والخدمات، ويحقق التكامل والفعالية في إدارة العمليات الحكومية.

5-2-3- قسم خاص لمساعدة المواطن

ينبغي أن يتضمن القسم الخاص بمساعدة المواطن في المواقع الحكومية المعلومات والخدمات التي تضمن وضوح حقوق وواجبات المواطن، وتيسّر تواصله مع الجهة الحكومية، وذلك من خلال العناصر التالية:

1. آليات معالجة الشكاوى: توفير شرح واضح لكيفية تقديم الشكاوى أو الملاحظات، مع وجود استمارات إلكترونية أو قنوات مباشرة لتقديمها، وإتاحة متابعة حالة الشكوى إلكترونيًا عند الإمكان.

2. استمارات تقديم الطلبات أو الحصول على الخدمات: إتاحة نماذج إلكترونية مبسطة لتقديم الطلبات أو الاستفسارات أو الحصول على الخدمات، مع توضيح الخطوات المطلوبة والمستندات اللازمة.

3. قنوات الحصول على الخدمات: عرض جميع القنوات المتاحة للحصول على الخدمات، سواء كانت إلكترونية (عبر الموقع أو تطبيقات الهاتف)، أو تقليدية (مراكز الخدمة، الهاتف، البريد)، مع توضيح ساعات العمل وطرق التواصل.

4. جميع السياسات المعمول بها في تقديم الخدمات: نشر السياسات والإجراءات المنظمة لتقديم الخدمات بشكل واضح وشفاف، مع إضافة ملاحظات توضيحية تشرح حقوق المواطن وواجباته، وما هو متوقع من الجهة الحكومية في كل خدمة.

5. قسم الأسئلة الشائعة (FAQ): تخصيص قسم للإجابة على الاستفسارات المتكررة من المواطنين، مع تحديثه بشكل دوري بناءً على الملاحظات والأسئلة الواردة فعليًا من المستخدمين، واستخدام لغة واضحة ومباشرة تسهّل الفهم والوصول السريع للمعلومة.

5-2-4- نماذج العمل

يجب إتاحة نماذج العمل أو الاستمارات المستخدمة على نطاق واسع من قبل المواطنين على المواقع الإلكترونية للجهات الحكومية، سواء بصيغ قابلة للتحميل أو من خلال نماذج إلكترونية قابلة للتعبئة والتقديم المباشر عبر الموقع.

ينبغي أن تتسم هذه النماذج بالوضوح وسهولة الاستخدام، وأن تُصمم وفق أفضل الممارسات لضمان سهولة الوصول لجميع المستخدمين، بما في ذلك ذوو الاحتياجات الخاصة. يُوصى باستخدام لغة بسيطة ومباشرة، وتوضيح أي معلومات أو تعليمات غير بديهية ضمن النموذج. كما يجب تقسيم النماذج الطويلة إلى أقسام منطقية، وتوفير إرشادات واضحة في كل جزء لتسهيل عملية الملء.

تُعد النماذج الإلكترونية وسيلة فعّالة لتيسير التفاعل بين المواطن والجهة الحكومية، وتُسهم في تحسين كفاءة تقديم الخدمات وزيادة رضا المستفيدين.

6- المعرفات البصرية الحكومية

6-1- المعرفات البصرية للمواقع والمنصات الحكومية

يجب إبراز الهوية السورية بشكل واضح وتوضيح تبعيتها للحكومة السورية على جميع المواقع الإلكترونية للجهات العامة، وعلى كافة المستويات الإدارية (الوزارات، المديريات، ...إلخ)،. ولتحقيق ذلك، يجب الالتزام بالمبادئ التوجيهية التالية:

1. عرض الشعار الوطني (العقاب الذهبي) على الصفحة الرئيسية لكافة المواقع الإلكترونية للوزارات.
2. تعرض بقية الجهات الحكومية شعاراتها الرسمية على الصفحة الرئيسية لمواقعها الإلكترونية لتأكيد هويتها.
3. يجب أن تتضمن الصفحة الرئيسية وجميع البوابات المهمة للموقع معلومات تبعية أو ملكية الموقع الإلكتروني، سواء في ترويسة الصفحة أو تذييلها. ويمكن عرض معلومات التبعية ضمن تذييل الصفحة، على سبيل المثال:
   - الهيئة الوطنية لخدمات تقانة المعلومات (NAITS) – جميع الحقوق محفوظة.
   - الموقع الرسمي للهيئة الوطنية لخدمات تقانة المعلومات (NAITS) – 2023
   - الموقع الرسمي لوزارة الاتصالات والتقانة السورية.
4. يجب أن تعرض جميع الصفحات الأخرى للموقع معلومات الملكية بشكل موجز قدر الإمكان.
5. يجب أن تبين الصفحة الرئيسية للموقع الإلكتروني وبوضوح الاسم الرسمي للجهة أو الخدمة الحكومية المعنية.
6. يجب ضمان بقاء الهوية البصرية (الشعار، الاسم، تبعية الجهة) واضحة عند تصفح الموقع من الأجهزة المحمولة أو الشاشات الصغيرة، مع التأكد من توافق التصميم مع مختلف الأجهزة والشاشات، وذلك باعتماد مبادئ التصميم المتجاوب واختبار توافق الموقع فعليًا على الأجهزة المختلفة.
7. يجب تضمين روابط لسياسة الخصوصية، شروط الاستخدام، التواصل مع المؤسسة الحكومية، وسياسة ملفات تعريف الارتباط ((Cookies في تذييل الصفحة، حيث تُعد هذه الروابط عنصرًا أساسيًا في تعزيز الموثوقية والشفافية لدى المستخدمين.

تساعد هذه الإجراءات في التأكيد على هوية الموقع، تعزيز مصداقيته، وضمان تجربة مستخدم موثوقة ومتسقة على جميع الأجهزة والمنصات.

6-2- أسماء النطاقات الحكومية

1. تُعد أسماء النطاقات الحكومية، بما في ذلك اسم النطاق وجميع محددات الموارد الموحدة (URL) لأي موقع حكومي على الشبكة، المؤشر الأساسي على تبعية الموقع واعتباره موقعًا رسميًا.
2. يجب الالتزام بالشكل المعياري في اختيار أسماء النطاقات، وذلك وفقًا للبلاغ رقم 15/13741 بتاريخ 2011/9/28 الصادر عن رئاسة مجلس الوزراء.
3. الجهات الحكومية التي يكون اسم النطاق الخاص بها طويلًا، يُنصح بأن تختار أسماء نطاقات قصيرة، سهلة التذكر، ومعبرة عن اختصاص الجهة في الوقت نفسه.
4. يمكن التواصل مع الهيئة الوطنية لخدمات تقانة المعلومات لحجز أسماء النطاقات أو لأي استفسار بهذا الخصوص.
5. يجب أن يُعرض العقاب الذهبي في الجزء العلوي الأيسر أو الأيمن من الموقع حسب اتجاه اللغة (اليمين للعربية، اليسار للإنجليزية).
6. يجب أن يكون الشعار واضحًا وبدقة عالية، وألا يتم تحريف أبعاده أو ألوانه.
7. يمكن الحصول على شعار الجمهورية العربية السورية (الهوية البصرية) من خلال زيارة الموقع التالي: https://syrianidentity.sy

شعار الجمهورية العربية السورية هو عقاب ذهبي مستلهم من تراث فتح الشام على يد خالد بن الوليد في معركة ثنية العقاب ضد البيزنطيين، وشعار الفنان (خالد العسلي عام 1945).

الأجنحة تضم 14ريشة (تمثل محافظات البلاد)،والذيل 5ريش (تمثل المناطق الجغرافية الخمس)، ما يعكس وحدة وتكامل الدولة .

النجوم الثلاث تحررت من موقعها التقليدي ورفعت إلى فوق العقاب، رمزًا لتحرر الشعب وتمكينه من السيادة فوق الدولة نفسها.

ألوان الهوية البصرية ورموزها

#002623 Forest	#b9a779 Golden wheat	#260f14 Deep Umber	#161616 Charcoal
#094239 Emerald Shadow	#988561 Antique Sand	#4a151e Black Cherry	#3d3a3b Stone
#428177 Mounatain Teal	#edebe0 Ivory Mist	#6b1f2a Damask Red	#ffffff White

7- أدلة استرشادية للتصميم

7-1- إرشادات تصميمية

يجب أن تُصمم مواقع الويب الحكومية لتلبية احتياجات جميع فئات الجمهور، مع مراعاة تنوع مستويات المعرفة الفنية وتعدد الاهتمامات والاختصاصات لديهم. يهدف ذلك إلى تمكين المستخدمين من الوصول إلى المعلومات والخدمات الحكومية بطريقة أكثر فعالية وكفاءة، مع التركيز على وضوح العلامة التجارية وتجربة المستخدم في جميع عناصر التصميم.

7-2- بنية الموقع

تُعنى بنية الموقع الإلكتروني بكيفية تنظيم محتوى الموقع وتدفق المعلومات وهيكلية المواضيع والتصنيفات، بما يتيح للمستخدمين التنقل بسهولة عبر الموقع، وتتبع تقدمهم وتحديد موقعهم ضمن الموقع انطلاقًا من أي صفحة.

عند تصميم أي موقع حكومي، يجب مراعاة ما يلي:

- ألا يحتاج المستخدم إلى أي فهم أو معرفة بالهيكل الداخلي للجهة للعثور على المعلومات أو الخدمات المطلوبة.
- تصنيف عناصر القائمة بشكل صحيح وبطريقة تؤكد سياق المعلومات، بحيث يتمكن الزوار من التفاعل مع عناصر القوائم بسلاسة ووضوح.

7-3- تخطيط الصفحات

7-3-1- الصفحة الرئيسية

1. ينبغي أن تكون الصفحة الرئيسية مفيدة وجذابة، مختصرة وسهلة القراءة.
2. يجب أن تتيح التنقل السهل بين مكونات الموقع.
3. كما ينبغي أن تتجنب الفوضى، مثل الرسوم المتحركة المشتتة، أو العناصر الرسومية غير الضرورية، أو النصوص اللامعة أو المتحركة.

7-3-2- الصفحات الأخرى

يجب اعتماد هوية بصرية موحدة وتطبيقها على جميع صفحات الموقع. يمكن تحقيق ذلك من خلال استخدام عناصر تصميم مشتركة، مثل الألوان، والشعارات، والأنماط، وغيرها، في كل صفحة.

كما ينبغي أن تكون الصفحات مختصرة. وفي حال وجود صفحات طويلة أو كثيرة المحتوى، يُفضل تقسيمها إلى عدة صفحات أصغر، بحيث تبقى مترابطة ومصنفة ضمن قوائم فرعية مناسبة.

7-3-3- تصفح الموقع

1. توفير روابط تنقل متسقة.
2. يجب أن تكون آلية تصفح الموقع سهلة الاستخدام وبديهية، لمساعدة المستخدم في الوصول إلى المعلومات أو الخدمات بسهولة.
3. ينبغي توفير روابط للصفحة الرئيسية وخاصية البحث في كل صفحة، بحيث تتيح هذه الروابط التنقل السلس بين صفحات الموقع.
4. يجب أن يبقى حجم المكونات المهمة، وشكلها، وموضعها، ووظيفتها متسقًا عبر جميع صفحات الموقع.
5. ينبغي أن يتيح الموقع التنقل بين جميع صفحاته ومكوناته دون الحاجة لاستخدام زر الرجوع في المتصفح.
6. عند استخدام روابط تشير إلى مواقع أخرى تحت اسم نطاق مختلف، يجب أن تُفتح في نافذة أو تبويب جديد.

- استخدام روابط تنقل يسهل التعرف عليها

تُعد العديد من أسماء الصفحات الشائعة مثل "الصفحة الرئيسية"، و"من نحن"، و"المنشورات"، و"البحث"، و"الاتصال بنا"، و"الروابط المفيدة"، و"خريطة الموقع" مصطلحات مقبولة على نطاق واسع. قد تبدو الأسماء الفريدة والإبداعية جذابة، لكنها قد تؤثر سلبًا على سهولة استخدام الموقع. يفضل الالتزام قدر الإمكان بالمصطلحات البسيطة والشائعة لأسماء صفحات التنقل، إلا في الحالات التي يكون فيها استخدام مصطلحات غير شائعة أمرًا ضروريًا.

7-3-4- توفير الوصول إلى بوابة الخدمات الحكومية

قد يجد بعض المستخدمين صعوبة في فهم هيكلية الحكومة أو تحديد الجهة المسؤولة عن تقديم المعلومات أو الخدمات المطلوبة. لذلك، يُنصح بتوفير رابط مباشر إلى بوابة الحكومة الالكترونية السورية (https://egov.sy)، التي تتيح الوصول إلى دليل شامل للخدمات الحكومية، وتساعد المواطنين وأصحاب الأعمال في التعرف على الإجراءات والحصول على الخدمات بسهولة.

7-3-5- مسار الصفحات ضمن الموقع

يُفضل توفير قائمة "Breadcrumb" في الجزء العلوي من كل صفحة ويب، توضح جميع المستويات بين الصفحة الرئيسية والصفحة الحالية، بحيث يكون كل مستوى عبارة عن رابط.

على سبيل المثال:

"الصفحة الرئيسية ← خدماتنا ← خدمات الاستضافة ← خدمة حجز اسم نطاق".

تتيح هذه الآلية للمستخدم التنقل ضمن هيكلية الموقع إلى أي مستوى مباشرة، دون الحاجة إلى المرور بجميع الروابط الوسيطة.

7-3-6- خريطة الموقع للمساعدة في التنقل

تمثل خريطة الموقع بنية الموقع بشكل نصي أو بياني في صفحة واحدة، وتوفر نظرة عامة واضحة على محتوى الموقع. كما تتيح الوصول السريع إلى الصفحات الرئيسية، مما يسهم في تحسين تجربة المستخدم وتسهيل التنقل ضمن الموقع.

7-4- الارتباطات التشعبية

7-4-1- إنشاء تسميات تصف بدقة وجهة الروابط

يجب أن تكون نصوص الروابط واضحة ودقيقة في وصف وجهة الرابط، بحيث يتمكن المستخدم من معرفة ما سيحصل عليه عند النقر دون الحاجة لقراءة النص المحيط. يُنصح تجنب العبارات العامة مثل "انقر هنا" أو "انتقال"، واستبدالها بمسميات معبّرة تصف محتوى الصفحة أو الخدمة، مثل "انقر هنا لمعرفة المزيد عن خدماتنا" أو "اطلع على تفاصيل المشروع". هذا يعزز سهولة الاستخدام ويخدم المستخدمين الذين يعتمدون على تقنيات المساعدة.

7-4-2- إنشاء روابط يسهل التعرف عليها

يجب تصميم الروابط بحيث تكون مميزة عن النص العادي، سواء كانت نصوصًا أو صورًا أو أزرارًا. يمكن تحقيق ذلك من خلال:

1. وضع خط أسفل الروابط النصية أو تلوينها بلون مميز، مع الحفاظ على التباين الكافي.
2. استخدام تأثيرات عند تمرير الماوس مثل تغيير لون الخلفية أو النص، لتوضيح أن العنصر قابل للنقر.
3. تجنب الروابط الطويلة جدًا أو التي تحتوي على رموز غير مألوفة، كي لا تبدو مشبوهة أو غير مفهومة.

ملاحظة هامة:

لا تخضع المنصات الداخلية أو المنصات التي تعنى بإجراءات العمل أو منصات تقديم الخدمة غير المتاحة للعموم لأي من معايير تخطيط المحتوى أو هيكلية الصفحات، ويقع تقدير التصميم والمحتوى على عاتق الجهة العامة وحاجتها للمحتوى.

7-4-3- تقييم الروابط الخارجية

عند وجود روابط تشير إلى مواقع أو جهات خارجية، يجب إعلام المستخدم بأنه سيغادر الموقع الحالي، ويتم فتح هذه الروابط في نافذة جديدة. يُستحسن أيضًا استخدام أيقونات أو إشارات بصرية توضح أن الرابط خارجي، مع التأكيد على أن صحة المعلومات المقدمة عبر هذه الروابط مسؤولية المصدر الخارجي.

7-4-4- التحقق من صلاحية الروابط

يجب التأكد دائمًا من أن الروابط تؤدي إلى صفحات فعّالة تحتوي على معلومات ذات صلة، وتجنب الروابط المكسورة أو غير الفعالة.

7-5- دقة الشاشة

يجب أن تكون مواقع الجهات الحكومية مصممة بأسلوب "التصميم المتجاوب" (Responsive Web Design)، بحيث تتكيف تلقائيًا مع مختلف أحجام الشاشات، بدءًا من الهواتف المحمولة الصغيرة جدًا، مرورًا بالأجهزة اللوحية، وصولًا إلى شاشات الحواسيب المكتبية الكبيرة. هذا النهج يضمن تجربة استخدام سلسة وسهلة لجميع الزوار، بغض النظر عن نوع الجهاز أو دقة الشاشة المستخدمة.

7-5-I- الخطوط

1. يجب الحرص على جعل النصوص سهلة القراءة من خلال استخدام الخطوط الافتراضية أو المعيارية، وضبط خصائص النص مثل شكل الحروف، حجمها، ولونها، بحيث تكون واضحة وقابلة للقراءة سواء عند العرض الإلكتروني أو عند الطباعة.
2. يُفضّل تحديد أنواع خطوط معيارية مدعومة على نطاق واسع، أو تضمين الخطوط المطلوبة باستخدام تقنيات CSS التي تشير إلى ملفات الخطوط، لضمان ظهور النص بالشكل المطلوب لدى جميع المستخدمين. ليست كل الخطوط متاحة أو مدعومة في جميع الأجهزة أو المتصفحات، لذا يُنصح بالاعتماد على خطوط شائعة مثل "Times New Roman، Tahoma،Arial "، أو الخطوط الافتراضية الخاصة بنظام التشغيل.
3. ينبغي استخدام أحجام خطوط مناسبة تسهّل قراءة النصوص على الشاشات، مع الأخذ في الاعتبار أن متصفح المستخدم قد يؤثر على طريقة عرض النص النهائي. كما يُفضّل اعتماد نوع خط واحد أو نوعين كحد أقصى، وتطبيق نمط الخط المعتمد بشكل موحد على جميع صفحات ومحتويات الموقع، مما يعزز وضوح الهوية البصرية ويوفر تجربة قراءة متسقة وسهلة للمستخدمين.
4. يُنصح باستخدام وحدات قياس نسبية بدلاً من الثابتة عند تحديد حجم الخطوط، مثل استخدام وحدات em أو rem، لضمان توافق حجم النص مع إعدادات المستخدم واحتياجاته.
5. يجب توفير زر أو آلية لتفعيل وضع الألوان عالية التباين للمستخدمين ذوي الإعاقات البصرية، مما يسهم في تحسين إمكانية الوصول لجميع فئات المستخدمين.

7-5-2- الألوان والخلفيات

- يجب استخدام نظام ألوان متسق وتطبيقه على جميع صفحات ومحتويات الموقع.
- ينبغي اختيار ألوان ذات تباين جيد، سواء على الشاشة أو على الورق، بحيث يكون تباين النص مع الخلفية مرتفعًا بما يكفي لضمان وضوحه في جميع الحالات.
- يُنصح بتجنب عرض الزخارف أو الرسومات في خلفيات الصفحات، حتى لا تزيد من حجم الصفحة وتؤثر سلبًا على سرعة التحميل.
- يجب استخدام ألوان تناسب الأشخاص ذوي الإعاقات اللونية، مع مراعاة سهولة تمييز جميع العناصر البصرية.
- يُفضل دعم خاصية الوضع الداكن (Dark Mode)، لما لها من دور في تعزيز راحة العين وزيادة رضا المستخدمين.

7-5-3- الصور

- يجب استخدام الصور والمخططات ووسائل الإيضاح بشكل معتدل وغير مبالغ فيه، لتقليل استهلاك الموارد وتسريع تحميل الصفحة لدى المستخدم.
- ينبغي اختيار صيغ الصور المناسبة (مثل JPEG للصور الفوتوغرافية وPNG للرسومات ذات الشفافية) بهدف تقليل وقت التحميل مع الحفاظ على أعلى جودة عرض ممكنة.
- يُفضل إعادة استخدام الصور الشائعة، مثل تلك المرتبطة بهوية الموقع أو عناصر التنقل، لتقليل وقت التنزيل وتحسين الأداء، حيث إن الصور المخزنة في ذاكرة التخزين المؤقت للمتصفح لا تحتاج لإعادة تحميل وستُعرض بشكل أسرع.
- من المهم أيضًا ضغط الصور وضبط أبعادها بما يتناسب مع العرض الفعلي على الصفحة، لتفادي تحميل بيانات زائدة لا يحتاجها المستخدم.

7-6- الوسائط المتعددة والرسوم المتحركة

7-6-1- تقليل استخدام الرسوم المتحركة

1. يجب تجنب استخدام الرسوم المتحركة (GIF) إلا عند الضرورة القصوى، حيث إنها رغم فعاليتها في جذب الانتباه إلى عناصر مهمة ضمن الموقع، قد تتسبب في تشتيت المستخدمين وإبطاء سرعة تحميل الصفحات.

2. يفضل الاعتماد على التحريك باستخدام تنسيقات CSS الحديثة، مع تجنب استخدام رسوم GIF المتحركة أو التقنيات القديمة مثل Adobe Flash التي لم تعد شائعة أو مدعومة.
3. ينبغي أيضًا الحفاظ على أحجام ملفات الصور المتحركة صغيرة قدر الإمكان، وذلك من خلال الحد من عدد الإطارات في الثانية، لتقليل وقت التحميل وتحسين أداء الموقع.
4. إضافة Lazy Loading للصور والفيديوهات: لمنع تحميل جميع الصور والوسائط دفعة واحدة مما يستهلك الموارد ويبطئ الأداء، يجب تأخير تحميل الوسائط حتى يحتاج المستخدم لرؤيتها. هذه التقنية تساعد في تحسين سرعة تحميل الصفحات وتقليل استهلاك البيانات.
5. دمج الـ SVG بدلاً من PNG للأيقونات: تُعتبر ملفات SVG أكثر وضوحًا وأخف وزنًا مقارنة بصيغة PNG، مما يساهم في تحسين جودة العرض وتقليل وقت التحميل. كما أن SVG قابلة للتكبير دون فقدان الجودة، مما يجعلها مثالية للأيقونات والعناصر الرسومية البسيطة.

7-6-2- توفير مُكافِئات نصية لمقاطع الفيديو والصوت

1. من المهم تعزيز إمكانية الوصول إلى محتوى مقاطع الفيديو والصوت لجميع المستخدمين، وذلك من خلال توفير نصوص مكتوبة أو توصيفات صوتية لمقاطع الفيديو، مما يساعد الأشخاص ذوي الإعاقة البصرية أو أولئك الذين يستخدمون وسائل اتصال بطيئة في الوصول إلى المعلومات بسهولة.
2. كما يُستحسن إضافة نصوص أو على الأقل وصف لمقاطع الصوت، لتلبية احتياجات ضعاف السمع أو من لا يستطيعون الاستماع لأسباب خاصة، وبذلك يتحقق وصول شامل وعادل للمحتوى الرقمي لجميع فئات المستخدمين.

7-6-3- توفير تفاصيل تحميل مقاطع الفيديو والصوت

- يجب تزويد المستخدمين بمعلومات واضحة حول كل ملف فيديو أو صوت متاح للتحميل، لمساعدتهم على اتخاذ قرار مناسب بشأن الوصول إليه. تشمل هذه المعلومات:
  - تعليمات التحميل والاستخدام
  - وصف لموضوع الملف ومحتواه
  - حجم الملف
  - تنسيق الملف (مثل 3mpeg/mp4/mp)
  - تاريخ النشر واسم الملف عند الحاجة.

- إذا كان تشغيل الوسائط يتطلب برنامجًا معينًا، يجب توفير رابط مباشر لتحميل هذا البرنامج، مع توضيح ذلك للمستخدم بشكل صريح.
- يُنصح باعتماد تنسيق موحد للوسائط قدر الإمكان (مثل 4MP للفيديو و3MP للصوت)، وذلك لضمان التوافق مع معظم الأجهزة والمتصفحات وتحقيق أفضل تجربة للمستخدمين.
- يُفضل توفير إمكانية البث المباشر (Streaming) للوسائط من الموقع نفسه، بدلاً من إلزام المستخدمين بتحميل الملف بالكامل قبل تشغيله. البث المباشر يتيح مشاهدة أو الإستماع الفوري مع تقليل الحاجة إلى تخزين الملفات على أجهزة المستخدمين، كما أنه يدعم التكيف مع سرعات الانترنت المختلفة ويوفر تجربة أكثر سلاسة.
- من الأفضل أيضًا تضمين عنوان ووصف موجز للوسائط، مع الإشارة إلى ما إذا كانت جزءًا من سلسلة أو مرتبطة بمواضيع أخرى ذات صلة، مما يساعد المستخدمين في تحديد مدى ملاءمة المحتوى لاحتياجاتهم.

7-6-4- تصميم متجاوب يدعم أوضاع الألوان المختلفة وقابلية التكبير

1. يجب أن يدعم الموقع أوضاع الألوان المختلفة (Color Schemes)، بحيث يمكن للمستخدم التبديل بين الوضع الداكن والفاتح وفق تفضيلاته أو إعدادات نظام التشغيل، وذلك باستخدام خاصية prefers-color-scheme في CSS أو عبر آلية اختيار يدوية. يجب توفير تباين لوني مناسب في كل وضع لضمان وضوح المحتوى وسهولة القراءة.
2. ينبغي أن يتيح التصميم إمكانية تكبير المحتوى حتى 200% على الأقل دون أن يتأثر تخطيط الصفحة أو تنكسر العناصر، تحقيقًا لمتطلبات معايير WCAG الحديثة، مع ضرورة اختبار الموقع على مختلف مستويات التكبير للتأكد من سلامة العرض.
3. يعتمد التصميم على فلسفة Mobile-First، أي البدء بتصميم الموقع للأجهزة الصغيرة أولًا، ثم التوسع تدريجيًا ليشمل الشاشات الأكبر، مع استخدام استعلامات وسائط (Media Queries) فعالة لضمان عرض المحتوى بشكل صحيح ومتجاوب على كافة الأجهزة والأحجام.

7-7-عرض الموقع

7-7-1- يجب تصميم التطبيق وفقاً للمعايير وليس للمتصفحات

تصميم تطبيقات الويب وفقًا للمعايير (Web Standards) وليس للمتصفحات الفردية يُعد من أفضل الممارسات في تطوير الويب الحديث. المعايير مثل HTML،CSS ، وJavaScript التي تضعها منظمات

مثل W3C، تهدف إلى ضمان أن يعمل الموقع بشكل صحيح ومتسق عبر جميع المتصفحات والأجهزة، دون الحاجة إلى تخصيص الكود المصدري أو إضافة حلول خاصة بكل متصفح.

7-7-2- استخدام ملفات تنسيق CSS للتحكم في العرض

1. يتيح استخدام CSS تعريف وتعديل أنماط العرض بشكل مستقل عن محتوى الموقع، مما يسهم في توحيد وتناسق المظهر عبر جميع صفحات ومكونات الموقع.
2. يجب التأكد من أن أنماط العرض متسقة وموحدة، مع تطبيقها بشكل متكامل على كامل الموقع لتوفير تجربة مستخدم متجانسة وواضحة.
3. ينبغي تجنب استخدام ميزات CSS غير المدعومة في بعض المتصفحات أو التي قد تؤثر على إمكانية الوصول، لضمان عمل الموقع بشكل صحيح لجميع المستخدمين بغض النظر عن المتصفح المستخدم.

7-7-3- استخدم القوالب من أجل الاتساق

استخدام قوالب صفحات الويب يساعد بشكل كبير على تحقيق الانسجام والاتساق ضمن الموقع، مما يعزز تجربة المستخدم ويجعل التنقل بين الصفحات أكثر سلاسة ووضوحًا. تساهم القوالب في تقليل الوقت والجهد اللازمين لإنشاء محتوى الموقع، إذ يمكن إعادة استخدام عناصر التصميم الأساسية مثل استدعاءات CSS المعيارية، وعناصر الترويسة والتذييل، وعناصر التنقل بين الصفحات.

هذا النهج يضمن توحيد المظهر والأسلوب عبر جميع صفحات الموقع، مما يعزز الهوية البصرية ويقلل من الأخطاء الناتجة عن اختلاف التنسيقات بين الصفحات. باستخدام القوالب، يمكن للمطورين والمصممين التركيز على محتوى الموقع بدلاً من إعادة تصميم كل صفحة من الصفر، مما يزيد من كفاءة العمل ويسرع عملية التطوير.

7-7-4- تجنب استخدام الإطارات Frames

ينبغي تفادي استخدام الإطارات (Frames) في تصميم مواقع الويب لما تسببه من مشكلات متعددة في قابلية الاستخدام، من أبرزها:

1. مشاكل في الطباعة، حيث قد يقوم المتصفح بطباعة محتوى إطار واحد فقط بدلاً من الصفحة كاملة.
2. تعقيد عملية فهرسة واستعادة الصفحات باستخدام محركات البحث، إذ يُعامل كل إطار كوثيقة منفصلة مما يصعّب تحسين محركات البحث (SEO).

3. تعارض مع وظيفة زر "رجوع" في المتصفح، حيث لا يتم تحديث سجل التصفح بشكل صحيح عند التنقل داخل الإطارات.

4. صعوبات في الوصول بالنسبة للمستخدمين الذين يعتمدون على تقنيات المساعدة مثل قارئات الشاشة.

5. الإطارات تقنية قديمة وغير مدعومة في HTML5، حيث يُفضل استخدام CSS وJavaScript لتصميم التخطيطات الحديثة.

6. قد تتسبب الإطارات في تجربة مستخدم غير متسقة، وتعيق إمكانية حفظ أو مشاركة روابط صفحات محددة.

لذلك، يُوصى بالاعتماد على تقنيات التصميم الحديثة لضمان سهولة الاستخدام، التوافق مع محركات البحث، ودعم الوصولية لجميع المستخدمين.

7-7-5- تضمين اختصارات لوحة المفاتيح (Keyboard Shortcuts)

من المهم أيضًا توفير اختصارات لوحة مفاتيح واضحة تسهّل التنقل للمستخدمين ذوي الإعاقة البصرية أو الحركية، وتُحسّن إمكانية تصفح الموقع بدون الحاجة لاستخدام الماوس. هذه الميزة تدعم سهولة الاستخدام وتحقق معايير الوصول الرقمي، مما يضمن أن جميع المستخدمين يمكنهم الاستفادة من وظائف الموقع بكفاءة وسرعة.

7-8- بنية المجلدات وتسمية الملف

1. ينبغي اتباع أفضل الممارسات والأعراف عند اختيار أسماء الملفات والمجلدات، مما يسهل نقل مواقع الويب ويقلل من مخاطر الروابط المعطلة. يُفضل الالتزام بالتوصيات التالية:

2. استخدام الأحرف الصغيرة فقط في أسماء الملفات والمجلدات.

3. التأكد من أن الأسماء متصلة دون مسافات؛ ويمكن استخدام الشرطة "-" أو الشرطة السفلية "_" للفصل بين الكلمات عند الحاجة.

4. تقييد طول أسماء الملفات والمجلدات بحيث لا تتجاوز 20 حرفًا، لتسهيل التعامل معها وتجنب الأخطاء.

5. تحديد ملحقات الملفات بشكل صحيح وواضح، مثل: .html/ .htm/ .pdf/ .xls/ .png/ .gif.

7-9- التأليف ورسائل الخطأ والطباعة

7-9-1- إنشاء محتوى عبر نظام إدارة محتوى CMS

يُنصح بأن تعتمد كل جهة حكومية على نظام إدارة محتوى (CMS)، وهو تطبيق برمجي يمكّن المستخدمين من إنشاء محتوى موقع الويب وإدارته وتعديله ونشره بسهولة، دون الحاجة إلى خبرة برمجية مسبقة، وذلك عبر واجهة استخدام مبسطة وواضحة.

من المهم عند تطبيق نظام إدارة المحتوى الالتزام بالمبادئ التالية:

1. وجود تسلسل هرمي واضح للموافقة على المحتوى ونشره، مع تحديد المسؤولين عن الموافقة في كل مرحلة من مراحل العمل.
2. تنفيذ المهام بناءً على الأدوار المحددة في هذا التسلسل، مثل: منشئ المحتوى، المراجع، الناشر، المحرر، ومدير الموقع.
3. ربط كل دور بمجموعة من الأحداث أو المهام، مثل إضافة محتوى جديد، مراجعة وتعديل المحتوى، أو إزالة المحتوى، لضمان تنظيم العمل وسهولة تتبع العمليات.
4. يساهم هذا التنظيم في الحفاظ على تحديث ودقة المحتوى، وضمان وضوح المسؤوليات، وتحقيق تجربة مستخدم متسقة وموثوقة ضمن الموقع الحكومي.

يجب على كل جهة حكومية استخدام نظام إدارة المحتوى، وهو عبارة عن تطبيق برمجي يتيح للمستخدمين إنشاء محتوى الموقع الإلكتروني وإدارته وتعديله ونشره دون الحاجة إلى البرمجة من البداية وحتى دون معرفة بالبرمجة على الإطلاق، وكل ذلك عبر واجهة سهلة الاستخدام ومن المهم تطبيق المبادئ التالية:

يجب وجود تسلسل هرمي واضح للموافقة على المحتوى ونشره، مع تحديد المسؤولين عن اعتماد المحتوى، وتوضيح كيفية وآلية الموافقة، والمرحلة التي تتم فيها هذه العملية.

تنفذ المهام حسب الأدوار في التسلسل الهرمي، مثل؛ منشئ، مراجع، ناشر، محرر، مدير موقع.

كل دور يكون مرتبط بمجموعة مختلفة من الأحداث، مثل إضافة محتوى جديد ومراجعة وتعديل المحتوى وإزالة المحتوى ...الخ.

7-9-2- رسائل خطأ واضحة وذات معنى

ينبغي على المؤسسات الحكومية الالتزام بالممارسات التالية لضمان تقديم رسائل خطأ واضحة وفعّالة ضمن مواقعها الإلكترونية:

1. تفادي حدوث أخطاء تظهر للمستخدمين أثناء الصيانة الدورية للموقع، وذلك من خلال التخطيط الجيد وجدولة أعمال الصيانة وتنبيه المستخدمين مسبقًا عند الحاجة.
2. عدم إزالة أو نقل أي صفحة دون تصحيح جميع الروابط التي تشير إليها، لتجنب ظهور رسائل خطأ غير ضرورية وضمان استمرارية الوصول للمحتوى.
3. إعداد رسائل خطأ تقدم شرحًا واضحًا للمستخدم دون تضمين أي معلومات فنية قد تُستغل في محاولات اختراق الموقع أو تهديد أمنه.

7-9-3- الطباعة

1. في حال كانت البيانات مترابطة وتتبع لنفس الموضوع لكنها موزعة على أكثر من صفحة، يجب توفير خيار طباعة كافة المحتويات عبر وثيقة واحدة، مثل ملف PDF يمكن تحميله وطباعته.
2. ينبغي أن يكون خيار الطباعة سهل الوصول والاستخدام، مع ضمان تنسيق المحتوى بشكل مناسب للطباعة، بحيث يحافظ على وضوح المعلومات وترتيبها.

تلميح خاص بطباعة صفحات الويب

عند إضافة خاصية طباعة مقال أو محتوى من صفحة الويب، يمكن الاستفادة من إمكانيات CSS لتنسيق المخرجات الورقية بما يتوافق مع الهوية الرسمية للجهة العامة .يتيح CSS التحكم الكامل في مظهر الصفحة عند الطباعة من خلال تخصيص خطوط، ألوان، أحجام، وإخفاء أو إظهار عناصر محددة.

8- أدلة استرشادية للمحتوى

يجب على المؤسسات الحكومية التأكد من أن المعلومات المنشورة على مواقعها الإلكترونية هي معلومات موثوقة وذات مصداقية.

8-1- إرشادات المحتوى

لتحقيق الفعالية في التواصل عبر الإنترنت، يجب الالتزام عند إعداد النصوص والمواد الرقمية باتباع الإرشادات التالية، لكي يصبح المحتوى أكثر جذبًا وفعالية، ويحقق أهداف التواصل الرقمي بكفاءة أعلى.

8-1-1- إنشاء المحتوى

عند إنشاء وعرض المحتوى، يجب مراعاة ما يلي:

1. بناء بنية معلومات واضحة بحيث تقتصر كل صفحة على عرض مفهوم واحد.
2. استخدام كلمات رئيسية مميزة في العناوين والفقرات لتعزيز وضوح المحتوى وجاذبيته.
3. اعتماد نفس مبادئ الكتابة المطبقة على الوثائق المطبوعة، خاصة من حيث الصيغ والمصطلحات، مع شرح المصطلحات المعقدة أو إدراج روابط لصفحات توضيحية.
4. توخي الدقة لتفادي نشر معلومات متضاربة من قبل مؤلفين مختلفين.
5. إضافة المحتوى بكافة اللغات المدعومة من الموقع، مع الحفاظ على نفس أسلوب الكتابة ومستوى التفصيل. عند الاكتفاء بلغة واحدة، يجب كتابة العنوان بجميع اللغات المدعومة مع ملاحظة توضح اللغة المتوفّر بها المحتوى.

8-1-2- أسلوب الكتابة

1. استخدام لغة عربية بسيطة وواضحة، وتجنب الاختصارات والمصطلحات والكلمات المعقدة.
2. التزام الموضوعية والمهنية في الصياغة، وتجنب اللهجات الهجومية.
3. استخدام عناوين رئيسية وفرعية لتنظيم النص وتسهيل تصفحه.
4. تخصيص كل فقرة لفكرة واحدة وعدم الخروج عن نطاقها.
5. استخدام علامات الترقيم الصحيحة وأدوات التعداد أو الترقيم النقطي حسب الحاجة.

8-1-3- تنسيق النص

يجب مراعاة الملاحظات التالية بما يخص تنسيق النص:

1. تحسين قابلية القراءة عبر ضبط محاذاة النص إلى اليمين للغة العربية وإلى اليسار للإنجليزية، مع استثناء الحالات الخاصة.
2. استخدام نمط الخط الغامق للتأكيد على العبارات المهمة.
3. تجنب وضع خط تحت النص حتى لا يُخلط بينه وبين الروابط التشعبية.
4. تجنب استخدام النص الملون لما قد يسببه من صعوبة في القراءة أو التباس مع الروابط، خاصة لدى من يعانون من عمى الألوان.
5. استخدام الخط المائل عند الإشارة إلى الوثائق المنشورة مثل التقارير والقوانين والسياسات.
6. مراعاة عرض معلومات التاريخ والوقت وأرقام هواتف التواصل والموقع الفيزيائي حسب الموقع الجغرافي للمستخدمين عند الحاجة.

8-1-4- تنظيم المحتوى

1. تنسيق المحتوى بشكل منظم باستخدام عناوين فرعية، فقرات قصيرة، وقوائم تعدادية عند الحاجة.
2. توظيف لغة مباشرة وسهلة الفهم، مع إبراز الأفكار الرئيسية بوضوح.
3. مراجعة وتدقيق النص للتأكد من صحة الهجاء وسلامة الأسلوب.
4. باتباع هذه الإرشادات، يصبح المحتوى أكثر جذبًا ووضوحًا وفعالية، ويحقق أهداف التواصل الرقمي بكفاءة أعلى.

8-2- متطلبات النشر على الانترنت

للتأكد من أن المحتوى مناسب للنشر عبر الويب يجب اتباع ما يلي:

1. الكتابة بإيجاز.
2. جعل النص سهلًا وسريع القراءة.
3. استخدام لغة عربية بسيطة.
4. استخدام اللغة العربية أو الإنجليزية حسب الجمهور المستهدف (مثل مواقع القنصليات أو السفارات السورية في الخارج).
5. مراعاة الجمهور المستهدف، خاصة فيما يتعلق بإمكانيات الوصول للموقع، مثل إمكانية تعديل حجم الخط من الواجهة بسهولة.

8-3- المعلومات المنشورة

يجب أن تكون الوثائق المنشورة مناسبة ومكتوبة بشكل واضح، خالية من التعقيد والغموض. ويُفضّل استخدام الرسومات بشكل معتدل، نظرًا لتأثيرها المحتمل على وقت تحميل الصفحة.

8-4- جودة المحتوى

لضمان أن المحتوى المنشور على الموقع الإلكتروني هو محتوى عالي الجودة، دقيق، وحديث، يجب وضع إجراءات عمل واضحة تشمل ما يلي:

1. تعيين مسؤول لكل خدمة أو مورد معلومات، سواء كان فردًا أو وحدة تنظيمية، يتحمل مسؤولية جودة المعلومات ودقتها وتحديثها في الوقت المناسب وبشكل مستمر.
2. وضع جدول زمني دوري لمراجعة المحتوى وتحديثه بناءً على التغيرات في السياسات أو المعلومات الجديدة.
3. اعتماد آليات تدقيق ومراجعة المحتوى قبل النشر، تشمل مراجعة لغوية وفنية لضمان الدقة والوضوح.
4. استخدام أدوات وتقنيات لمراقبة جودة المحتوى، مثل فحص الروابط، التحقق من صحة البيانات، وتحليل تفاعل المستخدمين.
5. تعريف الجمهور المستهدف بدقة من خلال دراسات وبيانات تحليلية، وتحديد احتياجاتهم ومتطلباتهم لتوجيه المحتوى بما يتناسب معهم.
6. توفير قنوات تواصل مع الجمهور لجمع الملاحظات والاقتراحات لتحسين المحتوى.

9- إمكانيات الوصول

دمج عناصر التصميم الشائعة مثل الألوان والعلامات والشعارات والأنماط في صفحات الويب يجب أن يتم بطريقة احترافية ومتسقة لتحسين تجربة المستخدم وتعزيزها.

9-1- التشجيع على تصفح الموقع الإلكتروني

يجب أن تتيح المواقع الإلكترونية الحكومية الوصول إلى محتوى الموقع ووظائفه لجميع المستخدمين.

ولضمان وصول المستخدمين إلى الموقع الحكومي، على الجهات الحكومية التأكد مما يلي:

1. اعتماد إرشادات الوصول إلى محتوى الويب (WCAG) التي طورها اتحاد W3C، حيث تغطي هذه الإرشادات مجموعة واسعة من التوصيات لجعل محتوى الويب أكثر سهولة في الوصول إلى شريحة أوسع

من المستخدمين، بما في ذلك ذوي الإعاقة (ضعاف البصر، الصم، الإعاقات السمعية، صعوبات الكلام، الحساسية للضوء، وغيرها).

2. يجب ألا تحتوي أي من صفحات الموقع على نص أو مكونات وامضة.
3. يجب عدم استخدام أي مكونات غير شائعة قد تحتاج برامج/مكونات أخرى لتتم معالجتها وقد تعيد توجيه المستخدمين إلى مواقع إلكترونية أخرى لتنزيل هذه البرامج.

9-2- البيانات الوصفية METADATA

البيانات الوصفية (metadata) هي بيانات منظمة تصف خصائص موقع الويب وصفحاته، مثل العنوان، والوصف، والكلمات المفتاحية، واسم المؤلف، وتاريخ النشر وغيرها. تساعد خصائص البيانات الوصفية روبوتات محركات البحث في فهرسة وجمع البيانات ضمن الموقع الحكومي، مما يمكّنها من تحديد المصطلحات التي ستظهر في نتائج البحث.

9-2-1- إرشادات عامة لاستخدام البيانات الوصفية

يجب أخذ الإرشادات التالية بعين الاعتبار عند وصف وإدارة وحفظ المعلومات المنشورة على الويب:

1. استخدام البيانات الوصفية لوصف المعلومات المنشورة على الويب بهدف تحسين ظهور هذه الموارد وقابليتها للاكتشاف عبر محركات البحث.
2. الاستفادة من البيانات الوصفية في حفظ السجلات الإلكترونية وإدارتها، وضمان استمرار الوصول إليها مع مرور الوقت.
3. تطبيق البيانات الوصفية العامة، مثل "الكلمات الرئيسية (keywords)" و"الوصف (description)"، حيث تتم فهرستها من قبل غالبية محركات البحث التجارية.
4. الحرص على استخدام أكبر عدد ممكن من عناصر البيانات الوصفية الإضافية اللازمة لتعزيز وصف الموارد وتعظيم إمكانية اكتشافها.

9-3- تحسين ظهور الموقع ضمن نتائج محركات البحث (SEO)

لتحقيق أفضل النتائج في تصدر نتائج البحث وزيادة الزيارات الفعالة للمواقع الحكومية، يجب تطبيق الإرشادات التالية:

1. تأكد من فهرسة كامل الموقع: يجب إعداد خريطة موقع ديناميكية (Dynamic XML Sitemap) تُحدَّث تلقائيًا مع إضافة أي محتوى جديد، وتُرسل دوريًا لمحركات البحث مثل Google و Bing. كما ينبغي

ضبط ملف robots.txt للسماح بالزحف إلى جميع الصفحات المهمة، بما في ذلك ملفات PDF و المحتوى القابل للتحميل.

2. اختيار الكلمات الرئيسية المناسبة: حدّد الكلمات الرئيسية التي يستخدمها الباحثون للعثور على محتوى الموقع، وادمج معها كلمات مفتاحية طويلة (long-tail keywords) لزيادة فرص الظهور في نتائج البحث المتخصصة. وزّع هذه الكلمات بشكل طبيعي في العناوين والمحتوى والوصف دون حشو أو مبالغة.

3. جودة ودقة المحتوى: احرص على خلو المحتوى من الأخطاء النحوية والإملائية، وحدثه بشكل دوري ليتوافق مع احتياجات الجمهور المستهدف ويعزز ثقة محركات البحث في الموقع. يجب أن يكون المحتوى منظمًا وسهل القراءة باستخدام العناوين الفرعية (H2،H3...)، تقسيم الفقرات، واستخدام الخط العريض والمائل والقوائم المرتبة وغير المرتبة.

4. تحسين عناصر المحتوى الرئيسية:

- استخدم وسوم العنوان (Title Tags) بشكل مناسب، مع تضمين الكلمات الرئيسية في بداية العنوان، والحفاظ على الطول المثالي (50-60 حرفًا)، وجعل كل عنوان فريدًا لكل صفحة.
- استخدم البيانات الوصفية (Meta Description) بشكل موجز وجذاب، تعكس محتوى الصفحة بدقة وتحتوي على الكلمات الرئيسية المهمة (150-160 حرفًا).
- استخدم علامات ترويسة الخط (H1 إلى H6) بشكل منظم، حيث يُخصص H1 لعنوان الصفحة الرئيسي، وتُستخدم H2-H6 للعناوين الفرعية مع تضمين الكلمات الرئيسية عند الحاجة.
- أضف نصًا بديلًا (Alt Text) وصفيًا ودقيقًا للصور، يتضمن كلمات رئيسية ذات صلة، لتحسين فهرسة الصور وظهور الموقع في نتائج البحث.

5. تحسين بنية الموقع والروابط الداخلية: اعتمد استراتيجية ربط داخلي (Internal Linking Strategy) فعالة، تربط الصفحات المهمة ببعضها بطريقة منطقية، مع التركيز على الصفحات ذات الأولوية العالية. يساعد ذلك محركات البحث على الزحف والفهرسة بفعالية، ويعزز تجربة المستخدم.

6. تحسين تجربة المستخدم وسرعة الموقع: احرص على أن يكون الموقع متوافقًا مع الأجهزة المحمولة (Responsive Design)، وحسّن سرعة تحميل الصفحات. المواقع السريعة والمتجاوبة تحصل على ترتيب أعلى في نتائج البحث.

7. تعزيز الأمان: استخدم HTTPS لحماية بيانات المستخدمين، حيث يعتبر ذلك عاملًا إيجابيًا في تصنيف الموقع على محركات البحث.

8. مراقبة وتحليل الأداء: استخدم أدوات التحليل السلوكي (Behavior Analytics Tools) مثل Google Analytics لتحليل سلوك الزوار وتحديد الصفحات التي يخرج منها الزائر بسرعة، ثم تحسينها بناءً على النتائج.

راقب أداء الموقع باستمرار، وحدث الاستراتيجية بناءً على البيانات الفعلية.

10- نواح قانونية

يجب مراعاة الجوانب القانونية التالية عند تطوير وإدارة المواقع الإلكترونية:

10-1- شروط وأحكام موقع الويب

يجب على جميع المؤسسات الحكومية التأكد من أن الشروط والأحكام الخاصة بالموقع تراعي الجوانب التالية:

1. تفاصيل ملكية وتبعية الموقع.
2. سياسة استخدام المحتوى المنشور على الموقع.
3. الاعتبارات القانونية المتعلقة باستخدام الموقع.
4. المسؤولية تجاه مصادر المعلومات الخارجية التي قد تشير إليها بعض الروابط ضمن الموقع.

لا يتم إخلاء المسؤولية بشكل صريح عن محتوى المواقع الإلكترونية الحكومية أخرى، بل تتم الإشارة إلى ملكية جزء معين من المحتوى مع إحالة المستخدمين إلى قنوات التواصل المناسبة ليتمكنوا من إجراء مزيد من الاستفسارات والتعليقات حول هذا المحتوى.

يجب أن تغطي الشروط والأحكام جميع جوانب مجال عمل ومحتوى الموقع، ويجب إتاحة هذه الشروط على الأقل في الصفحة الرئيسية للموقع، ويفضل أن تكون متاحة من جميع صفحات الموقع، سواء عبر تذييل الصفحات أو من خلال رسالة تظهر عند فتح الموقع ليوافق عليها الزائر.

10-2- حقوق الطبع والنشر المحتوى

1. يجب على جميع المؤسسات الحكومية التأكد مما يلي:
2. دعم أي معلومات أو مستندات يتم إتاحتها على الموقع بسياسة حقوق طبع ونشر واضحة تشرح شروط وأحكام استخدامها، مع الإشارة إليها عند إعادة الاستخدام أو الاقتباس من قبل الآخرين.
3. توخي الحذر عند نشر أي معلومات أو مواد تخضع لحقوق نشر خاصة بطرف ثالث، واتباع جميع الإجراءات اللازمة للحصول على إذن مسبق قبل نشر هذه المواد على المواقع الإلكترونية الحكومية.
4. عند نسخ أي منشور أو تقرير من موقع جهة حكومية أخرى، سواء جزئيًا أو كليًا، يجب الإشارة بوضوح إلى عنوان المستند أو التقرير، واسم الجهة الأصلية الناشرة، وسنة النشر.

10-3- سياسة الخصوصية

يجب على الجهات الحكومية ما يلي:

1. توخي الحذر عند جمع المعلومات أو التفاصيل الشخصية حول زوار الموقع، والاكتفاء بجمع البيانات الضرورية فقط لتقديم الخدمة المطلوبة.
2. عرض بيان الخصوصية بشكل بارز على الموقع، بحيث يوضح بوضوح الغرض من جمع المعلومات الشخصية، ونوع البيانات التي يتم جمعها، وكيفية استخدامها، وحقوق الأفراد في ما يتعلق ببياناتهم.
3. اتباع وسائل آمنة عند جمع المعلومات الشخصية عالية الحساسية من الزوار، مثل الحسابات البنكية أو البيانات الصحية، وذلك باستخدام تقنيات التشفير، وضمان سرية وأمان نقل وتخزين هذه البيانات.

ملحق ا- قائمة التحقق لتطوير وتشغيل المواقع الحكومية

تهدف القائمة إلى مساعدة فرق العمل في الجهات الحكومية على ضمان تطبيق جميع المعايير والإرشادات التنظيمية، التقنية، التصميمية، الأمنية، القانونية، والإدارية أثناء مراحل التخطيط، التطوير، التشغيل، والصيانة. تم إعداد البنود بشكل مفصل لتغطي جميع المتطلبات الأساسية والهامشية، بما يضمن جودة المواقع الحكومية، موثوقيتها، سهولة استخدامها، وأمانها، ويحقق تجربة متسقة لجميع المواطنين والمستفيدين.

1. التخطيط والتحليل

- تحديد الأهداف المرجوة من الموقع أو المنصة.
- تحليل الجمهور المستهدف واحتياجاته.
- دراسة المواقع المشابهة واستخلاص أفضل الممارسات.
- تحديد الموارد البشرية والتقنية والمالية.
- وضع خطة عمل وجدول زمني واضح.
- تحديد جهة اتصال رسمية للطوارئ والإبلاغ عن الحوادث الأمنية.

2. البنية والتنظيم

- تخطيط هيكلية الموقع (صفحات، قوائم، روابط داخلية).
- إعداد خريطة موقع (Site Map) نصية و/أو بيانية.
- اختيار اسم نطاق حكومي رسمي وموحّد.
- إبراز الهوية البصرية (الشعار، الألوان، الخطوط) بشكل واضح في جميع الصفحات.
- تضمين معلومات الملكية والتبعية الحكومية في الترويسة والتذييل.
- توفير دليل خدمات وهيكل تنظيمي مفصل ومحدث.
- توثيق إجراءات العمل التنظيمية لكل وحدة إدارية.

3. التصميم وتجربة المستخدم

- تطبيق مبادئ التصميم المتجاوب (Responsive Design) لجميع الأجهزة والشاشات.
- استخدام قوالب تصميم موحدة وتجنب الإطارات (Frames).
- تمييز الروابط وزيارة الروابط السابقة (Visited Links).

- توفير Breadcrumb وقوائم تنقل واضحة.
- دعم الوضع الداكن وخيارات ألوان عالية التباين.
- توفير اختصارات لوحة مفاتيح لذوي الاحتياجات الخاصة.
- اختبار توافق التصميم مع جميع المتصفحات الشائعة.
- تجنب الرسوم المتحركة غير الضرورية أو المشتتة.

4. المحتوى والنشر

- كتابة محتوى واضح، مختصر ، ودقيق، مع مراجعة لغوية وفنية.
- استخدام لغة عربية بسيطة وتوفير ترجمات عند الحاجة.
- تنظيم المحتوى بعناوين رئيسية وفرعية وقوائم نقطية.
- توفير قسم للأسئلة الشائعة (FAQ) وتحديثه دورياً.
- إتاحة نماذج إلكترونية قابلة للتعبئة وسهلة الاستخدام.
- تعيين مسؤول لكل خدمة أو مورد معلومات لمتابعة جودة ودقة وتحديث المعلومات.
- مراجعة وتدقيق النصوص قبل النشر.
- وضع جدول زمني دوري لمراجعة المحتوى.
- توفير قنوات تواصل لجمع الملاحظات والاقتراحات.
- استخدام نصوص بديلة (Alt Text) للصور والوسائط.

5. معايير الوصول (Accessibility)

- الالتزام بإرشادات WCAG لضمان وصول ذوي الإعاقة.
- تجنب النصوص أو المكونات الومّاضة أو غير الشائعة.
- دعم تكبير المحتوى حتى 200% دون فقدان التنسيق.
- اختبار الموقع باستخدام أدوات الوصول الرقمية.

6. الأمان وحماية البيانات

- تحديث البرمجيات ونظام التشغيل والخادم بشكل مستمر.
- تفعيل المصادقة الثنائية (FA2) لحسابات الإدارة.

- استخدام بروتوكولات تشفير حديثة (TLS 1.2 أو أعلى).
- حماية قواعد البيانات وتقييد الصلاحيات.
- تطبيق رؤوس الحماية الأمنية (HTTP Security Headers).
- إجراء نسخ احتياطية دورية واختبار الاسترجاع.
- تفعيل جدار حماية تطبيقات الويب (WAF) ومراقبة الهجمات.
- إجراء اختبارات أمان واختراق دورية قبل وبعد الإطلاق.
- إعداد خطة استمرارية الأعمال والتعافي من الكوارث.
- تقييد الوصول الإداري بعناوين IP محددة أو شبكة آمنة.
- إدارة صلاحيات المستخدمين بدقة وتطبيق مبدأ أقل صلاحية.
- حذف الحسابات والصلاحيات عند مغادرة الموظفين أو انتهاء التعاقد.
- حماية ملفات الربط مع قاعدة البيانات.
- حماية ميزة رفع الملفات (فحص الامتدادات، تغيير الأسماء، منع التنفيذ).
- توثيق جميع العمليات الأمنية والإدارية.

7. إدارة المحتوى والتشغيل

- استخدام نظام إدارة محتوى (CMS) مع تسلسل هرمي للموافقة على النشر.
- تحديد الأدوار والمسؤوليات (منشئ، مراجع، ناشر، مدير).
- مراقبة وصيانة الموقع بشكل دوري (فحص الروابط، مراقبة الأداء، تحديث البرمجيات).
- توفير آلية لتلقي ملاحظات المستخدمين والرد خلال 72 ساعة.
- تدريب الكوادر المسؤولة عن الموقع بشكل مستمر.
- إجراء تدقيق ذاتي دوري للموقع.
- مراقبة البريد الإلكتروني المرتبط بالموقع.

8. السياسات القانونية والإدارية

- نشر سياسة خصوصية واضحة وشروط وأحكام وحقوق النشر في تذييل الموقع.
- الامتثال للقوانين الوطنية ذات الصلة (حماية البيانات، مكافحة الجريمة المعلوماتية...).

- توثيق جميع العمليات والإجراءات الإدارية والفنية.
- تضمين بنود أمنية واضحة في عقود التطوير والدعم الفني.
- استلام الكود المصدري الكامل وبيانات الدخول عند انتهاء التعاقد مع أي جهة تطوير.
- التأكد من وجود ميزانية سنوية مخصصة للصيانة والتطوير.

9. تحسين محركات البحث (SEO) والبيانات الوصفية

- إعداد خريطة موقع ديناميكية وإرسالها لمحركات البحث.
- استخدام بيانات وصفية دقيقة (Meta Tags) وعناوين فريدة لكل صفحة.
- تحسين سرعة الموقع وتجربة المستخدم.
- مراقبة وتحليل الأداء باستخدام أدوات التحليل المناسبة.
- استخدام الكلمات الرئيسية المناسبة وتوزيعها بشكل طبيعي.
- تحسين الروابط الداخلية و استراتيجية الربط.
- تطبيق سياسة robots.txt بشكل صحيح.
- تفعيل شهادة SSL.

10. إدارة الاستضافة والبنية التحتية

- استضافة الموقع داخل سوريا ضمن مركز بيانات حكومي معتمد.
- توقيع اتفاقية مستوى الخدمة (SLA) وعدم الإفشاء (NDA) مع مزود الخدمة.
- تحديث نظام تشغيل الخادم بشكل دوري.
- تقييد الوصول الفيزيائي للخوادم.
- إجراء اختبارات ضغط وتحمل دورية.
- تفعيل التقييد الجغرافي للوصول عند الحاجة.
- مراقبة السجلات (Logs) وحفظها لمدة لا تقل عن 6 أشهر.

11. إيقاف المواقع والأرشفة

- مراجعة دورية لفائدة الموقع واستمراريته.
- أرشفة المحتوى بشكل آمن عند إيقاف الموقع.

- حذف أو تعطيل جميع الحسابات والصلاحيات المرتبطة بالموقع.
- توثيق عملية الإيقاف والأرشفة وتحديث السجلات الرسمية.
- إلغاء الشهادات الرقمية وحذف النطاق وقواعد البيانات عند الإيقاف النهائي.
- توضيح أن المحتوى المؤرشف غير محدث إذا بقي متاحًا على الإنترنت.

12. متفرقات

- توفير معلومات تحميل الوسائط (الحجم، النوع، المتطلبات) للمستخدمين.
- دعم البث المباشر للوسائط إن أمكن.
- توفير خيار طباعة جميع المحتويات ذات الصلة في وثيقة واحدة.
- اختبار إمكانية عمل الموقع بدون JavaScript للوظائف الأساسية.
- منع حفظ ملفات النسخ الاحتياطي داخل مجلد الجذر أو المسارات العامة.
- تضمين آلية واضحة للإبلاغ عن الثغرات الأمنية في الموقع.
- توثيق تسليم واستلام جميع الحسابات وبيانات الدخول عند تغيير الفريق التقني أو انتهاء التعاقد.
- إجراء اختبارات محاكاة لهجمات DDoS عند الحاجة.

ملحق 2- قائمة التحقق الخاصة بالتعاقد مع الشركات، التسليم، والتسجيل مع مركز أمن المعلومات

تستند هذه القائمة إلى متطلبات الدليل الاسترشادي الرسمي، وتهدف إلى ضبط جميع الجوانب المتعلقة بالتعاقد مع الشركات المطورة، إجراءات التسليم والاستلام، والتسجيل والاعتمادية لدى مركز أمن المعلومات في الهيئة الوطنية لخدمات تقانة المعلومات. تهدف البنود إلى حماية حقوق الجهة الحكومية وضمان استمرارية التطوير والصيانة، وتوثيق جميع العمليات، والامتثال الكامل للمعايير الأمنية والتنظيمية الوطنية. توفر القائمة مرجعًا عمليًا لتضمينه في دفاتر الشروط والعقود الحكومية، وتساعد في ضبط العلاقة مع الشركات المطورة وضمان جاهزية المشروع للإطلاق الآمن والفعال.

1. إجراءات التعاقد مع الشركات

- التأكد من التعاقد فقط مع شركات تطوير وليس أفراد مستقلين.
- التحقق من أن الشركة مرخصة رسمياً وتملك سجلًا تجاريًا ساريًا.
- طلب عروض فنية ومالية مفصلة من الشركات.
- مقارنة العروض وفق معايير واضحة وموثقة.
- التأكد من خبرة الشركة في تنفيذ مشاريع مشابهة.
- طلب أمثلة عن أعمال سابقة للشركة.
- تضمين بند في العقد يُلزم الشركة بمعالجة أي ثغرات أمنية تُكتشف خلال فترة الضمان أو الدعم الفني.
- إلزام الشركة بتسليم الكود المصدري الكامل (غير مشفر) وجميع الملفات البرمجية.
- إلزام الشركة بتسليم قواعد البيانات والوثائق التقنية بالكامل.
- توقيع اتفاقية عدم إفشاء (NDA) لضمان سرية المعلومات.
- تضمين بند في العقد يحدد آلية التعاون مع الهيئة الوطنية لخدمات تقانة المعلومات في الفحص الأمني والاعتمادية.
- التأكد من حصول المنصة التي تتضمن معاملات إلكترونية على وثيقة اعتمادية من الهيئة الوطنية لخدمات تقانة المعلومات قبل توقيع العقد.
- تضمين بند يُلزم الشركة بتسليم جميع الحسابات وكلمات المرور ونسخ احتياطية حديثة عند انتهاء التعاقد أو تغيير الفريق التقني.

- تضمين بند يُلزم الشركة بمعالجة الثغرات الأمنية التي تكتشفها الهيئة الوطنية لخدمات تقانة المعلومات خلال فترة الدعم الفني أو الضمان.

2. إجراءات التسليم والاستلام

- استلام الكود المصدري الكامل غير مشفر.
- استلام جميع الوثائق التقنية المتعلقة بالمشروع.
- استلام قواعد البيانات بشكل كامل ومحدث.
- استلام جميع الحسابات المستخدمة أثناء التطوير (لوحات تحكم، استضافة، بريد إلكتروني...).
- تغيير جميع كلمات المرور فور الاستلام وحصرها بالأشخاص المخولين فقط.
- توثيق عملية الاستلام والتسليم بمحضر رسمي موقع من الطرفين.
- التأكد من استلام نسخ احتياطية حديثة من قواعد البيانات والموقع.
- إجراء اختبارات أمنية شاملة (اختبارات اختراق، فحص ثغرات) بالتنسيق مع مركز أمن المعلومات قبل الإطلاق النهائي.
- عدم استلام الموقع أو المنصة أو التطبيق إلا بعد اجتياز جميع الاختبارات الأمنية المطلوبة من الهيئة الوطنية لخدمات تقانة المعلومات.
- التأكد من حذف جميع الحسابات والصلاحيات المتعلقة بالشركة المطورة من بيئة الإنتاج بعد الاستلام النهائي.

3. التسجيل والاعتمادية مع مركز أمن المعلومات

- تسجيل المشروع/الموقع لدى مركز أمن المعلومات في الهيئة الوطنية لخدمات تقانة المعلومات قبل الإطلاق.
- إرسال جميع البيانات والمستندات المطلوبة (بيانات التواصل، الكود المصدري، الوثائق التقنية، خطط الأمن والاستمرارية) إلى المركز.
- إجراء الفحوصات الأمنية والاختبارات اللازمة من قبل المركز والحصول على موافقة خطية بالإطلاق.
- الالتزام بإبلاغ مركز أمن المعلومات عن أي حادث أمني أو اختراق خلال مدة لا تزيد عن 72 ساعة من اكتشافه.

- التعاون الكامل مع الهيئة الوطنية لخدمات تقانة المعلومات في معالجة الثغرات والاستجابة للحوادث الأمنية.
- تحديث بيانات التواصل مع المركز بشكل دوري وتعيين جهة اتصال رسمية للطوارئ.
- الالتزام بإجراء اختبارات أمنية دورية (سنوية على الأقل أو عند كل تغيير رئيسي) بالتنسيق مع المركز.

4. بنود إضافية هامة

- التأكد من وجود ميزانية سنوية مخصصة للصيانة والتطوير الأمني.
- توثيق جميع عمليات التسليم والاستلام عند تغيير الفريق التقني أو انتهاء التعاقد.
- إلزام الشركة المطورة بتقديم الدعم الفني خلال فترة الضمان أو الدعم الفني المنصوص عليها في العقد.
- التأكد من تسليم جميع بيانات الدخول وتغييرها عند انتهاء التعاقد أو تغيير الفريق.
- تضمين بند يُلزم الشركة بتسليم جميع الوثائق التقنية وأدلة التشغيل والصيانة.

الهيئة الوطنية لخدمات تقانة المعلومات

National Authority for IT Services