السياسات العامة لأمن المعلومات
في الجهات الحكومية

# سياسة تطوير وصيانة الأنظمة والتطبيقات

م / عمار الجحافي

# بنود السياسة

- يجب ان يكون هناك ضمان لأي تصميم أو تطوير أو تطبيق أو اختبار لأنظمة المعلومات بما يتوافق مع متطلبات سياسات أمن المعلومات وخطة أمن المعلومات.
- يجب على فريق تطوير الأنظمة والتطبيقات امتلاك الخطط الأمنية وتنفيذ التدابير الأمنية والضوابط المناسبة للنظام قيد التطوير.
- يجب أن تصان الوثائق وقوائم الأنظمة والتطبيقات بشكل سليم على أن تقيد وفق معايير الحاجة للمعرفة.
- يجب الحفاظ على سلامة الأنظمة والتطبيقات في ظل ضوابط أمنية ملائمة مثل آلية التحكم في الإصدار والفصل بين بيئات التطوير والاختبار والتشغيل.
- تعتبر الدراسات والوثائق والمخططات المتعلقة بتحليل وتصميم أنظمة المعلومات والبرمجيات المراد تطويرها أو صيانتها، والبرمجية المصدرية (الكود المصدري)، وكافة الملفات الخاصة بهذه الأنظمة والبرمجيات معلومات سرية، يجب التعامل معها بالاستناد إلى سياسات تصنيف وحساسية المعلومات وأن تكون ملكاً للجهة وليس لفريق التطوير أو غيره.
- لا يسمح بإجراء أي تغييرات على أنظمة المعلومات والبرمجيات المستخدمة إلا إذا دعت الحاجة لذلك، على أن يتم توثيق ذلك عن طريق عملية ضبط التغيير المتبعة في الجهة الحكومية بالتوافق مع سياسات ضبط التغيير.
- يسمح بتطوير وشراء البرمجيات المطورة خصيصاً للجهة الحكومية عندما يتم ضمانها بدراسة جدوى فعّالة ومدعّمة وبعد اختبار أمنها وفحصها والتأكد من سلامتها.

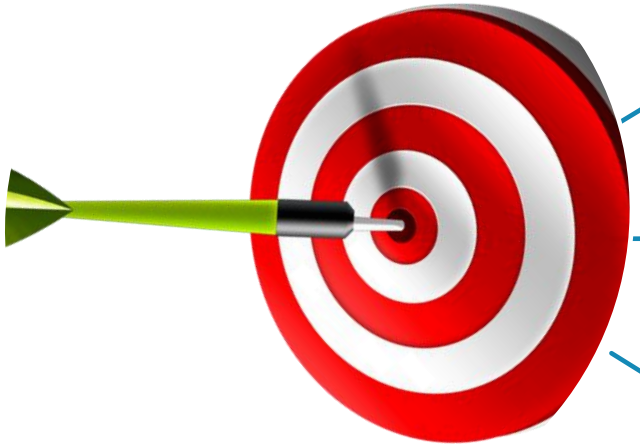
# بنود السياسة

- يجب عند تطوير/اقتناء أي نظم معلومات جديدة أن تختبر أولاً على بيئة خاصة بالتطوير والتجارب إلى أن تحصل على الاعتماد والموافقة بعد نجاحها في تحقيق المؤشرات المطلوبة وخلوها من الثغرات ومن ثم ينتقل العمل على البيئة الفعلية.
- يجب اختبار أي تغييرات خاصة بأنظمة المعلومات أو البرمجيات المستخدمة في الجهة الحكومية بطريقة صحيحة وآمنة من قبل المختصين في الجهة قبل إقرارها ثم إطلاقها.
- لا يسمح باستخدام البيانات الحقيقية قيد الاستخدام عند اختبار الأنظمة قبل وضع ضوابط خاصة لضبط أمن هذه البيانات والمعلومات وسلامتها.
- يجب العمل بأنظمة المعلومات والبرمجيات المستخدمة في الجهة الحكومية بالتوازي مع الأنظمة والبرمجيات المطورة لحين التأكد من مطابقة الأخيرة لمتطلبات العمل ومتطلبات الأمن والحماية التي تم التطوير من أجلها.
- يجب التأكد من تطبيق التحديثات التي تعمل على تقليل درجة المخاطر للأخطاء الناجمة عن المعالجة الداخلية لكي لا تؤدي إلى التأثير سلبًا على سلامة أنظمة المعلومات والبرمجيات أو بياناتها.
- يجب تقييم المخاطر الأمنية للأنظمة من أجل تحديد فيما إذا كانت رسائل التحقق مطلوبة ولتحديد الطريقة الأنسب لتطبيقها.
- يجب استخدام أنظمة التشفير لحماية المعلومات في حال احتمال تعرضها للمخاطر، وعند عدم وجود ضوابط دخول قادرة على حمايتها بشكل كافٍ، وذلك بالتوافق مع سياسات التشفير.

# المقدمة

- يقصد بسياسة تطوير وصيانة الأنظمة والتطبيقات ضمان عملية التطوير والتصميم والاختبار والصيانة مع ما يتلاءم من متطلبات أمن المعلومات.
- فتأمين البرمجيات لا يقتصر على حمايتها عند استخدامها في بيئة التشغيل، لأن عملية الحماية متكاملة خلال دورة حياة البرمجيات بأكملها.
- لذا يجب ضمان حماية البرمجيات سواء عند شرائها أو تطويرها داخل الجهة خلال دورة حياة تلك البرمجيات كاملة Software Development Life Cycle. SDLCمرو راً بجمع المتطلبات، بالتحليل، ثم التصميم، ثم البناء، ثم الفحص، ثم التثبيت وإدخال البيانات، والتشغيل، والترقية والصيانة، والتطوير.

# الاهداف



- تحقيق متطلبات الامن والسلامة
- المساهمة في تحقيق مستوى من التوافق الأمني بين كل الانظمة والخدمات
- ضمان توفر الثقة والأمن والموثوقية في البرمجيات.

# النطاق

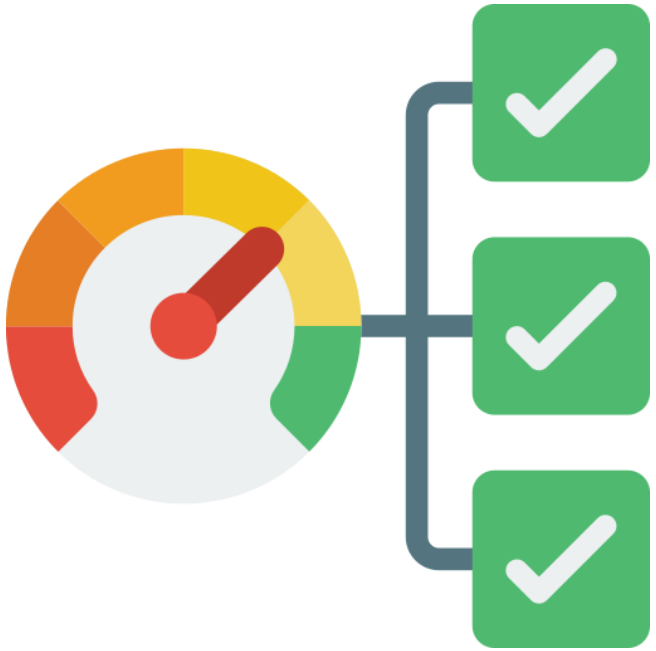
- تطبق هذه السياسة على جميع الأنظمة المعلوماتية والتطبيقات والتجهيزات والمعدات التي يتم صيانتها وبرمجتها وتطويرها سواء بداخل الجهة الحكومية او عن طريق طرف خارجي بما يضمن حمايتها اثناء هذه العملية.
- وكذلك المختصين من محللين ومطورين للأنظمة سواءً داخل الجهة أو خارجها.

# الأدوار والمسئوليات

## ❖ مسئوليات الجهة

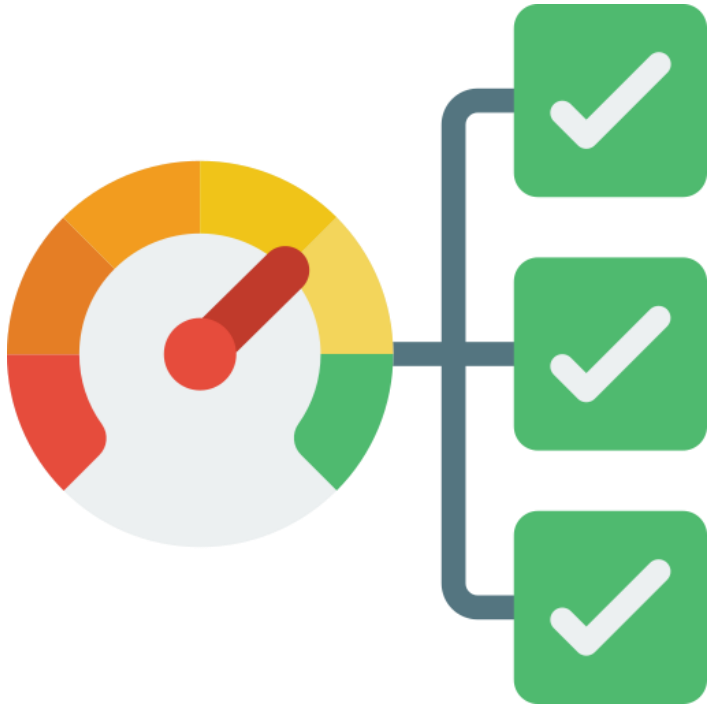
- تلتزم الإدارة العليا في الجهة باعتماد سياسة تطوير وصيانة الأنظمة والتطبيقات.

## ❖ مسئوليات مدير تطوير البرمجيات / مدير نظم المعلومات



- وضع المعايير والضوابط الخاصة بمراحل تطوير وتحديث الأنظمة والبرمجيات
- تحديد متطلبات الحماية المطلوب استخدامها خلال دورة حياة البرمجيات
- تقييم المخاطر التي تنتج عن تطوير وصيانة أنظمة المعلومات والبرمجيات ودرجة تأثيرها على مستوى امن وحماية المعلومات التي يتم معالجتها
- التأكد من اغلاق وعدم وجود قنوات سرية او برمجيات طروادة في أنظمة المعلومات التي يتم تطويرها
- التأكد من الفصل بين المهام لجميع مجالات التطوير المتعلقة بتطوير الأنظمة والعمليات المتعلقة بها
- الموافقة بعد الانتقال من مرحلة لأخرى بعد التأكد من اكتمال المتطلبات والمواصفات الخاصة بأمن المعلومات واختبارها بالشكل السليم

# الأدوار والمسئوليات



## ❖ مسئوليات المطورين

- الالتزام باتباع كافة البنود الواردة في السياسة.
- القيام بتصميم وتطوير التطبيقات والأنظمة وفقًا لمتطلبات أمن المعلومات.
- التعامل مع تحسين الأداء وتصحيح الأخطاء وتوفير التحديثات الضرورية.
- توثيق جميع مراحل التطوير والوثائق والدراسات والخطط الخاصة بتطوير واختبار الأنظمة وتأمينها.

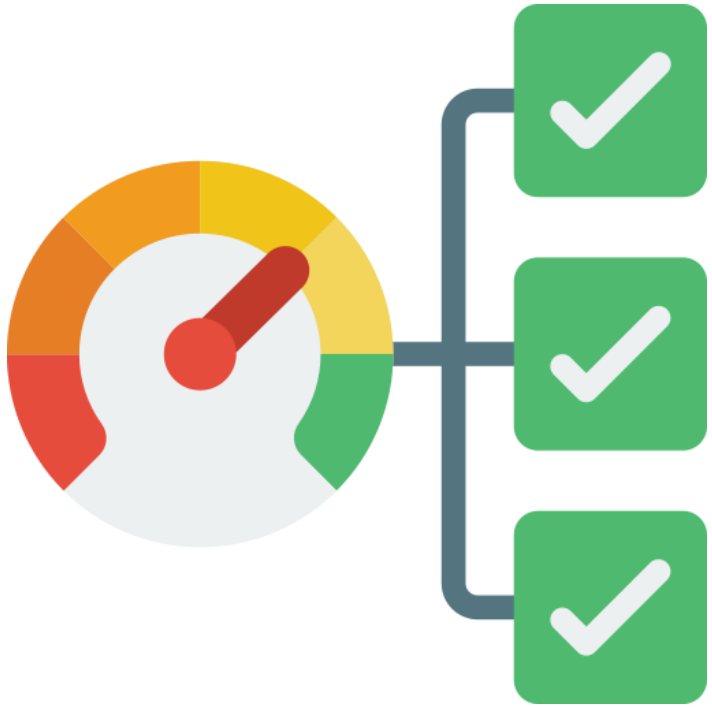
## ❖ مسئوليات مسؤول أمن المعلومات

- يضمن أمان التطبيقات والأنظمة من خلال تقديم إرشادات ومراجعات أمنية.
- يقوم بتحليل وتقييم الثغرات الأمنية ويعمل على تصحيحها.
- يتحقق من جودة وأداء التطبيقات والأنظمة.
- يضمن تنفيذ اختبارات الاداء والتصحيح اللازم للأخطاء والعيوب.

# الأدوار والمسئوليات

## ❖ مسئوليات مسؤول قاعدة البيانات

- التأكد من تنفيذ ممارسات أمان قواعد البيانات مثل تقييد الوصول إلى البيانات وتطبيق مبادئ الحماية عند إدارة قواعد البيانات التي تستخدمها التطبيقات والأنظمة وذلك عبر تقييد الوصول إلى البيانات وتطبيق مبادئ الحماية ورصد ومراقبة الأنشطة على قواعد البيانات لاكتشاف أي نشاط غير مصرح به للمحافظة على أمن البيانات.
- تنفيذ استراتيجيات النسخ الاحتياطي والاستعادة بمراعاة أمن المعلومات.



# انتهى،،،