منشآت
monsha'at
الهيئة العامة للمنشآت الصغيرة والمتوسطة
Small & Medium Enterprises General Authority

مركز الابتكار

كتيّب

منهجية تضمين الأمن السيبراني في المشاريع البرمجية

إعداد
د. ماجدة وزان

Thakaa_center Thakaacenter

سياسة الاستخدام

إن المعلومات الواردة في هذا التقرير جُمِعَت ونُسِّقت بجهود موظفي مركز ذكاء التابع للهيئة العامة للمنشآت الصغيرة والمتوسطة "منشآت"، ولا ينبغي لقارئها أن يعمل بها دون مشورة مناسبة من المتخصصين.

للمزيد من المعلومات، نرجو التواصل معنا على البريد الإلكتروني: **support@thakaa.sa**

تقوم المنشآت بمختلف أحجامها بالعمل على عدد من المشاريع التقنية والتي يتم إدارتها من قبل المختصين في المنشأة وتحتاج إدارة هذه المشاريع إلى تطبيق عدد من متطلبات الأمن السيبراني وتضمينها خلال دورة حياة المشاريع بهدف زيادة مستوى نضج الأمن السيبراني. ومع تزايد التوقعات نحو استمرار توافر الخدمات وشفافية تجربة المستخدمين، وكذلك فاعلية حماية الأنظمة والبيانات الحساسة، أصبح تعزيز الأمن السيبراني أمراً في غاية الأهمية لزيادة الثقة في المنشأة وخدماتها وسلامة وصمود بنيتها التحتية.

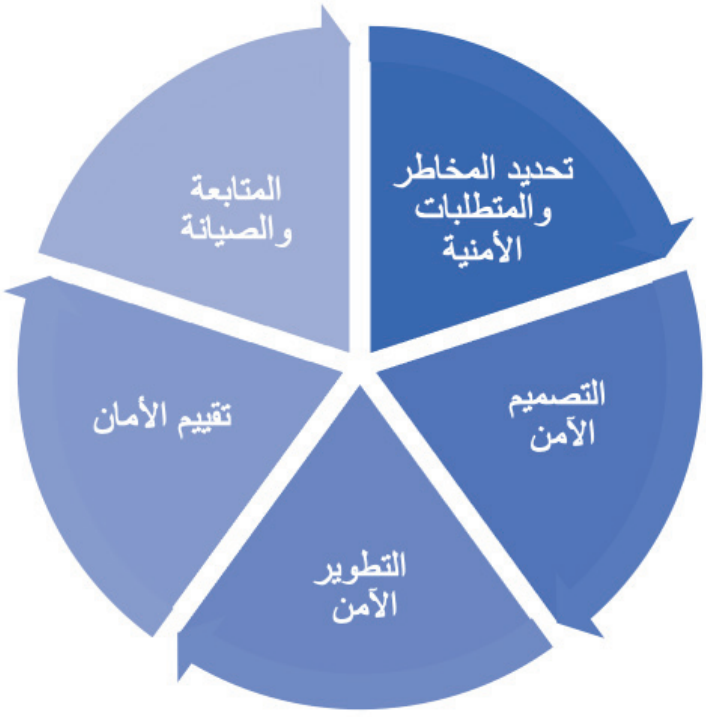
إن تضمين الأمن السيبراني في المشاريع هو عملية تلبية متطلبات الأمن السيبراني واستيفاءها خلال دورة حياة المشروع، وهذا الأمر من شأنه أن يدعم حماية القيمة التي يقوم المشروع بخلقها، حماية الأصول المرتبطة بدورة حياة المشروع، التغيير الآمن في عمليات المشروع ، السيطرة على المخاطر وإدارتها بشكل ملائم إضافة إلى الالتزام بالتشريعات والأنظمة ذات العلاقة بالأنظمة والبيانات.

ومما لا شك فيه أن المشاريع البرمجية تمثل أحد الركائز الأساسية في النمو الاقتصادي فهي توفر القدرة التنافسية من خلال الخدمات الإلكترونية التي تقدمها وارتباط المستخدمين بها.
وعندما يتعلق الأمر بمشاريع البرمجيات، يعد الأمن السيبراني أمراً حاسماً لضمان سلامة البيانات وحماية التطبيقات والمستخدمين. إن تضمين الأمن السيبراني في المشاريع البرمجية يتطلب اتباع منهجية شاملة تضمن تحقيق أعلى مستويات الأمان.

في هذا الكتيب، سنستعرض منهجية من خمس مراحل رئيسية لتضمين الأمن السيبراني في المشاريع البرمجية وهي كالتالي:

تحديد المخاطر والمتطلبات الأمنية، التصميم الآمن، التطوير الأمن، تقييم الأمان والمتابعة والصيانة

كما سنقوم بتوضيح كل مرحلة من مراحل هذه المنهجية بشكل مفصل مع ذكر أمثلة توضح كيفية العمل على هذه المراحل



شكل 1 : منهجية تضمين الأمن السيبراني في المشاريع البرمجية

مراحل منهجية تضمين الأمن السيبراني في المشاريع البرمجية

المرحلة الأولى: تحديد المخاطر والمتطلبات الأمنية

تبدأ المنهجية بعملية تحليل وتحديد المخاطر المحتملة وتحديد متطلبات الأمان للمشروع. ينبغي أن يشارك فريق التطوير وفريق الأمن السيبراني في هذه العملية. يتضمن ذلك تحليل المخاطر وتقييم التهديدات المحتملة التي يمكن أن تواجه المشروع، مثل هجمات الاختراق وتسريب البيانات والقرصنة. يجب توثيق المخاطر وتحديد الأهداف الأمنية الرئيسية التي يجب تحقيقها.

إن تحديد المخاطر والمتطلبات الأمنية في المشاريع البرمجية يتطلب إجراء تحليل شامل للأمان. فيما يلي بعض الخطوات التوضيحية التي يمكن اتباعها لتحقيق ذلك:

1. تحديد أصول البيانات:

حدد البيانات والموارد الهامة التي تحتاج إلى الحماية. قد تشمل هذه الأصول قواعد البيانات، والملفات، والمعلومات الحساسة، والبيانات الشخصية للمستخدمين، وأي موارد أخرى ذات قيمة للمشروع.

2. تحليل التهديدات

قم بتحديد التهديدات المحتملة التي قد تؤثر على أمن المشروع البرمجي. يمكن أن تشمل التهديدات الشائعة هجمات الاختراق، والبرمجيات الخبيثة، وسرقة الهوية، والاختراقات الداخلية، وغيرها من التهديدات المحتملة.

3. تحليل الثغرات:

قم بتحليل الثغرات المحتملة في التصميم والتطوير البرمجي. فحص النقاط الضعيفة المحتملة في النظام والتطبيقات والبرمجيات المستخدمة. يمكن استخدام تقنيات مثل فحص الشبكات، وفحص الثغرات، وتحليل الشفرة المصدرية لتحديد الثغرات الأمنية المحتملة.

4. تحديد المتطلبات الأمنية:

استناداً إلى تحليل الثغرات المحتملة، حدد المتطلبات الأمنية اللازمة لحماية المشروع البرمجي. يمكن أن تشمل هذه المتطلبات استخدام التشفير، وتوفير آليات التوثيق، وتنفيذ التحقق من الهوية، وتطبيق إجراءات الوصول المناسبة، وتنفيذ نظم الكشف عن الاختراق والحماية ضد الفيروسات، وغيرها من المتطلبات الأمنية الضرورية. يمكن الاستعانة بقائمة التحقق من متطلبات الأمن السيبراني في تطوير البرمجيات، سياسة ومعيار التطوير الأمن لتطبيقات الويب، سياسة دورة حياة تطوير البرمجيات الآمنة.

5. توثيق المخاطر والمتطلبات:

يجب توثيق جميع المخاطر المحددة والمتطلبات الأمنية في وثيقة أمان المشروع. ينبغي أن تكون هذا الوثيقة مرجعاً لفريق التطوير وفريق الأمن السيبراني للتأكد من تنفيذ الإجراءات الأمنية المناسبة.

باستخدام هذه الخطوات، يمكن لفريق المشروع تحديد المخاطر والمتطلبات الأمنية الخاصة بالمشروع البرمجي. يجب أن يستمر هذا التحليل والتقييم على مدار مراحل التطوير للتأكد من متابعة الأمان وتحديثه بشكل منتظم. كما ينبغي أن يشارك فريق الأمن السيبراني في عملية تحديد المخاطر وتحديد المتطلبات الأمنية للحصول على رؤى وخبرات الفريق المهنية وضمان تنفيذ أفضل الممارسات الأمنية في المشروع البرمجي.

المرحلة الثانية: التصميم الآمن

بناءً على التحليل الأمني، يجب تضمين التصميم الآمن منذ بداية المشروع. يتضمن ذلك تحديد البنية الأمنية للتطبيقات والنظم والبيانات المرتبطة بالمشروع. يجب أن يتم مراعاة العديد من الجوانب الأمنية، مثل ضمان تحقيق متطلبات التوثيق والتحقق من الهوية والتشفير. ينبغي أن يتم مراجعة التصميمات الأمنية من قبل فريق الأمن السيبراني لضمان الالتزام بالمعايير والممارسات الأمنية القياسية.

إن العمل على التصميم الآمن في المشاريع البرمجية يشمل اتخاذ إجراءات وتطبيق مبادئ الأمن السيبراني في جميع جوانب التصميم. فيما يلي بعض النصائح العامة لعمل تصميم آمن في المشاريع البرمجية:

1. **مبدأ الدفاع في العمق:** يتضمن هذا المبدأ فصل وتجزئة النظام إلى مكونات مختلفة وتخطيط طبقات الأمن المتعددة. يجب أن يكون هناك طبقات متعددة من الحماية للوقاية من أي اختراقات محتملة. على سبيل المثال، يمكن تقسيم التطبيق إلى طبقة عرض البيانات، وطبقة منطق الأعمال (business logic)، وطبقة قاعدة البيانات، وتطبيق إجراءات الحماية المناسبة في كل طبقة.

2. **التحقق من الهوية وإدارة الوصول:** قم بتصميم آليات التحقق من الهوية وإدارة الوصول للتحكم في حقوق الوصول إلى الموارد والبيانات الحساسة. على سبيل المثال يجب تحديد من يمكنه الوصول إلى ما وكيف يتم ضبط الصلاحيات والتحقق من صحة الهوية.

3. **تحديد تقنيات التشفير والحماية:** حدد تقنيات التشفير لحماية البيانات الحساسة أثناء التخزين والنقل. يجب تصميم النظام لدعم بروتوكولات التشفير الآمنة والسماح بتطبيقها بشكل صحيح.

4. **التخطيط للتدقيق والمراقبة:** قم بتصميم نظام التدقيق والمراقبة لتسجيل الأنشطة والأحداث المهمة في المشروع. يساعد هذا في اكتشاف أي أنشطة غير مرغوب فيها أو غير مصرح بها وتتبعها.

5. **إدارة الثغرات وتحديث البرامج:** قم بالتخطيط لعمليات إدارة الثغرات وتحديث البرامج. يتضمن ذلك تحديث البرمجيات وإصلاح الثغرات الأمنية المعروفة وتنفيذ التحديثات الأمنية اللازمة.

6. **التدريب والتوعية الأمنية:** قم بتوعية فريق التطوير والمستخدمين بمبادئ الأمن السيبراني والممارسات الجيدة. يجب أن يكون فريق التطوير على دراية بمخاطر الأمن السيبراني المتعلقة بالمشروع وكيفية التعامل معها بشكل صحيح.

7. **المراجعة الأمنية:** قم بإجراء مراجعات أمنية دورية للتحقق من أن جميع التدابير الأمنية المطبقة لا تزال فعالة وتلبي المتطلبات الأمنية المحددة. يجب أن تشمل هذه المراجعات فحص التغييرات الجديدة في التصميم وتقييم تأثيرها على أمن المشروع.

هذه بعض النصائح لعمل تصميم آمن في المشاريع البرمجية. ينبغي أن يتم تخصيص وتطبيق المبادئ والتقنيات الأمنية وفقاً لاحتياجات ومتطلبات المشروع. يجب أيضاً العمل بشكل مستمر على تحديث وتحسين التصميم الآمن بمرور الوقت وتكامل المزيد من الخبرات والممارسات الأمنية المتقدمة.

المرحلة الثالثة: التطوير الآمن

تشمل هذه المرحلة ممارسات التطوير الآمنة التي يجب على فريق التطوير اتباعها. ينبغي تنفيذ الضوابط الأمنية المناسبة التي تم الاتفاق عليها واعتمادها في المرحلة السابقة أثناء عملية البرمجة وتطوير التطبيقات. ينبغي تعزيز الوعي بالأمن السيبراني بين أعضاء الفريق وتوفير التدريب المناسب حول مفاهيم الأمن وأفضل الممارسات. يجب أيضاً تنفيذ إجراءات الفحص والاختبار أثناء التطوير للتحقق من سلامة البرمجيات وكشف الثغرات الأمنية وإصلاحها.إن العمل على التطوير الآمن في المشاريع البرمجية يشمل اتخاذ إجراءات وتطبيق ممارسات الأمان خلال عملية التطوير.

فيما يلي بعض النصائح لعمل تطوير آمن في المشاريع البرمجية:

1. مراجعة تقييم المخاطر:

قم بمراجعة تحليل وتقييم المخاطر الأمنية المحتملة أثناء تطوير مشروعك البرمجي. تأكد من النقاط الضعيفة المحتملة والتهديدات الأمنية وقيِّم تأثيرها واحتمالية حدوثها. استند إلى هذا التقييم لتوجيه جهودك في تنفيذ الإجراءات الأمنية اللازمة.

2. تطبيق مبادئ التصميم الآمن:

قم بتطبيق مبادئ تصميم آمن أثناء تطوير التطبيق. اعتبر الأمان كعامل أساسي في عملية التصميم وحاول تجنب الثغرات الأمنية الشائعة مثل ثغرات حقن البرمجيات (Injection) وتعددية الجوانب (Cross-Site Scripting) والتصيد (Phishing). واستخدم مبادئ فصل المسؤوليات وتنفيذ التحقق من الهوية وإدارة الوصول بشكل صحيح.

3. تنفيذ التدقيق الأمني:

قم بتنفيذ التدقيق الأمني دورياً لتحديد الثغرات الأمنية والضعف في التطبيق. يمكن استخدام أدوات التحليل الثابتة والديناميكية لتحديد الثغرات الشائعة مثل الثغرات في التحقق من الإدخالات والإخراجات وتحقق من قواعد الأمان والتحقق من الهوية وغيرها. يتعين إصلاح الثغرات المكتشفة بسرعة ومراجعة الأمان بشكل مستمر.

4. تنفيذ الاختبار الأمني:

قم بتنفيذ اختبارات أمان شاملة للتأكد من سلامة التطبيق من الهجمات الخارجية. يمكن استخدام اختبار الاختراق واختبار الضغط واختبار الثغرات لتحديد الثغرات الأمنية المحتملة وتحسين التصميم والتنفيذ.

5. إدارة التحديثات والثغرات

قم بتحديث البرمجيات والمكتبات المستخدمة بانتظام لضمان استخدام الإصدارات الأحدث والأكثر أماناً. قم بمراجعة الثغرات الأمنية المعروفة وتطبيق التصحيحات والتحديثات الأمنية اللازمة فور توفرها.

6. إدارة الشهادات والمصادقة

قم بإدارة الشهادات الأمنية والمصادقة بشكل صحيح. استخدم شهادات توقيع البرمجيات (Code Signing) للتحقق من هوية المطور وأصالة البرمجيات. قم بتنفيذ آليات المصادقة القوية مثل التحقق الثنائي لتعزيز أمان الوصول إلى التطبيق.

7. الحفاظ على سرية البيانات:

قم بتطبيق تدابير الحماية المناسبة للحفاظ على سرية البيانات المستخدمة في التطبيق. استخدم تقنيات التشفير المناسبة لحماية البيانات في النقل وفي التخزين. ولضمان خصوصية البيانات تأكد من الرجوع لقانون حماية البيانات الشخصية.

المرحلة الرابعة: تقييم الأمان

بعد الانتهاء من تطوير المشروع، يجب إجراء تقييم أمان شامل. يهدف التقييم الأمني إلى اكتشاف الثغرات الأمنية الجديدة والتأكد من فعالية الإجراءات الأمنية المتبعة. يجب توثيق نتائج التقييم والعمل على إصلاح الثغرات المكتشفة قبل الانتقال إلى المرحلة التالية. إن عمل تقييم الأمان في المشاريع البرمجية يساهم في تحسين جودة وأمان التطبيقات والنظم البرمجية وتقليل المخاطر الأمنية المحتملة. ويهدف إلى تحديد الثغرات الأمنية وتقييم مدى قوة إجراءات الأمان المطبقة. يمكن اتباع الخطوات التالية لعمل تقييم الأمان في المشاريع البرمجية:

1. **تحديد معايير التقييم:** قم بتحديد المعايير التي ستستخدمها لتقييم الأمان. يمكن أن تشمل هذه المعايير المعايير العامة للأمان مثل OWASP Top 10 ، قم بتوضيح المعايير والمتطلبات المطلوبة بوضوح لضمان الفهم الصحيح للفريق.

2. **تقييم التهديدات والمخاطر:** قم بتحليل وتحديد التهديدات الأمنية التي تواجه المشروع البرمجي. قد تشمل هذه التهديدات الاختراق الهجمات الخارجية، وتهديدات التطبيق الداخلية، وثغرات الأمان المحتملة في البرمجيات المستخدمة. قم بتصنيف التهديدات حسب مستوى التأثير واحتمالية حدوثها.

3. **إدارة الثغرات بعد اطلاق التطبيق:** قم بإنشاء عملية إدارة الثغرات للتعامل مع الثغرات الأمنية التي يتم اكتشافها بعد إطلاق التطبيق. يمكن استخدام أدوات الاختبار التلقائي للتحقق من الثغرات الشائعة مثل ثغرات حقن البرمجيات (Injection) وتعددية الجوانب (Cross-Site Scripting) والتصيد (Phishing). يجب توثيق وتحليل وحل الثغرات المكتشفة بشكل منتظم للحفاظ على أمان التطبيق على المدى الطويل. استخدم أدوات الرصد والتحليل لتحديد أي أنماط أو ثغرات أمنية جديدة واتخاذ الإجراءات اللازمة لتحسين الأمان. من الأفضل الاستعانة بأنظمة مسح الثغرات.

4. **تقييم الحماية الحالية:** قم بتقييم مدى فعالية إجراءات الأمان المعمول بها حالياً في المشروع. هل تتوافق مع المعايير المطلوبة والتي تم اعتمادها في مرحلة التصميم؟ هل تغطي جميع التهديدات الأمنية المحتملة؟ قم بتحليل الثغرات المكتشفة في الخطوة السابقة وتقييم مدى تأثيرها على أمان المشروع.

5. **تطبيق التحسينات:** استناداً إلى الثغرات المكتشفة وتقييم الحماية الحالية، قم بتحديد التحسينات التي يجب تنفيذها. يمكن أن تشمل هذه التحسينات تحسينات في التصميم الأمني، وتحديثات البرمجيات والتصحيحات، وتعزيز سياسات ومعايير الأمن السيبراني وإجراءاته.

6. **إعداد تقرير مفصل وشامل:** قم بتوثيق نتائج تقييم الأمان والتحسينات المطلوبة في تقرير مفصل. هذا يمكن أن يشمل الثغرات المكتشفة، والتوصيات لتحسين الأمان، وجدول زمني لتنفيذ التحسينات، وتوضيح أي تأثير قد يكون له ذلك على جدول المشروع والموارد المطلوبة لتنفيذ التحسينات.

يجب ملاحظة أن تقييم الأمان للمشاريع البرمجية يجب أن يتم بواسطة خبراء في مجال الأمن السيبراني جنباً إلى جنب مع قادة المشروع الذين يفهمون الجوانب التقنية ومنطق الأعمال للمشروع. قد يستدعي الأمر أحياناً الاستعانة بشخص خبير من جهة خارجية متخصصة في تقييم الأمان للحصول على وجهة نظر مستقلة وموثوقة.

المرحلة الخامسة: المتابعة والصيانة

بعد تطبيق التحسينات وتصحيح الثغرات، يجب متابعة الأمان السيبراني للمشروع على المدى الطويل. ينبغي تنفيذ إجراءات الصيانة الدورية وتحديثات الأمان للتأكد من استمرارية الحماية. يجب أيضاً مراجعة وتحديث سياسات الأمان والإجراءات بناءً على التهديدات الجديدة والتطورات التكنولوجية.
هذه المرحلة تعتبر جزءاً هاماً لضمان استمرارية النظام البرمجي وتحسينه على مر الوقت. فيما يلي خطوات عامة يمكن اتباعها لعمل المتابعة والصيانة في المشاريع البرمجية:

1. إنشاء فريق صيانة:

قم بتشكيل فريق مختص بالصيانة يتألف من مطورين ومهندسين لضمان توافر المهارات اللازمة لإدارة وصيانة النظام البرمجي. يجب أن يكون للفريق واجبات ومسؤوليات واضحة.

2. إدارة الأعطال وتصحيح الأخطاء:

قم بتوثيق الأعطال والأخطاء التي يتم الإبلاغ عنها من المستخدمين أو من خلال عمليات التحقق الداخلية. قم بتحليل وتصنيف هذه الأخطاء حسب مستوى الأولوية وتأثيرها على النظام البرمجي. ثم قم بتصحيح الأخطاء واختبار التصحيحات للتأكد من حلها بشكل صحيح.

3. تحسين الأداء:

قم بمراقبة أداء النظام البرمجي وتحليله لتحديد أي مشاكل أداء محتملة. قد تشمل هذه المشاكل زمن الاستجابة البطيء، استهلاك موارد غير فعال، أو حدود السعة التي يمكن أن تتسبب في تعطل النظام. قم بتطبيق التحسينات اللازمة لتحسين الأداء وتعزيز استجابة النظام.

4. التحديثات والتطويرات:

قم بتقييم احتياجات التحديث والتحسين في النظام البرمجي. قد تتضمن هذه التحديثات إصلاحات أمان، وإصلاحات أخطاء، وتحسينات وظيفية جديدة. قم بإدارة عملية التطوير والاختبار والنشر لضمان تحديث النظام بشكل سليم ودون إحداث أي تأثيرات سلبية.

5. إدارة التغييرات:

قم بتطبيق إجراءات إدارة التغييرات لضمان توثيق ومراقبة أي تغييرات تتم على النظام البرمجي مع مراعاة متطلبات الأمن التي تم توثيقها مسبقاً واعتمادها. يجب تحديد المتطلبات الأمنية وتحديد المخاطر المحتملة لكل تغيير، واختباره ومراجعته قبل تطبيقه بشكل فعلي.

6. الدعم الفني والتواصل:

- قدم الدعم الفني للمستخدمين والعملاء المتعلق بالنظام البرمجي.
- استجب للاستفسارات والمشاكل وقدم الحلول والتوجيه للمشكلات الفنية.
- قم بإنشاء آليات للتواصل مع المستخدمين مثل نظام تذاكر الدعم إضافة إلى الإبلاغ عن الحوادث الأمنية.

7. توثيق وتحديث الوثائق:

قم بتوثيق النظام البرمجي وتحديث الوثائق بشكل منتظم. يجب أن تكون الوثائق واضحة وشاملة لتسهيل فهم وصيانة النظام في المستقبل

8. مراجعة الأداء وتقييم الجودة:

قم بإجراء مراجعات دورية لأداء الفريق ونتائج الصيانة. قم بتحليل البيانات وقياس الأداء وتحسين العمليات الداخلية لضمان استقرار التطبيق ولتحقيق أعلى مستوى من الجودة وكفاءة الصيانة.

هذه الخطوات التي يمكن اتباعها في مرحلة المتابعة والصيانة في المشاريع البرمجية. يجب أن تتكيف هذه الخطوات مع طبيعة وحجم المشروع ومتطلبات الصيانة الخاصة به.

مصادر هامة

توفر الهيئة الوطنية للأمن السيبراني العديد من الأدوات المتعلقة بالأمن السيبراني في المشاريع البرمجية وتشمل سياسات ومعايير ووثائق حوكمة حيث يمكن الاطلاع عليها من هنا. وفيما يلي توضيح مبسط لأهم هذه الأدوات والتي يمكن الاستفادة منها لتحقيق الالتزام بضوابط الأمن السيبراني المتعلقة بالمشاريع البرمجية

- **قائمة التحقق من متطلبات الأمن السيبراني في تطوير البرمجيات**

تهدف هذه القائمة التي تم إعدادها من قبل الهيئة الوطنية للأمن السيبراني إلى تحديد متطلبات الأمن السيبراني التي تنطبق على أنشطة تطوير البرمجيات حيث أن تنفيذ هذه المتطلبات يساعد في تطوير برمجيات آمنة وإصدارها للمستخدمين النهائيين بشكل سليم والحفاظ على توافر الأصول والمعلومات وسلامتها وسريتها.

- **سياسة دورة حياة تطوير البرمجيات الآمنة**

الغرض من هذه السياسة هو تحديد متطلبات الأمن السيبراني المتعلقة بدورة حياة تطوير البرمجيات الآمنة (SSDLC) . حيث تهدف السياسة إلى وضع البنود المناسبة التي تحكم عملية تطوير الأنظمة والبرمجيات للحد من احتمالية وقوع هجمات الأمن السيبراني بسبب عدم ملائمة التصميمات أو الوظائف. حيث أن دعم الممارسات الجيدة لدورة حياة تطوير البرمجيات الآمنة (SSDLC) ضمن عمليات إدارة مشاريع تقنية المعلومات والتغييرات يساعد في الحد من عدد الثغرات في تصميمات وإعدادات الأنظمة وحزم البرمجيات والتخفيف من آثارها وعلاج الأسباب الأساسية لها.

- **معيار التطوير الآمن للتطبيقات**

يهدف هذا المعيار إلى تحديد متطلبات الأمن السيبراني التفصيلية لحماية تطوير البرمجيات والتطبيقات وذلك لتحقيق الغرض الأساسي وهو تقليل المخاطر السيبرانية الناتجة عن التهديدات الداخلية والخارجية.

- **معيار حماية تطبيقات الويب**

تحديد متطلبات الأمن السيبراني التفصيلية المتعلقة بحماية تطبيقات الويب الخارجية لتقليل مخاطر الأمن السيبراني وحمايتها من التهديدات الداخلية والخارجية.

- **معيار الأمن السيبراني للبيانات**

الغرض من هذا المعيار هو تحديد متطلبات الأمن السيبراني التفصيلية المتعلقة بحماية البيانات. ويهدف هذا المعيار إلى تحديد مجموعة من ضوابط الأمن السيبراني للتأكد من حماية البيانات الخاصة بالأصول المعلوماتية.

مما تقدم شرحه أعلاه تتضمن منهجية تضمين الأمن السيبراني في المشاريع البرمجية كما ذكرنا خمس مراحل وهي على الترتيب كالآتي: تحديد المخاطر والمتطلبات الأمنية، التصميم الآمن، التطوير الأمن، تقييم الأمان و المتابعة والصيانة. يجب أن يكون الأمن السيبراني عملية مستمرة تتطلب التعاون والتنسيق بين فرق التطوير وفريق الأمن السيبراني لضمان حماية فعالة للمشاريع البرمجية والبيانات الحساسة
هذه النصائح بمثابة اتجاهات لتنفيذ التطوير الآمن في المشاريع البرمجية. ومع ذلك، يجب الأخذ في الاعتبار أن كل مشروع قد يحتاج إلى اهتمام خاص بناءً على طبيعته ومتطلباته الخاصة.

شكراً