تطبيق تدريبي لنظام إدارة أمن المعلومات (ISMS)

By Hessa Albaqami

ملخص تنفيذي(Executive Summary)

في ظل تزايد التهديدات السيبرانية المعقدة، يُعد تطبيق نظام إدارة أمن المعلومات (ISMS) ضرورة استراتيجية لضمان حماية سرية، سلامة، وتوافر معلومات الشركات الحيوية. يوضح هذا المستند تطبيق ISMS في شركةSecureStart Solutions ، مركّزًا على تحديد النطاق، صياغة سياسة أمن المعلومات، تقييم المخاطر وخطط المعالجة، وبيان الضوابط الأمنية، وفقًا لمتطلبات المعيار الدوليISO/IEC 27001:2022 ، مما يعكس التزام الشركة بأعلى معايير الحوكمة الأمنية.

تعريف المصطلحات الأساسية(Glossary)

- ISMS نظام إدارة أمن المعلومات.(Information Security Management System)
- Annex A المرفق أ في معيار ISO/IEC 27001 يحتوي على قائمة الضوابط الأمنية.
- SLA اتفاقية مستوى الخدمة.(Service Level Agreement)
- MFA التحقق المتعدد العوامل.(Multi-Factor Authentication)
- DDoS هجوم حجب الخدمة الموزع.(Distributed Denial of Service)
- CIA Triad ثلاثي السرية، السلامة، والتوافر.(Confidentiality, Integrity, Availability)

إطار زمني للتطبيق والمراجعة(Timeline & Review)

- يتم مراجعة وتحديث وثائق ISMS بشكل دوري كل 12 شهرًا أو عند حدوث تغييرات كبيرة في بيئة العمل أو اللوائح التنظيمية.
- يتم إجراء تقييم المخاطر سنويًا، مع تحديث خطة المعالجة حسب النتائج.
- تتضمن خطة التنفيذ مراحل واضحة مع جداول زمنية للمراقبة والمتابعة.

أمثلة عملية وأدوات مستخدمة(Practical Examples & Tools)

- تقييم المخاطر :استخدام أدوات مثلNessus ، OpenVAS لفحص الثغرات الأمنية.
- مراقبة الدخول والأنظمة :نظام SIEM مثل Splunk أو Elastic Stack لتحليل سجلات الأنظمة والتنبيهات الأمنية.
- التوعية والتدريب :منصات تدريب إلكترونية مثل KnowBe4 لرفع وعي الموظفين بالأمن السيبراني.
- حماية البريد الإلكتروني :استخدام فلاتر متقدمة مثل Proofpoint أو.Microsoft Defender for Office 365

ربط الضوابط بأهداف أمن المعلومات(Link Controls to CIA Triad)

الضابط	الهدف الأمني	شرح مختصر
تفعيل التحقق المتعدد العوامل (MFA)	السرية(Confidentiality)	يمنع الوصول غير المصرح به للحسابات

الضابط	الهدف الأمني	شرح مختصر
جدران الحماية وأنظمة كشف التسلل	التوافر والسلامة (Availability & Integrity)	تحمي الشبكة من الهجمات وتحافظ على استمرارية الخدمة
تشفير البيانات	السرية والسلامة	يحمي البيانات من الاطلاع والتعديل غير المصرح به

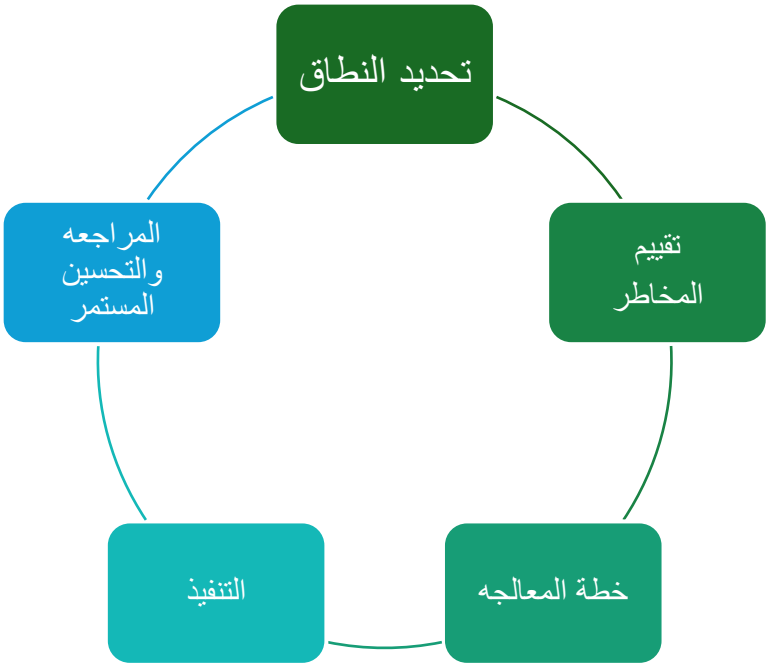
التعامل مع الحوادث الأمنية (Incident Management)

تم وضع إجراءات واضحة للإبلاغ عن الحوادث الأمنية والاستجابة السريعة لها، تشمل:

- تحديد الحادث وتوثيقه.
- تقييم التأثير.
- اتخاذ إجراءات احترازية لتقليل الضرر.
- مراجعة الحادث وتحديث الضوابط لتجنب تكراره.

ISMS (ISMS Lifecycle Diagram)

مقترح تخطيطي بسيط يوضح المراحل:



الدروس المستفادة والتوصيات (Lessons Learned & Recommendations)

- التحديات :صعوبة تغطية كامل المتطلبات في وقت محدود، وأهمية مشاركة الجميع من موظفين وإدارة.
- التوصيات:
  - البدء بنطاق واضح ومحدد.

- تدريب مستمر للموظفين على الوعي الأمني.
- تحديث دوري للسياسات والخطط.
- الاستثمار في أدوات أتمتة المراقبة والاستجابة.

صياغة الأهداف الأمنية بشكل واضح (Clear Security Objectives)

- السرية :(Confidentiality) حماية المعلومات من الوصول غير المصرح به.
- السلامة :(Integrity) ضمان دقة وسلامة البيانات ومنع التعديل غير المصرح به.
- التوافر :(Availability) ضمان توفر المعلومات والخدمات للمستخدمين المخولين عند الحاجة.

أهمية وهدف بيان قابلية التطبيق (Statement of Applicability - SoA)

هذا البيان يوضح الضوابط الأمنية المطبقة أو المستثناة ضمن نظامISMS ، مع مبررات واضحة. يساعد SoA في:

- توضيح التزام الشركة بمعايير الأمن.
- تسهيل المراجعة الداخلية والخارجية.
- تحديد النقاط التي تحتاج تطوير أو مراجعة مستمرة.

ISMS Scope Document — المرحلة 1

اسم الشركة: **SecureStart Solutions** شركة ناشئة متخصصة في تطوير وتشغيل تطبيقات الأعمال السحابية.

تاريخ الإصدار 11 **:**أغسطس 2025
الإصدار: 1.0
اعتمدها :الإدارة العليا

---

1. مقدمة

يهدف هذا المستند إلى تحديد نطاق نظام إدارة أمن المعلومات (ISMS) في شركةSecureStart Solutions ، بما يتوافق مع متطلبات المعيار الدولي .ISO/IEC 27001:2022 يضمن هذا النطاق حماية المعلومات الحيوية والأصول التقنية للشركة وعملائها من المخاطر الأمنية المحتملة.

---

2. نطاق النظام: (Scope)

يشمل نطاق ISMS جميع الأنشطة، العمليات، والأنظمة التقنية المتعلقة بتطوير، استضافة، وإدارة خدمات الشركة السحابية، بما في ذلك:

- البنية التحتية السحابية المستضافة على .**AWS**
- أنظمة البريد الإلكتروني الرسمية عبر .**Google Workspace**
- مستودعات الأكواد المصدرية الخاصة على .**GitHub**
- أنظمة إدارة علاقات العملاء.**(CRM)**
- البيانات المخزنة والمعالجة ضمن بيئة الإنتاج السحابية.

يُستثنى من النطاق :الأجهزة الشخصية للموظفين والأنظمة غير المرتبطة بشكل مباشر بخدمات العملاء.

---

3. الأصول الأساسية: (Assets)

1. بيانات العملاء.
2. الأكواد المصدرية للتطبيقات.
3. حسابات الخدمات السحابية وأذوناتها.
4. البريد الإلكتروني الرسمي.
5. وثائق وسياسات الشركة الداخلية.

---

4. الأطراف المعنية: (Stakeholders)

- **الإدارة العليا :**مسؤولة عن اعتماد السياسات وتوفير الموارد.
- **الفريق التقني :**مسؤول عن تنفيذ الضوابط الأمنية في التطوير والتشغيل.
- **العملاء :**يعتمدون على خدمات الشركة لحماية بياناتهم.
- **مزودو الخدمات**AWS : Google، ومزودو الطرف الثالث.

---

5. المتطلبات القانونية والتعاقدية:

- الالتزام بالقوانين المحلية لحماية البيانات الشخصية.
- الالتزام بالاتفاقيات الموقعة مع العملاء.(SLAs)
- الالتزام بشروط وأحكام مزودي الخدمات السحابية.

المرحلة 2 — Information Security Policy

---

1. الغرض:

تهدف سياسة أمن المعلومات إلى حماية سرية، سلامة، وتوافر المعلومات والأصول التقنية الخاصة بالشركة وعملائها، وضمان إدارة المخاطر الأمنية بطريقة منهجية وفعّالة.

---

2. النطاق:

تسري هذه السياسة على جميع الموظفين، المتعاقدين، والجهات الخارجية التي لها حق الوصول إلى أصول أو بيانات الشركة، سواء داخل أو خارج مقر العمل.

---

3. الأهداف:

- **السرية :(Confidentiality)** منع الوصول غير المصرح به إلى المعلومات.
- **السلامة :(Integrity)** منع التغيير غير المصرح به للمعلومات أو الأنظمة.
- **التوافر :(Availability)** ضمان إتاحة المعلومات والخدمات عند الحاجة.

---

4. المبادئ الأساسية:

- الالتزام المستمر بتحديد وتقييم ومعالجة مخاطر أمن المعلومات.
- تطبيق ضوابط أمنية مناسبة تتماشى مع متطلبات.ISO/IEC 27001:2022
- تعزيز وعي الموظفين حول ممارسات الأمن السيبراني.
- مراجعة وتحديث هذه السياسة بشكل دوري أو عند حدوث تغييرات جوهرية.

---

5. الأدوار والمسؤوليات:

- **الإدارة العليا :**اعتماد السياسة، توفير الموارد، دعم التنفيذ.
- **مسؤول أمن المعلومات :(ISO)** الإشراف على تنفيذ ومراقبة النظام.
- **جميع الموظفين :**الالتزام بالسياسة والإبلاغ عن أي حوادث أمنية.

---

6. المراجعة:

تُراجع هذه السياسة سنويًا أو عند حدوث تغييرات في بيئة العمل أو المتطلبات التنظيمية.

المرحلة 3 — تقييم المخاطر وخطة المعالجة(Risk Assessment & Treatment Plan)

1. مقدمة

يهدف هذا القسم إلى تحديد وتقييم المخاطر الأمنية المحتملة على أصول المعلومات الحيوية في الشركة، وتحديد الإجراءات المناسبة لمعالجتها وتقليل تأثيرها بما يتوافق مع متطلبات ISO/IEC 27001:2022.

2. منهجية التقييم:

- **تحديد الأصول (Assets):** التعرف على كل الأصول الرقمية والبيانات المهمة.
- **تحديد التهديدات (Threats):** المخاطر التي قد تؤثر على الأصول.
- **تقييم الاحتمالية (Likelihood):** مدى احتمال وقوع التهديد (منخفض، متوسط، عالي).
- **تقييم التأثير (Impact):** مدى خطورة تأثير التهديد إذا تحقق (منخفض، متوسط، عالي).
- **تحديد مستوى المخاطر (Risk Level):** بناءً على الاحتمالية والتأثير.
- **خطة المعالجة (Treatment Plan):** الإجراءات الأمنية التي تقلل أو تتجنب المخاطر.

3. جدول تقييم المخاطر:

الأصل / العملية	التهديد	الاحتمالية	التأثير	مستوى الخطر	خطة المعالجة / الضوابط المقترحة
قاعدة بيانات العملاء	الوصول غير المصرح به	متوسط	عالي	عالي	تفعيل التحقق المتعدد العوامل، وتسجيل الدخول والمراقبة
نظام البريد الإلكتروني	هجمات التصيد الاحتيالي	عالي	متوسط	عالي	تدريب الموظفين على الوعي الأمني، واستخدام فلتر البريد العشوائي
خوادم التطبيقات	هجوم رفض الخدمة (DDoS)	متوسط	متوسط	متوسط	تفعيل جدران الحماية وأنظمة كشف التسلل
مستودعات الأكواد	تسرب الأكواد المصدرية	منخفض	عالي	متوسط	تقييد الوصول، واستخدام التحكم في النسخ والإصدارات
الأجهزة المحمولة للموظفين	فقدان الجهاز أو سرقته	متوسط	متوسط	متوسط	تشفير البيانات، وتمكين مسح البيانات عن بُعد

المرحلة 4 — بيان قابلية التطبيق(Statement of Applicability - SoA)

---

1. مقدمة

يحدد هذا البيان الضوابط الأمنية المطبقة في نظام إدارة أمن المعلومات لدى الشركة، مع مبررات تطبيقها أو استثنائها، وفقًا للمعيار ISO/IEC 27001:2022 - Annex A.

---

2. جدول ضوابط قابلة للتطبيق:

الضابط(Annex A)	مطبق؟ (نعم/لا)	مبرر التطبيق / الاستثناء
A.5.1 Information Security Policies	نعم	تم توثيق السياسة واعتمادها من الإدارة العليا
A.6.1 Organization of Information Security	لا	غير مناسب لحجم الشركة الحالي
A.7.2 User Awareness and Training	نعم	تدريب الموظفين مستمر لتعزيز الوعي بالأمن
A.8.1 Asset Management	نعم	جرد وتوثيق الأصول بشكل دوري
A.9.2 User Access Management	نعم	تطبيق مبدأ الأقل امتيازًا للتحكم في الوصول
A.10.1 Cryptographic Controls	لا	لم يتم تطبيقه بعد، لكنه مخطط للتنفيذ في المرحلة القادمة
A.11.1 Physical Security	نعم	مراقبة دخول المكاتب والتجهيزات الأمنية الفيزيائية
A.12.2 Protection from Malware	نعم	استخدام برامج مكافحة الفيروسات وتحديثها بشكل دوري
A.13.1 Network Security Management	نعم	جدران حماية وأنظمة كشف التسلل مُفعّلة
A.14.2 Security in Development and Support	نعم	تطبيق إجراءات أمنية في دورة حياة تطوير البرمجيات
A.15.1 Supplier Relationships	نعم	تقييم ومراقبة مزودي الخدمة لضمان الالتزام الأمني
A.16.1 Management of Information Security Incidents	نعم	آلية للإبلاغ والاستجابة للحوادث الأمنية
A.17.1 Business Continuity Management	لا	خطة استمرارية الأعمال قيد التطوير

الضابط(Annex A)	مطبق؟ (نعم/لا)	مبرر التطبيق / الاستثناء
A.18.1 Compliance with Legal Requirements	نعم	مراجعة دورية للامتثال للقوانين واللوائح

الخاتمة:

هذا المستند هو انتاج عملي الشخصي المبني على فهم عميق لمتطلبات معيار ISO/IEC 27001:2022 ، وتجربة عملية في تصميم وتنفيذ نظم إدارة أمن المعلومات المتكاملة. يهدف هذا المشروع إلى إظهار قدرتي المهنية على بناء إطار أمني شامل ومتكامل، قادر على حماية الأصول الرقمية والمعلومات الحساسة لأي مؤسسة ناشئة في بيئة سحابية متطورة مثل SecureStart Solutions.

من خلال هذا العمل، أثبت مهاراتي في تحليل المخاطر، وضع السياسات الأمنية، وتطبيق الضوابط العملية التي تضمن التزام الشركة بأفضل ممارسات الأمن السيبراني، مع القدرة على التكيف والتطوير المستمر بما يتوافق مع متطلبات السوق والتقنيات الحديثة.

أسعى دائماً لتطبيق هذه المعرفة في واقع العمل، لتحقيق تحسينات ملموسة في أمن المعلومات واستمرارية الأعمال بالمؤسسات.