



حوكمة السيادة الرقمية وأمن البيانات الوطنية



الإمارات العربية المتحدة - دبي

2026 / 10 / 22 – 18



مقدمة:

في المشهد العالمي لعام 2026، لم تعد البيانات مجرد "نقط جديد"، بل أصبحت حجر الزاوية في السيادة الوطنية. إن القدرة على التحكم في تدفق المعلومات وحمايتها داخل الحدود الرقمية للدولة هي ما يحدد قوتها واستقلاليتها. يهدف هذا البرنامج إلى تمكين القادة من أدوات حوكمة البيانات الاستراتيجية، وتوظيف التقنيات السيادية لتصفير البيروقراطية في إجراءات الامتثال، مع ضمان النزاهة المطلقة والمصادقية الدولية، مما يعزز ريادة الدولة كنموذج عالمي في الاقتصاد الرقمي الآمن والمستقل.

أهداف الدورة:

- استيعاب أبعاد "السيادة الرقمية" (التقنية، المعلوماتية، والتشريعية) وأثرها على الأمن القومي.
- تطوير مهارات هندسة "أطر حوكمة البيانات" الوطنية لضمان جودة وتصنيف الأصول المعلوماتية.
- إتقان فن بناء "السحابة السيادية (Sovereign Cloud)" وتأمينها ضد التدخلات الخارجية.
- حوكمة ممارسات مشاركة البيانات بين القطاعات لتصفير البيروقراطية وتحقيق الرقابة الحكومية.
- تعزيز السيادة المعلوماتية عبر امتلاك الخوارزميات والشيفرات الوطنية المستقلة.
- تطبيق استراتيجيات القيادة في إدارة "الأزمات السيادية الرقمية" وضمان السمعة الدولية والنمو.



محتويات الورشة:

اليوم الأول :

فلسفة السيادة في العصر الرقمي والرشاقة الاستراتيجية

هندسة الاستقلال الرقمي وتصفير البيروقراطية في تدفق البيانات

- مفهوم السيادة الرقمية 2026: من "توطين البيانات" إلى "امتلاك القرار التقني" والنمو والتميز العالمي.
- موازنة استراتيجيات الحوكمة مع مبدأ تصفير البيروقراطية عبر "الربط الحكومي الشامل" (G-Cloud).
- تحليل العلاقة بين "الاستقلال المعلوماتي" وبين بناء الثقة والمصادقية الدولية في النموذج الوطني.
- تمرين هندسة الاستباقية لتصميم دورة حياة للبيانات تصفّر زمن "الوصول والتحقق" بنزاهة وشفافية.

قيادة النزاهة في حوكمة "الأصول المعرفية" والريادة الوطنية الشاملة

- تعزيز السيادة على الأنظمة التقنية للحوكمة لضمان استقلاليتها وتوافقها مع القيم والهوية والتميز.
- دور القائد في حماية صورة المؤسسة عبر ممارسات النزاهة في إدارة البيانات الضخمة (Big Data).
- بناء ثقافة "البيانات كأمانة وطنية" وعلاقتها بجودة الحياة والولاء المؤسسي والأمن القومي الشامل.
- صياغة ميثاق أخلاقيات قائد البيانات السيادي لدعم النزاهة والقُدوة في كافة المستويات القيادية.

اليوم الثاني :

السيادة التقنية وهندسة السحابة الوطنية والذكاء الاصطناعي

تصفير مخاطر الارتهان الخارجي عبر "السحب السيادية" والذكاء الاصطناعي الوطني

- توظيف تقنيات السحابة السيادية لتصفير فجوات الخصوصية والتحكم في البيانات الحساسة بنزاهة والتميز.
- حماية "الخوارزميات السيادية" عبر أنظمة تشفير وطنية تضمن موثوقية النتائج والنزاهة الرقمية والريادة.
- تطبيق الهوية الرقمية للأصول المعلوماتية لتصفير الهدر البيروقراطي في إجراءات الجرد والتصنيف.
- تطوير لوحات تحكم سيادية (Sovereignty Dashboards) للرصد اللحظي لصحة ونزاهة البيانات الوطنية.



حوكمة الأنظمة الخوارزمية والنزاهة في استنباط الرؤى الوطنية

- إدارة المسؤولية البشرية القيادية عند استخدام الذكاء الاصطناعي في إصدار "قرارات حوكمة البيانات".
- حوكمة مخرجات أنظمة التنبؤ لضمان الحياد الأخلاقي وتصحيح الانحيازات الرقمية في تقدير الأخطار.
- ترسيخ مفهوم الأمانة في البيانات المستقاة من رصد الأداء لضمان المصداقية أمام صانع القرار والسيادة.
- ورشة عمل حول ضوابط استخدام البيانات الضخمة في تحسين جودة قرارات الحوكمة بنزاهة تامة والتميز.

اليوم الثالث :

هندسة مشاركة البيانات والحياد في إدارة الموارد والشمولية

تفسير البيروقراطية في "اتفاقيات مشاركة البيانات" والشمولية الرقمية

- هندسة منصات تبادل البيانات (Data Exchange) التي تصفّر زمن التنسيق بين الجهات بنزاهة والتميز.
- تفعيل الرقابة الأخلاقية على منصات "البيانات المفتوحة" لضمان حياد النظم الرقمية والنمو الشامل.
- تطبيق تقنيات "سلاسل الكتل (Blockchain)" لتوثيق ملكية البيانات وتصفير احتمالات التلاعب بالسجلات.
- حساب معامل الثقة في مؤشرات الإنجاز الرقمي لتقليل احتمالات الخطأ الناتج عن الفجوات التقنية والسيادة.

المسؤولية المهنية وحماية مكتسبات المجتمع والريادة الوطنية الشاملة

- حوكمة الشراكات مع مزودي التكنولوجيا لضمان توافقها مع معايير جودة الحياة والسيادة والنزاهة والنمو.
- تطوير آليات رصد الأثر الاجتماعي لسياسات البيانات لضمان النزاهة والعدالة والتميز والريادة.
- بناء سجلات نزاهة رقمية لكل عملية "فتح بيانات" كبرى لضمان الشفافية المطلقة والوضوح والريادة.
- تمرين محاكاة لإدارة حوار استراتيجي حول "السيادة والتعاون الدولي" بأسلوب قيادي واثق وملهم.



اليوم الرابع :

المسؤولية المهنية وإدارة السمعة والنزاهة في العصر الرقمي

القيادة الاتصالية وحماية السمعة الرقمية للجهازية الوطنية الشاملة

- أخلاقيات التواصل عند حدوث "خروقات سيادية للبيانات" والموازنة بين الإبهار والوقار والنزاهة والتميز.
- الرقابة على البصمة الرقمية لأنظمة الحوكمة لتعزيز مصداقية القرار السيادي عالمياً والريادة والنمو.
- بناء أنظمة الإفصاح الاستباقي عن كفاءة "الحصانة المعلوماتية" لتصفير فرص انتشار الشائعات والنزاهة.
- التدقيق الأخلاقي على سلاسل توريد البرمجيات لضمان خلوها من الممارسات الضارة والسيادة والريادة.

حصانة المنظومة السيادية ضد الانتهاكات المعلوماتية والتلاعب بالنتائج

- المسؤولية القيادية في التبليغ عن الثغرات التقنية التي قد تهدد أمن بنك المعلومات الوطني والسيادة 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 الرقمي والتميز.
- بناء خطة الحصانة المنظومية الشاملة لتحسين نتائج الرصد ضد التلاعب بالمنهج بالبيانات والواقع الرقمي.



اليوم الخامس :

خارطة الطريق وصناعة القائد الرقمي "السيادي" القدوة: من حوكمة البيانات إلى هندسة السيادة الرقمية الشاملة

هندسة "النبض الاستراتيجي" والرشاقة السيادية في حوكمة البيانات

- مصفوفة "النبض اللحظي" للسيادة المعلوماتية: تصميم نظام رصد سيادي يعتمد على الذكاء الاصطناعي لتحويل تدفقات "الأصول المعرفية" إلى نبضات استراتيجية تظهر للقائد فوراً. يهدف هذا النظام إلى تصفير زمن "التحقق من تصنيف البيانات" وضمان معالجتها داخل السحابة السيادية الوطنية بنزاهة ومصداقية تامة، بعيداً عن أي ارتهان خارجي.
- بروتوكول "الرشاقة السيادية" لمشاركة البيانات الشاملة: هندسة مسار قرار "صفري الإجراءات" يسمح بتبادل البيانات الحساسة بين الجهات الحكومية ألياً فور رصد النبضة الاستراتيجية التي تؤكد "الحاجة المعرفية". يضمن هذا البروتوكول سرعة الإنجاز الحكومي دون قيود بيروقراطية أو انتظار لاتفاقيات مشاركة ورقية تعطل نمو الاقتصاد الرقمي.
- حوكمة "القرار التقني المستقل" والنزاهة: وضع ضوابط أخلاقية تضمن ملكية الدولة الكاملة للخوارزميات والشيفرات المصدرية، وتفعيل ميثاق "النزاهة في الرؤى الوطنية" لضمان استقلال مخرجات الذكاء الاصطناعي عن الانحيازات الرقمية الخارجية، والوضوح التام أمام صانع القرار.
- مختبر "هندسة الحصانة ضد الأزمات السيادية": تمرين محاكاة متقدم لاختبار قدرة القائد على إدارة "نبضة أزمة" ناتجة عن محاولة تدخل خارجي في الأنظمة الوطنية، وكيفية تفعيل "بروتوكول الاستقلال الرقمي" لحماية الأسرار الوطنية والسيادة المعلوماتية.

المخرجات الرئيسية للدورة:

- امتلاك استراتيجية حصانة معلوماتية تضمن نزاهة التعامل مع البيانات والمشاريع الوطنية بنسبة 100%.
- القدرة على هندسة منظومات حوكمة 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 الاستراتيجي للبيانات يدعم اتخاذ القرار القيادي الآمن والمستدام للوطن.

الفئة المستهدفة:

- القيادات العليا ومدراء التحول الرقمي، ومسؤولو البيانات (CDOS)، ومدراء أمن المعلومات (CISOs).
- مسؤولو التخطيط الاستراتيجي والتميز المؤسسي وفرق تصفير البيروقراطية في الجهات السيادية.
- خبراء الحوكمة والنزاهة والرقابة التقنية المعنيون بضبط جودة الأداء والسيادة المعلوماتية.
- رؤساء مكاتب السياسات الرقمية ومحللو الأمن القومي في الهيئات الاتحادية والمحلية.



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 أو الخاص. (Expert Panels)
- المختبرات التكنولوجية التفاعلية (Interactive Technology Labs)
- التعلم من الأقران عبر الجهات الحكومية (Inter-Agency Peer Learning)
- نهج التعلم المدمج والمستمر (Blended & Continuous Learning Approach)