الهيئة العامة للإتصالات والمعلوماتية
الإدارة العامة للخدمات الإلكترونية

معايير جودة الأنظمة الرقمية

يوليو 2025

معايير جودة الأنظمة الرقمية

اعـداد

قسم المعايير والتصاميم المرجعية

إدارة الاستشارات والتحول الرقمي

إدارة العامة للخدمات الإلكترونية

إشـراف

مدير عام الإدارة العامة للخدمات الإلكترونية

مدير إدارة الاستشارات والتحول الرقمي

إخـراج

إدارة التمكين الإلكتروني

يوليو 2025

الإصدار V1.0

جدول
المحتويات

المقدمة

تتناول هذه الوثيقة مجموعة من المعايير والمبادئ التي يتم إتباعها لضمان جودة وموثوقية الأنظمة الرقمية حيث تضمن هذه المعايير قيام النظام بالوظائف التي صمم من أجلها وسرعة واستجابة النظام الرقمي لإرسال واستقبال المعلومات كما تضمن سهولة الاستخدام وتعزز أمان النظام الرقمي و حماية المعلومات الحساسة من التهديدات المحتملة. كذلك تضمن تشغيل الأنظمة الرقمية ومراقبتها بشكل فعّال.

ما هي معايير الجودة للنظم الرقمية
Quality Standards

تعرف معايير الجودة للنظم الرقمية بأنها مجموعة من القواعد والإرشادات التي توفر وتوضّح المتطلبات، أو المواصفات، أو الخصائص التي يمكن استخدامها وإتباعها ومراعاتها باستمرار لضمان جودة وموثوقية الأنظمة الرقمية وطرق تشغيلها وحمايتها ومراقبة أداءها وتوافقها مع الغرض من تصميمها. كما تُوفّر هذه المعايير للمؤسسات الرؤية والفهم والإجراءات اللازمة لتلبية توقعات أصحاب المصلحة.

أهمية معايير جودة الأنظمة الرقمية

معايير جودة الأنظمة الرقمية تساهم في تحسين الأداء والأمان والموثوقية وقابلية الصيانة، مما يضمن تحقيق أقصى استفادة من التقنيات الرقمية ويساهم في نجاح المؤسسات والشركات على المدى الطويل. كذلك يمثل الالتزام بهذه المعايير آلية شاملة تعزز من كفاءة وفعالية العمليات وتوفر لغة مشتركة لتقييم وتحسين جودة الأنظمة داخل المؤسسة .

١ أهم معايير جودة الأنظمة الرقمية

1 استيفاء المتطلبات
Meeting Requirements

- يجب أن يكون للنظام أهداف محددة بشكل جيد تتماشى مع أهداف العمل واحتياجات المستخدم.
- يجب أن يعالج النظام ويحل المشكلات التي تم تصميمها لمعالجتها بشكل فعال.
- يجب أن يفي النظام بالغرض المطلوب منه ويلبي جميع المتطلبات المحددة له .
- يجب أن يؤدي النظام جميع المهام دون أخطاء ويتم التأكد من ذلك عبر إجراء اختبار قبول العميل (Client Acceptance Testing)

2 معايير تصميم وتنفيذ النظام

Standards for System Design and Implementation

- يجب أن تكون لغة البرمجة المستخدمة والتقنيات المرافقة لتنفيذ النظام مستخدمة على نطاق واسع وذات شعبية وقد أثبتت مكانتها في مجال النظام.
- يجب أن يكون الكود سهل الفهم والقراءة والتعديل.
- ينبغي تنظيم الكود بتقسيمه إلى وحدات منطقية قابلة للفهم وإعادة الاستخدام وتجنب الكود المتشابك أو ما يسمى كود "السباغيتي", مما يسهل من عملية التطوير والوصول الى ما تريد بأسرع وقت.
- يجب إعتماد مبدأ تقسيم النظام إلى طبقات متعددة (Multitier architecture) ما أمكن ذلك، وأن يكون التعامل مع قاعدة البيانات عبر طبقة البيانات Data Tier عند إرسال واستلام البيانات من قواعد البيانات.
- يجب استخدام التعليقات والتوثيق الجيد، وإدارة الأخطاء والاستثناءات بشكل صحيح داخل الكود وتوفير رسائل خطأ ورسائل تحذير واضحة للمستخدم.
- قابلية الاختبار(Testability) : ينبغي أن يمر النظام بالاختبارات التالية للتأكد من الأداء الوظيفي بشكل فعال :

أ - اختبار الوحدة (Unit Testing): ويشمل اختبار مكونات النظام.

ب - اختبار التكامل(Integration Test): يركز على التحقق من أن التفاعل بين مكونات النظام كما هو متوقع.

ج - اختبار النظام (System Testing) : يركز على مدى تلبية النظام لمتطلبات التصميم.

د - اختبار قبول المستخدم أو العميل (Acceptance Testing): يتم إجراؤه لتحديد ما إذا كان النظام يستوفي معايير قبول المستخدمين.

3 قابلية التوسع Scalability

- قدرة البنية التحتية على التعامل مع أحمال ضخمة من تدفق البيانات وقدرتها على الزيادة العمودية (إضافة ذاكرة إضافية، معالجات، ذاكرة تخزينية) والزيادة الأفقية (إضافة خوادم لتوزيع أحمال البيانات).
- قدرة النظام على التكيف والتوسع لمتطلبات مستقبلية مثل زيادة عدد المستخدمين أو إضافة وظائف جديدة.
- يجب أن يكون لدى النظام القدرة على توفير خدماته ببناء آليات لتجاوز الفشل وإنشاء نسخ احتياطية للنظام.

4 تصميم الواجهات screen Design

- التصميم المستجيب (Responsive Design): تصميم واجهة المستخدم وتنسيقها بحيث يتكيف التطبيق مع جميع أنواع الشاشات بمختلف أحجامها، بحيث يتم استخدام تقنيات مثل تخطيط الشبكة المرنة والوسائط المتعددة لتعديل تصميم الواجهة تلقائيًا بناءً على حجم الشاشة.
- التوافق مع المتصفحات والأجهزة المختلفة: يتم اختبار النظام على مجموعة متنوعة من المتصفحات مثل Google, Chrome, Firefox, Mozilla, Safarig , Microsoft Edge وغيرها . بالإضافة إلى اختباره على أجهزة مختلفة مثل الهواتف الذكية والأجهزة اللوحية وأجهزة الكمبيوتر المحمولة والأجهزة المكتبية.
- إتباع معايير ومبادئ تطوير الويب: يجب إتباع المعايير والمبادئ التوجيهية المعترف بها في تطوير الويب، مثل مبادئ وثائق W3C وتوافقية المتصفحات وإمكانية الوصول لضمان تجربة سلسة ومتوافقة.
- يجب أن تتوافر الممارسات الجيدة لتحقيق الأمان في برمجة الأنظمة والتطبيقات والمتمثلة في:

- التحقق من المدخلات (Input Validation) :ينبغي التحقق الجيد من جميع المدخلات التي يتلقاها النظام، للتأكد من صحتها ومطابقتها للتنسيق المتوقع ورفض المدخلات غير المناسبة أو الضارة.
- تنقية البيانات (Data Sanitization) :يجب تنقية البيانات المدخلة لإزالة أي رموز ضارة أو غير مرغوب فيها، مثل النصوص المُهيأة (HTML/JavaScript) أو الاستعلامات المضرة .(SQL Injection) يمكن استخدام وظائف أمان مثل تجزئة HTML وتنقية استعلامات قواعد البيانات (SQL) لتحقيق ذلك .
- التحقق من صحة الجلسة (Session Validation) :يجب التأكد من صحة وسلامة جلسات المستخدم لمنع هجمات اختراق الجلسة (Session Hijacking) ، ويمكن استخدام معرفات جلسة فريدة وآمنة والتحقق من صحتها بشكل دوري، وبمكن ايضاً استخدام آليات تأمين الجلسة مثل التشفير والتوقيع الرقمي.
- إدارة الصلاحيات (Access Control) :يجب تنفيذ نماذج صلاحيات فعالة وتوفير مستويات وأذونات وصلاحيات مختلفة للمستخدمين والأدوار المختلفة، كما يجب التحقق من صحة صلاحيات المستخدم والتأكد من أنه لا يحصل على وصول غير مشروع إلى الموارد أو الوظائف غير المسموح بها.
- تحديث البرمجيات وتطبيق التصحيحات الأمنية بانتظام، كما ينبغي مراقبة وتحديث الإطارات والمكتبات والأدوات المستخدمة في تطوير التطبيقات للحفاظ على أمان النظام وملء الثغرات الأمنية المعروفة.
- حماية قواعد البيانات من الهجمات والاختراقات عن طريق تطبيق إجراءات أمان قوية مثل تجزئة المدخلات، وتحديث برامج قواعد البيانات، واستخدام صلاحيات الوصول المناسبة للمستخدمين.

5 التوثيق Documentation

- توفير وثائق ومستندات شاملة وواضحة تصف وتشرح النظام وطرق استخدامه ووظائفه والمراحل والدورات التي مر بها
(الإعداد، جمع المتطلبات، التحليل، التصميم، التنفيذ، الاختبار، الإطلاق) ومخرجات كل مرحلة بناءً على آلية التنفيذ المتبعة.
- ينبغي توثيق شامل للكود وواجهات البرمجة ومتطلبات التشغيل والتثبيت.
- توثيق تفصيلي لبنية النظام والمكونات والواجهات وانتقال البيانات داخل النظام.

6 الأمان Security

- إتباع إجراءات حماية الهوية والوصول لضمان الوصول المصرح به فقط للمستخدمين المعتمدين.
- يجب حماية النظام من الوصول غير المصرح به أو الاختراقات الأمنية بإتباع أفضل المعايير الموصي بها دوليا في مجال حماية الأنظمة الرقمية.
- يجب تأمين بيانات المستخدمين الشخصية ومعلومات الدفع.
- تأمين النظام أو التطبيق من خلال اعتماد بروتوكولات أمان متقدمة مثل التشفير والتوقيع الرقمي واستخدام بروتوكول HTTPS لتأمين الاتصالات بين المستخدم والخادم، يتم ذلك باستخدام شهادات SSL/TLS الموثوقة وتشفير البيانات المرسلة والمستلمة عبر الشبكة.
- التحقق من الثغرات الأمنية المحتملة وتطبيق إجراءات الوقاية المناسبة.
- ينبغي إجراء اختبارات الضعف واختبارات الاختراق (Vulnerability Testing and Penetration Testing)بشكل دوري لتحديد الثغرات الأمنية والضعف في التطبيقات.

7 التحكم في الوصول Access Control

- استخدام أنظمة للتحقق من الهوية (مثل المصادقة الثنائية) لضمان أن الأشخاص المصرح لهم فقط يمكنهم الوصول إلى النظام.
- تفعيل مبدأ أقل الامتيازات، بحيث يحصل كل مستخدم على الحد الأدنى من الصلاحيات اللازمة لأداء عمله.

8 القابلية للصيانة Maintainability

الصيانة الدورية تحسن أداء النظم حيث إنها تضمن أن جميع المكونات تعمل بشكل صحيح، مما يقلل من الأعطال والأخطاء ويزيد من الإنتاجية،ويترجم ذلك إلى معدلات إنتاج أعلى ومراقبة أفضل للجودة. وتشمل الجوانب التالية :

- سهولة تعديل البرمجيات لتصحيح الأخطاء أو تحسين الأداء.
- وجود توثيق جيد لتسهيل عملية الصيانة .
- تنفيذ اختبارات شاملة للنظام للتحقق من سلامته ووظائفه.

9 التوافقية Compatibility

قدرة التطبيق أو النظام على التعامل مع مختلف البيئات والمنصات والأجهزة بشكل سليم وتشمل:

- توافق التطبيق مع مختلف أنظمة التشغيل مثل : IOS/windows/Android .
- التأكد من أن التطبيق يعمل بشكل سليم مع التقنيات والبرمجيات الأخرى المستخدمة.
- التأكد من أن التطبيق يدعم البروتوكولات والتنسيقات القياسية لتبادل البيانات.
- القدرة على نقل البيانات بسلاسة بين أنظمة أو تطبيقات برمجية مختلفة، مما يضمن بقاء البيانات سليمة وقابلة للاستخدام.

10 آلية تعليقات المستخدمين

User Feedback Mechanism

قدرة النظام على استقبال وتجميع اراء وتعليقات المستخدمين سواء لـــــلإبلاغ عن المشكلات التقنية أو لإقتراح التحسينات ,علي ســــــــــبيل المثـــــال مايـــــــــلي:

- زر الإبلاغ عن مشكلة : يتيح للمستخدم الإبلاغ عن خلل تقني أو خطأ في النظـــــــام.
- الدردشة المباشرة أو الروبوتات التفاعلية (Chatbots) : تفاعل مباشر مع المستخدم لجمع ملاحظاته أو مساعدته.
- رسال الملاحظات عبر البريد الإلكتروني: خيار مرن يسمح للمستخدمين بمشاركة آرائهم أو اقتراحاتهم بشكل مفصل.

11 الموثوقية

Reliability

- تجنب وقوع أخطاء نظامية مثل البيانات المتكررة وتضارب البيانات.
- اختبار ومـراجعة النـظام بانتظام للتحقق من عمله بـــشكل سليم.

12 مراقبة الأداء

Performance monitoring

- يجـب أن تـخـضع الأنـظمة الـرقمية للتـطوير والتـحسين المـستمر بنـــاءً على نتائج قياس مؤشرات الأداء واستبيانات رضا المتعاملين والشكاوى والاقتراحات وأفضل الممارسات العالمية.
- يجب الرصد المستمر لمعالجة المشاكل التقنية على وجه السرعة.

13 إدارة المخاطر
Risk Management

تبني التفكير القائم على إدارة المخاطر، مما يضمن التحديد الاستباقي للمشكلات المحتملة في الأنظمة الرقمية والتخفيف من آثارها واقتراح البدائل.Workarounds

14 نسخ احتياطي للبيانات
Data Backup

- القدرة على عمل نسخ احتياطية منتظمة للبيانات لضمان استعادتها في حال حدوث اختراق أو فشل في النظام.
- يجب تخزين النسخ الاحتياطية في موقع آمن.

15 تحديث الأنظمة
Systems Update

- تحديث البرمجيات والأنظمة بشكل دوري لسد الثغرات الأمنية.
- التحقق من استخدام أحدث الإصدارات من البرامج والأدوات.