أمن المعلومات والسرية وتصنيف البيانات وضوابط الوصول

الإمارات العربية المتحدة - دبي

13 – 17/ 12 / 2026

مقدمة:

في قلب التحول الرقمي الشامل لعام 2026، تمثل البيانات "النفط الجديد" والذخيرة الاستراتيجية للدولة. إن حماية هذه الأصول لا تقتصر على التقنيات فحسب، بل تبدأ من قدرة القادة على فهم قيمة المعلومة وحوكمة الوصول إليها بنزاهة مطلقة. يهدف هذا البرنامج إلى تمكين القادة من أدوات تصنيف البيانات السيادية وتطبيق ضوابط وصول ذكية تصفّر البيروقراطية في تدفق المعلومات، مع ضمان أعلى معايير السرية والمصداقية، مما يعزز ريادة المؤسسة ويحمي أمنها القومي الرقمي.

أهداف الدورة:

- استيعاب مفاهيم أمن المعلومات السيادي وعلاقته بتصفير البيروقراطية وجودة الحياة الرقمية.
- تطوير مهارات هندسة "أطر تصنيف البيانات" بناءً على الحساسية والأثر الاستراتيجي.
- إتقان فن تطبيق ضوابط الوصول (Access Controls) بنهج "انعدام الثقة Zero) " Trust).
- حوكمة ممارسات السرية والخصوصية لضمان النزاهة والشفافية أمام الجهات الرقابية.
- تعزيز السيادة المعلوماتية عبر بناء أدوات وطنية مستقلة لإدارة الهوية والوصول.
- تطبيق استراتيجيات القيادة في إدارة "الأصول المعرفية" وضمان استدامة التميز المؤسسي والريادة.

محتويات الورشة:

اليوم الأول :

فلسفة أمن المعلومات والسيادة الرقمية في عام 2026

هندسة الحصانة المعلوماتية وتصفير البيروقراطية الإجرائية

- مفهوم أمن المعلومات السيادي كدرع لحماية الهوية الوطنية والأصول المعرفية للدولة والريادة.
- مواءمة استراتيجيات الأمن مع مبدأ تصفير البيروقراطية عبر أتمتة حماية البيانات "بناءً على التصميم."
- تحليل العلاقة بين "أمن المعلومة" وبين بناء الثقة والمصداقية الدولية في المنظومة الحكومية والتميز.
- تمرين هندسة الجاهزية لتصميم دورة حياة آمنة للمعلومة تصفّر زمن المعالجة بنزاهة وشفافية مطلقة.

قيادة النزاهة في حوكمة الأصول المعرفية والريادة الوطنية

- تعزيز السيادة على الأنظمة التقنية للأمن لضمان استقلاليتها وتوافقها مع القيم الوطنية والنمو.
- دور القائد في حماية صورة المؤسسة عبر ممارسات النزاهة في حفظ السرية المهنية والبيانات.
- بناء ثقافة "الأمان الممكن للابتكار" وعلاقتها بجودة الحياة والولاء المؤسسي والمجتمعي الشامل.
- صياغة ميثاق أخلاقيات قائد أمن المعلومات لدعم النزاهة والقدوة في كافة المستويات القيادية والوطنية.

اليوم الثاني :

السيادة التقنية وهندسة تصنيف البيانات الاستراتيجية

تصفير مخاطر التسريب عبر التصنيف الذكي والتحليلات المتقدمة

- توظيف الذكاء الاصطناعي في تصنيف البيانات (سري، حساس، عام) وتصفير احتمالات الخطأ البشري.
- حماية "البيانات السيادية المصنفة" عبر أنظمة تشفير وطنية لضمان موثوقية المعلومات والنزاهة.
- تطبيق الهوية الرقمية للوثائق لتصفير الهدر البيروقراطي في إجراءات التدقيق والتحقق من الحساسية.
- تطوير لوحات تحكم سيادية (Sovereignty Dashboards) للرصد اللحظي لمستويات تصنيف الأصول.

حوكمة الأنظمة الخوارزمية والنزاهة في استنباط مستويات الحساسية

- إدارة المسؤولية البشرية القيادية عند استخدام أنظمة التصنيف الآلي للبيانات الحكومية والسيادية.
- حوكمة مخرجات أنظمة التنبؤ لضمان الحياد الأخلاقي وتصحيح الانحيازات الرقمية في تقدير الأثر.
- ترسيخ مفهوم الأمانة في البيانات المصنفة لضمان المصداقية أمام صانع القرار والجهات الرقابية.
- ورشة عمل حول ضوابط استخدام البيانات الضخمة في تحسين جودة قرارات التصنيف بنزاهة تامة والتميز.

اليوم الثالث :

ضوابط الوصول والحياد في إدارة الصلاحيات والشمولية

هندسة الوصول الرشيق والشمولية الرقمية في إدارة الهوية

- استخدام تقنيات "انعدام الثقة (Zero Trust) "لضمان عدالة ومنطقية الوصول للبيانات بنزاهة وشفافية.
- تفعيل الرقابة الأخلاقية على منصات منح الصلاحيات لضمان الشفافية وحياد النظم الرقمية في النتائج.
- تطبيق قاعدة الإرادة البشرية القيادية للتدخل وتعديل مسارات الوصول التي قد تغفل البعد الإنساني.
- حساب معامل الثقة في مؤشرات الوصول الآمن لتقليل احتمالات الخطأ الناتج عن الفجوات التقنية.

المسؤولية المهنية وحماية مكتسبات المجتمع والريادة الوطنية

- حوكمة الشراكات مع مزودي السحب الرقمية لضمان توافق ضوابط الوصول مع معايير السيادة والنزاهة.
- تطوير آليات رصد الأثر الاجتماعي لسياسات السرية لضمان النزاهة والعدالة في تقديم الخدمة والتميز.
- بناء سجلات نزاهة رقمية لكل عملية وصول حساسة لضمان الشفافية المطلقة والوضوح التام والريادة.
- تمرين محاكاة لإدارة حوار تقني حول "الوصول والخصوصية" بأسلوب قيادي واثق وملهم للشركاء والجمهور.

اليوم الرابع :

المسؤولية المهنية وإدارة السمعة والنزاهة في حماية السرية

القيادة الاتصالية وحماية السمعة الرقمية للجاهزية المعلوماتية

- أخلاقيات التواصل عند الكشف عن ثغرات أمنية والموازنة بين الإبهار وبين الوقار السيادي الحكومي.
- الرقابة على البصمة الرقمية للالتزام بالسرية وأثرها في تعزيز مصداقية القرار السيادي والوطني.
- بناء أنظمة الإفصاح الاستباقي عن الحوادث المجهضة لضمان الشفافية وتصفير الشائعات الرقمية المضللة.
- التدقيق الأخلاقي على سلاسل توريد البرمجيات الأمنية لضمان خلوها من الممارسات الضارة والنزاهة.

حصانة الأنظمة السيادية ضد الانتهاكات المعلوماتية والتلاعب بالبيانات

- المسؤولية القيادية في التبليغ عن الثغرات التقنية التي قد تهدد أمن بنك المعلومات السيادي والريادة.
- مهارات التواصل الأخلاقي عند حدوث خطأ في تصنيف البيانات لضمان استعادة الثقة ببيانات صادقة.
- إدارة التعافي المؤسسي وإعادة بناء الصورة الذهنية بعد رصد أي انحراف في قيم العمل والنزاهة والتميز.
- بناء خطة الحصانة المنظومية الشاملة لتحصين نتائج العمل الأمني ضد التلاعب الممنهج بالبيانات والواقع.

اليوم الخامس :

هندسة الاستجابة السيادية وتصفير البيروقراطية في أمن المعلومات والسرية الوطنية الشاملة

مختبر "محور المعلومات السيادي" وإدارة الحصانة الرقمية تحت محاكاة "انعدام الثقة"

- محاكاة "تسريب البيانات الاستباقي" والسيادة المعلوماتية: وضع القادة في سيناريو يحاكي محاولة وصول غير مصرح به لأصول بيانات "عالية الحساسية"، واختبار قدرتهم على تفعيل أنظمة "التصنيف الذكي" وتطبيق بروتوكول "التحقق المستمر" بنزاهة ووضوح تام لضمان حماية السرية السيادية دون تعطيل انسيابية العمل.
- تصفير البيروقراطية في "هندسة منح الصلاحيات اللحظية": تطبيق مسار قرار صفري الإجراءات لمنح أو حجب صلاحيات الوصول بناءً على "الهوية الرقمية" والسياق الأمني اللحظي، لضمان تدفق المعلومة للمستحقين في الزمن الحقيقي دون انتظار الموافقات الإدارية التقليدية أو المراسلات الورقية المجهدة، مع الحفاظ على الحصانة الرقمية والريادة العالمية الشاملة.
- هندسة "النزاهة والخصوصية" والتحقق المزدوج: اختبار مهارة القائد في الموازنة بين ضوابط الوصول الصارمة وبين "الحكمة البشرية السيادية" لضمان عدالة توزيع الصلاحيات، ومنع أي انحيازات خوارزمية قد تعيق الكفاءات الوطنية من أداء مهامها، مما يعزز ريادة الدولة كبيئة حوكمة معلوماتية فائقة الموثوقية والشفافية تضع الأمن القومي في قلب أهدافها.
- ورشة "تفكيك صوامع البيانات والربط السيادي": مراجعة فورية لنتائج المحاكاة باستخدام تحليلات "لوحات التحكم السيادية" لتحديد الفجوات في "منظومة تصنيف الأصول"، وتطوير حلول هندسية استباقية تمنع تضارب الصلاحيات بين الجهات المختلفة، مما يحقق التميز في الأداء الوطني والوضوح التام أمام صانع القرار لبناء "رادار أمن معلومات وطني معصوم".

المخرجات الرئيسية للدورة:

- امتلاك استراتيجية حصانة معلوماتية تضمن نزاهة التعامل مع البيانات والمشاريع الوطنية بنسبة 100.%
- القدرة على هندسة منظومات تصنيف رشيقة وسيادية تتوافق مع متطلبات الريادة والتميز العالمية الشاملة.
- إتقان أدوات الرقابة الأخلاقية على الأنظمة الذكية لضمان الشفافية وتصفير مخاطر الانحياز الرقمي في النتائج.
- بناء سجل ممارسات فضلى في إدارة الذكاء الأمني الاستراتيجي يدعم اتخاذ القرار القيادي الآمن والمستدام.

الفئة المستهدفة:

- القيادات والمدراء في إدارات أمن المعلومات، والبيانات، والتحول الرقمي الحكومي.
- مسؤولو حماية البيانات (DPOs) وفرق التميز المؤسسي وتصفير البيروقراطية.
- خبراء الحوكمة والنزاهة والرقابة الداخلية المعنيون بضبط جودة تدفق المعلومات.
- رؤساء فرق العمل الإدارية والتقنية المشرفون على الأنظمة والمنصات السيادية.

أساليب التدريب:

يتم استخدام بعض من الأساليب التالية أو الكل حسب المتطلبات لكل تخصص :

- دراسة الحالة المعقدة (Complex Case Studies)
- المحاكاة والألعاب الاستراتيجية (Simulation and War Gaming)
- ورش العمل القائمة على التفكير التصميمي (Design Thinking Workshops)
- حلقات النقاش مع خبير من القطاعين العام أوالخاص.(Expert Panels)
- المختبرات التقنية التفاعلية (Interactive Technology Labs)
- التعلم من الأقران عبر الجهات الحكومية (Inter-Agency Peer Learning)
- نهج التعلم المدمج والمستمر (Blended & Continuous Learning Approach)