

حقيبة تدريبية

حماية البيانات وتعزيز الثقة في الخدمات الرقمية الحكومية

(Protecting data and enhancing confidence in government digital services)



دليل المتدرب

لا يجوز نسخ أو إعادة نشر الوثيقة أو أي من محتوياتها لأي غرض دون موافقة خطية من صاحب حقوق الطبع

جميع الحقوق محفوظة لصالح البورد الدولي الخليجي للجودة

/http://www.b2bpartnership.com

mail to: Info@b2bpartnership.com-

(+20) 01285323438 / (+966) 551715783



قال تعالى :

{وَقُلِ اعْمَلُوا فَسَيَرَى اللَّهُ عَمَلَكُمْ وَرَسُولُهُ وَالْمُؤْمِنُونَ ۖ وَسَتُرَدُّونَ إِلَىٰ عَالِمِ الْغَيْبِ وَالشَّهَادَةِ فَيُنَبِّئُكُم بِمَا كُنتُمْ تَعْمَلُونَ}

التوبة (١٠٥)

الفهرس

م	الموضوعات	ص
١	المقدمة	١٣
٢	تعريف حماية البيانات وأهميتها في القطاع الحكومي	١٥
٣	التحديات الأمنية التي تواجه الخدمات الرقمية الحكومية	١٦
٤	القوانين المستخدمة في حماية البيانات الدولية والمحلية	١٨
٥	أنواع التهديدات الأمنية	٢٢
٦	المفاهيم المتعلقة بالأمن السيبراني	٢٤
٧	أفضل الممارسات الأمنية لحماية البيانات	٢٦
٨	مبادئ بناء الثقة الرقمية	٢٩
٩	أمثلة على ممارسات ناجحة لبناء الثقة	٣١
١٠	استراتيجيات حماية البيانات في الخدمات الرقمية الحكومية	٤٠
١١	كيفية تقييم المخاطر الأمنية	٤٣
١٢	كيفية تنفيذ سياسات حماية البيانات	٤٥
١٣	كيفية إدارة الوصول والتحكم في البيانات	٤٨
١٤	ممارسات حماية البيانات	٥٠
١٥	طرق وأساليب التدقيق والرقابة على بيانات المستخدمين	٥٢
١٦	التشفير وتقنيات الحماية	٥٦
١٧	نظم إدارة الهوية والوصول (IAM).	٥٩
١٨	أدوات مراقبة الأمن السيبراني	٦٣
١٩	الذكاء الاصطناعي في حماية البيانات	٦٨

٢٠	التقنيات الحيوية والبيانات الحيوية	٧٠
٢١	البلوك تشين وحماية البيانات	٧٢
٢٢	أهمية مشاركة الجمهور في بناء الثقة	٧٧
٢٣	أهمية التواصل مع الجمهور حول حماية البيانات	٧٩
٢٤	أساليب التواصل الفعالة حول حماية البيانات	٨٢
٢٥	كيفية الرد على استفسارات الجمهور حول حماية البيانات	٨٤
٢٦	ورشة عمل تطبيقية "خطوات وإجراءات حماية البيانات الرقمية الحكومية" (نشاط ٩)	٨٧
٢٧	المراجع والمصادر	٨٩

كلمة الترحيب بالحضور

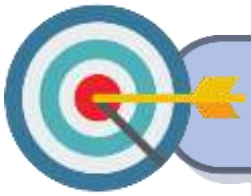
أخي المشارك، نرحب بك معنا فى هذا البرنامج التدريبي، ويسعدنا أن نبدأ معك هذا البرنامج التدريبي الذي نرجو أن تكتسب من خلاله مهارات وخبرات جديدة في مجـال عملـك،

- ✓ فكن مستمعاً جيداً لاكتساب المعلومة التي نود أن تصل إليك.
- ✓ وكن مناقشاً جاداً لاكتساب مهارة التفاعل مع البرنامج .
- ✓ وكن متدرباً نشطاً لاكتساب مهارة الممارسة الجيدة .

وذلك في ضوء مفهومنا للعمليات التدريبية وهو :

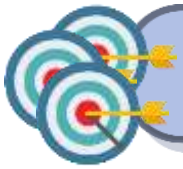
إكسـاب المعرفة والمهارات المتميـزة .

Gulf International Board for Quality
البورد الدولـي الخليجي للجودة



الهدف العام من الحقيبة

تهدف هذه الحقيبة إلى اكساب المتدربين المعارف والمهارات والتوجهات اللازمة لحماية البيانات الرقمية وتعزيز الثقة في الخدمات الرقمية الحكومية.



الأهداف التفصيلية للحقيبة

- التعرف على مفهوم حماية البيانات وأهميتها في القطاع الحكومي.
- التمييز بين التحديات الأمنية التي تواجه الخدمات الرقمية الحكومية.
- الإلمام بالقوانين المستخدمة في حماية البيانات الدولية والمحلية.
- التمييز بين أنواع التهديدات الأمنية.
- التعرف على المفاهيم المتعلقة بالأمن السيبراني.
- الإلمام بأفضل الممارسات الأمنية لحماية البيانات.
- إدراك مبادئ بناء الثقة الرقمية.
- التعرف على أمثلة على ممارسات ناجحة لبناء الثقة.
- الإلمام باستراتيجيات حماية البيانات في الخدمات الرقمية الحكومية.
- إدراك كيفية تقييم المخاطر الأمنية.
- التعرف على كيفية تنفيذ سياسات حماية البيانات.
- إدراك كيفية إدارة الوصول والتحكم في البيانات.
- الإلمام بممارسات حماية البيانات في مختلف مراحل دورة حياة الخدمة.
- التعرف على طرق وأساليب التدقيق والرقابة على بيانات المستخدمين.
- الإلمام بمجال التشفير وتقنيات الحماية.
- التعرف على نظم إدارة الهوية والوصول (IAM).
- التمييز بين أدوات مراقبة الأمن السيبراني.
- إدراك دور الذكاء الاصطناعي في حماية البيانات.

- التمييز بين التقنيات الحيوية والبيانات الحيوية.
- التعرف على البلوك تشين وكيفية حماية البيانات.
- تقدير أهمية مشاركة الجمهور في بناء الثقة.
- تقدير أهمية التواصل مع الجمهور حول حماية البيانات.
- التمييز بين أساليب التواصل الفعالة حول حماية البيانات.
- الإلمام بكيفية الرد على استفسارات الجمهور حول حماية البيانات.
- القدرة على تصميم خطة لحماية البيانات الرقمية الحكومية.



استراتيجيات التدريب المتبعة بالحقيبة



عصف ذهني



الحوار والمناقشة



مقاطع مرئية تدريبية



دراسات حالة



ورش عمل



تطبيقات

المدة الزمنية للحقيبة



عدد الأيام	٣ أيام
عدد ساعات اليوم	٤ ساعات
إجمالي عدد الساعات	١٢ ساعة تدريبية



المستهدفون من البرنامج



- مديري المؤسسات الرقمية الحكومية.
- العاملين بالمؤسسات الرقمية الحكومية.
- أخصائيو الأمن السيبراني في القطاع الحكومي.

التخطيط التفصيلي للبرنامج

	الجلسة الأولي لليوم الأول	
١	التقييم القبلي	١٠ د
٣	مقدمة	١٠ د
٤	نشاط (١) مقطع مرئي	٥ د
٥	تعريف حماية البيانات وأهميتها في القطاع الحكومي	٢٥ د
٦	التحديات الأمنية التي تواجه الخدمات الرقمية الحكومية	٣٠ د
	القوانين المستخدمة في حماية البيانات الدولية والمحلية	٤٠ د
	الجلسة الثانية: لليوم الأول	
١	المفاهيم المتعلقة بالأمن السيبراني	١٥ د
٢	نشاط (٢) عصف ذهني	١٥ د
٣	أفضل الممارسات الأمنية لحماية البيانات	٢٥ د
٤	نشاط (٣) دراسة حالة	٢٠ د
	مبادئ بناء الثقة الرقمية	١٥ د
	أمثلة على ممارسات ناجحة لبناء الثقة	٣٠ د
	الجلسة الأولي: لليوم الثاني	
١	نشاط (٤) ورشة عمل	٢٥ د
٢	استراتيجيات حماية البيانات في الخدمات الرقمية الحكومية	١٥ د
٣	نشاط (٥) حوار ومناقشة	٢٠ د
٤	كيفية تقييم المخاطر الأمنية	١٠ د
٥	كيفية تنفيذ سياسات حماية البيانات	١٠ د
٦	كيفية إدارة الوصول والتحكم في البيانات	١٥ د
٧	ممارسات حماية البيانات في مختلف مراحل دورة حياة الخدمة	١٠ د
٨	طرق وأساليب التدقيق والرقابة على بيانات المستخدمين	١٥ د
	الجلسة الثانية: لليوم الثاني	
١	التشفير وتقنيات الحماية	١٠ د
٢	نظم إدارة الهوية والوصول (IAM)	١٥ د
٣	أدوات مراقبة الأمن السيبراني	٢٠ د

٤	نشاط (٦) ورشة عمل	٢٥ د
٥	الذكاء الاصطناعي في حماية البيانات	١٥ د
٦	التقنيات الحيوية والبيانات الحيوية	٢٥ د
٧	البلوك تشين وحماية البيانات	١٠ د
	الجلسة الأولي لليوم الثالث	
١	نشاط (٧) عصف ذهني	١٥ د
٢	أهمية مشاركة الجمهور في بناء الثقة	١٥ د
٣	أهمية التواصل مع الجمهور حول حماية البيانات	١٠ د
٤	نشاط (٨) حوار ومناقشة	١٥ د
٥	أساليب التواصل الفعالة حول حماية البيانات	٢٥ د
٦	كيفية الرد على استفسارات الجمهور حول حماية البيانات	٢٥ د
	الجلسة الثانية لليوم الثالث	
١	تطبيقات عملية تصميم خطة عملية لحماية البيانات الرقمية في المؤسسات والجهات الحكومية	١٠٠ د
٢	التقييم البعدي	١٠ د



اليوم التدريبي الأول

الجلسة الأولى



أهداف الجلسة:

- التعرف على مفهوم حماية البيانات وأهميتها في القطاع الحكومي.
- التمييز بين التحديات الأمنية التي تواجه الخدمات الرقمية الحكومية.
- الإلمام بالقوانين المستخدمة في حماية البيانات الدولية والمحلية.
- التمييز بين أنواع التهديدات الأمنية.

مقدمة

في عصرٍ تتسابق فيه حكوماتُ العالم على تحويل خدماتها إلى الفضاء الرقمي بسرعة قياسية، أصبح من الضروري حماية بيانات المواطنين، حيث لم يعد هذا الخيار مجرد خيارًا تقنيًا بل تحول إلى مسؤولية أخلاقية وقانونية يُحدد وفقًا لها مدى مصداقية الحكومات واستمرارية ثقة الجمهور فيها. لكن، مع تزايد الهجمات الإلكترونية وانتشار انتهاكات الخصوصية، تواجه الخدمات الحكومية الرقمية تحديًا وجوديًا: كيف يتم بناء منصات ذكية تقدم الخدمات بسلاسة، وفي الوقت نفسه، نقوم بحماية خصوصيات المواطنين وبياناتهم بشكل احترافي.

هذه الحقيبة التدريبية ليست مجرد دليلًا تقنيًا فحسب، بل تُعتبر رحلةً استباقيةً لفهم التهديدات الخفية، واستيعاب أفضل الممارسات العالمية في تأمين البيانات وخصوصيات المواطنين، وبناء ثقافة مؤسسية تُقدِّس خصوصية المستخدم. حيث سنتعلم معًا كيف نُحوِّل التحديات إلى فرص: من تصميم أنظمة تخضع لأعلى معايير التشفير، إلى تبني سياسات شفافة تُعيد للمواطن شعوره بالأمان والسيطرة على معلوماته.



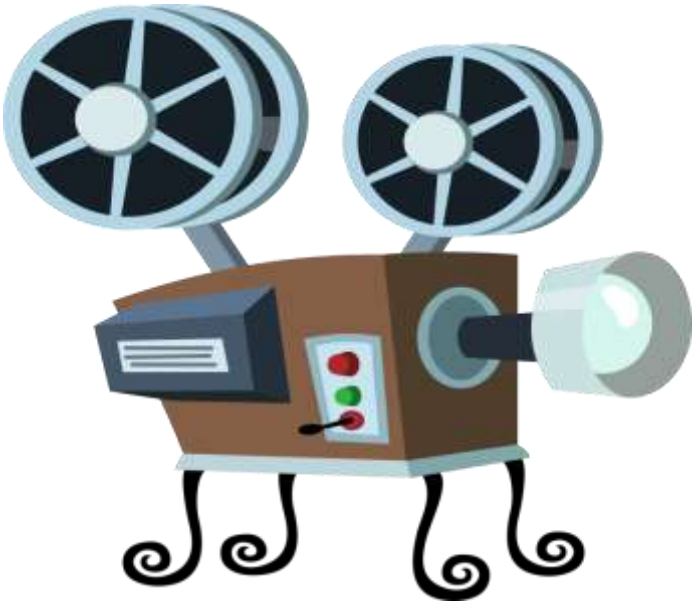
نشاط (١)

مقطع مرئي ٥ دقائق مجموعات

الجريمة الالكترونية

شاهد / شارك

https://www.youtube.com/watch?v=KOsv5_ds0Co&ab_channel=camstage



بالتعاون مع مجموعتك وبعد مشاهدتك للفيديو صف لنا من وجهة نظرك ما الذي استفدت؟:

.....

.....

.....

.....

تعريف حماية البيانات وأهميتها في القطاع الحكومي



تعريف حماية البيانات: إطار متكامل من المبادئ الرقابية والسياسات والإجراءات الفعّالة، المُصمَّمة خصيصًا لضمان سرية وسلامة المعلومات الخاصة بالأفراد، والحد من أي تعرض غير مشروع لها. ولا تقتصر هذه الحماية على الجوانب التقنية فحسب، بل تمتد لتشمل الالتزام الصارم بالتشريعات المحلية والدولية المنظمة لمعالجة البيانات، بما يحفظ حقوق الأفراد ويُعزز الشفافية في التعامل بيانات الأفراد.

أهمية "حماية البيانات" في القطاع الحكومي تتمثل تلك الأهمية فيما يلي:

تطوير الاقتصاد الرقمي:

أحد أبرز أهداف حماية البيانات هو تطوير الاقتصاد الرقمي، وذلك من خلال تعزيز التطور التقني والابتكار، حيث تصبح الحاجة إلى حماية البيانات أمرًا ملحًا مع انتشار وتطور التقنيات الرقمية، مما يعزز ثقة الأفراد في تلك التقنيات والذي بدوره ينعكس إيجابًا على الاقتصاد الرقمي.

تعزيز الشفافية في المهام الحكومية:

في ظل تعامل الجهات الحكومية مع كميات هائلة من البيانات الحساسة، يظل تأمينها بمعايير صارمة أولوية لا تقبل التأجيل، ليس فقط لحماية الخصوصية، بل لضمان نزاهة العمليات وموثوقية الخدمات المقدمة.

صناعة القرارات المستندة إلى البيانات:

حماية البيانات ليست مجرد درعٍ ضد الاختراقات، بل ضمانة لاستخلاص رؤى ذات مصداقية عالية، تُسهم في تخطيط اقتصادي مدروس، وابتكار حلول تلبي الاحتياجات المجتمعية دون المساس بالأخلاقيات الرقمية.

المصادر والمراجع:

- وزارة التعليم. (١٤٤٥ هـ). الأمن السيبراني - التعليم الثانوي - نظام المسارات - السنة الثالثة. وزارة التعليم السعودي
- بوخزر، أميمة، وجقريف، علي. (٢٠٢٤). أهمية اعتماد تقنية البلوك تشين في تعزيز الأمن السيبراني في القطاع المصرفي. مجلة البحوث في العلوم المالية والمحاسبة.
- الخوري، علي محمد. (٢٠٢١). الحكومة الرقمية: مفاهيم وممارسات. المنظمة العربية للتنمية الإدارية - جامعة الدول العربية.
- بايبر، فريد وميرفي، شون. (٢٠١٦). علم التشفير: مقدمة قصيرة جدا. مؤسسة هنداوي للتعليم والثقافة.
- خليفة، إيهاب، تهديدات الأمن الإقليمي العربي في الميدان الخامس: نحو إستراتيجية للحماية. Security Policy Papers.
- الهيئة السعودية للبيانات والذكاء الاصطناعي. (٢٠٢٣). مبادئ أخلاقيات الذكاء الاصطناعي.
- الهيئة الوطنية للأمن السيبراني. (٢٠١٨). الضوابط الأساسية للأمن السيبراني.
- أبو الخير، خالد زكي. (٢٠٢٣). سمات الجمهور الرقمي وعلاقتها بأنماط ومحددات تفاعله مع محتوى المنصات الإخبارية. المجلة العربية لبحوث الإعلام والاتصال.
- الهيئة السعودية للبيانات والذكاء الاصطناعي. (٢٠٢٣). دليل نظام حماية البيانات الشخصية.

مواقع الإنترنت:

الروابط العربية:

- موقع البنك المركزي الإماراتي "أفضل ممارسات حماية البيانات الشخصية".

https://www.cbiuae.com/ar/consumer-education-awareness/consumer-banking-/security/personal-data-protection-best-practices

- غرفة التجارة السعودية. https://www.chamber.sa/Privacy/Pages/PrivacyNotice.aspx

المصادر الاجنبية :

- GDPR.eu. (n.d.). What is GDPR, the EU's new data protection law? Retrieved from https://gdpr.eu/what-is-gdpr/
- Proofpoint. (n.d.). CCPA compliance. Retrieved from https://www.proofpoint.com/us/threat-reference/ccpa-compliance
- CSRC. (n.d.). Retrieved from https://csrc.nist.gov/
- ENISA. (n.d.). Retrieved from https://www.enisa.europa.eu/

- SANS Institute. (n.d.). Retrieved from https://www.sans.org/
- Palo Alto Networks. (n.d.). Firewall vs. antivirus. Retrieved from https://www.paloaltonetworks.com/cyberpedia/firewall-vs-antivirus
- Cloudian. (n.d.). 8 data security best practices you must know. Retrieved from https://cloudian.com/guides/data-security/8-data-security-best-practices-you-must-know/
- Microsoft. (n.d.). What is identity access management (IAM)? Retrieved from https://www.microsoft.com/ar/security/business/security-101/what-is-identity-access-management-iam
- 10xDS. (n.d.). AI for personal data protection and privacy. Retrieved from https://10xds.com/blog/ai-for-personal-data-protection-and-privacy