



## الإدارة الآمنة للمعلومات والسجلات الرقمية الحكومية



الإمارات العربية المتحدة - دبي

2026 / 05 / 21 – 17



## مقدمة:

في فضاء عام 2026، لم تعد المعلومات مجرد بيانات مخزنة، بل أصبحت "أصولاً سيادية" تمثل ذاكرة الدولة وقوتها. إن الإدارة الآمنة للسجلات الرقمية تتطلب فكراً قيادياً ينتقل من "حماية الأوعية" إلى "حوكمة المحتوى"؛ حيث يتم تصفير البيروقراطية في الوصول للمعلومة مع ضمان أعلى مستويات الحصانة ضد التهديدات. يهدف هذا البرنامج إلى تمكين القادة من هندسة "مستودعات معرفية ذكية" محمية سيادياً، تضمن النزاهة المطلقة وتدعم اتخاذ القرار اللحظي، مما يرسخ قيادة المؤسسة كمنظومة رقمية آمنة وموثوقة عالمياً.

## أهداف الدورة:

- استيعاب مفاهيم "السيادة المعلوماتية" وأثرها في تصفير البيروقراطية وتحقيق النمو الوطني.
- تطوير مهارات هندسة "الأرشيف الرقمي الحصين" باستخدام تقنيات التشفير السيادي.
- إتقان فن حوكمة "دورة حياة السجل الرقمي" من الإنشاء وحتى الإلتلاف الآمن بنزاهة.
- حوكمة ممارسات "الوصول اللامركزي" للمعلومات لضمان الشفافية وحماية الخصوصية.
- تعزيز السيادة الإدارية عبر بناء "أنظمة توثيق وطنية" مستقلة ومحمية بالكامل.
- تطبيق استراتيجيات القيادة في إدارة "الأمن الوثائقي" وضمان المصداقية والتميز العالمي.



## محتويات الورشة:

### اليوم الأول:

#### فلسفة "الأمن بالرشافة" والسيادة في هندسة المعلومات

#### هندسة الحصانة وتصفير البيروقراطية في "تصنيف البيانات"

- مفهوم المعلومات السيادية 2026 والتحول من "التخزين الساكن" إلى "المعرفة النشطة" والنمو.
- موازنة نظم السجلات مع مبدأ تصفير البيروقراطية عبر "التصنيف التلقائي الذكي" للوثائق.
- تحليل العلاقة بين "سلامة السجل" وبين بناء الثقة والمصادقية الدولية في المنظومة الحكومية.
- تمرين هندسة الاستباقية لتصميم مصفوفة وصول تصفّر زمن "استرجاع المعلومة" بنزاهة وشفافية.

#### قيادة النزاهة في حوكمة "الأمانة الرقمية" والريادة الوطنية الشاملة

- تعزيز السيادة على قواعد البيانات الوطنية لضمان استقلاليتها وتوافقها مع القيم والهوية.
- دور القائد في حماية صورة المؤسسة عبر ممارسات النزاهة في "منح صلاحيات الاطلاع" والخصوصية.
- بناء ثقافة "المعلومة كأمانة سيادية" وعلاقتها بالولاء المؤسسي والأمن القومي الشامل والريادة.
- صياغة ميثاق أخلاقيات مدير السجلات السيادي لدعم النزاهة والقدوة في كافة المستويات القيادية.

### اليوم الثاني:

#### السيادة التقنية وهندسة "الأرشفة الذكية" (Smart Archiving)

#### تصفير البيروقراطية الرقابية عبر "التوثيق الموثق" بالبلوك تشين

- توظيف تقنيات السجلات الموزعة لتصفير الهدر البيروقراطي في "إثبات صحة المستندات" بنزاهة.
- حماية "السجلات السيادية" عبر أنظمة تشفير وطنية تضمن نزاهة المعلومات والريادة والنمو الشامل.
- تطبيق تقنيات "التعرف الذكي على المحتوى" لتصفير فجوات البحث اليدوي المجهد والتميز والنمو.
- تطوير لوحات تحكم سيادية للرصد اللحظي لحالة أمن السجلات ومعدلات الرقمنة الشاملة والريادة.



## حوكمة الأنظمة الخوارزمية والنزاهة في "إدارة المحتوى الرقمي"

- إدارة المسؤولية البشرية القيادية عند استخدام الآلة في "تقييم أهمية الوثائق" والتميز والنمو.
- حوكمة مخرجات أنظمة التنبؤ لضمان الحياد الأخلاقي وتصحيح الانحيازات الرقمية في نتائج الأرشفة.
- ترسيخ مفهوم الأمانة في المعلومات المستقاة من السجلات لضمان المصداقية والسيادة والنمو الشامل.
- ورشة عمل حول ضوابط استخدام البيانات الضخمة في تحسين جودة "الذاكرة المؤسسية" بنزاهة تامة.

## اليوم الثالث:

### هندسة "الأمن السيبراني للسجلات" والحياد في الإدارة

#### تفسير البيروقراطية في "نماذج الثقة الصفرية (Zero Trust) والشمولية

- هندسة بروتوكولات الحماية التي تصفّر زمن "تأمين الملفات الحساسة" مع ضمان أعلى معايير السيادة.
- تفعيل الرقابة الأخلاقية على منصات "مشاركة السجلات" لضمان حياد النظم والتميز والنمو والريادة.
- تطبيق تقنيات "الحصانة الرقمية" للسجلات لتصفير فجوات الاختراق أو التلاعب المعلوماتي بنزاهة.
- قياس مؤشر "النضج الوثائقي" للمؤسسة لتقليل احتمالات الخطأ الناتج عن الفجوات التقنية والنمو الشامل.

#### المسؤولية المهنية وحماية مكتسبات المجتمع والريادة الوطنية الشاملة

- حوكمة التعامل مع "السجلات التاريخية" لضمان توافقها مع معايير جودة الحياة والسيادة والنزاهة.
- تطوير آليات رصد الأثر المعرفي للإدارة الأمانة للمعلومات لضمان النزاهة والعدالة والتميز والنمو.
- بناء سجلات نزاهة رقمية لكل عملية "إتلاف سجلات" كبرى لضمان الشفافية والوضوح والريادة والسيادة.
- تمرين محاكاة لإدارة حوار استراتيجي حول "السيادة والترابط المعلوماتي" بأسلوب قيادي واثق.



## اليوم الرابع:

### المسؤولية المهنية وإدارة السمعة والنزاهة في "أزمات البيانات"

#### القيادة الاتصالية وحماية السمعة المعلوماتية للجهازية الوطنية الشاملة

- أخلاقيات التواصل عند وقوع "محاولات اختراق للأرشيف" والموازنة بين الإبهار والوقار والنزاهة.
- الرقابة على البصمة الرقمية للأنظمة المعلوماتية لتعزيز مصداقية القرار السيادي عالمياً والريادة.
- بناء أنظمة الإفصاح الاستباقي عن نجاحات "تصفير المخاطر الوثائقية" لتعزيز النزاهة والشفافية التامة.
- التدقيق الأخلاقي على سلاسل توريد برمجيات السجلات لضمان خلوها من الممارسات الضارة والسيادة.

#### حصانة المنظومة السيادية ضد الانتهاكات المعلوماتية والتلاعب بالنتائج

- المسؤولية القيادية في التبليغ عن الثغرات التي قد تهدد أمن "أسرار الدولة" والسيادة والريادة الشاملة.
- مهارات التواصل الأخلاقي عند حدوث خطأ في "نظام استرجاع السجلات" لضمان استعادة الثقة ببيانات صادقة.
- إدارة التعافي المؤسسي وإعادة بناء الصورة الذهنية بعد رصد أي انحراف في قيم العمل والتميز والنمو.
- بناء خطة الحصانة المنظومية الشاملة لتحسين نتائج العمل ضد التلاعب الممنهج بالواقع الرقمي والنمو.



## اليوم الخامس:

### خارطة الطريق وصناعة القائد الرقمي "Record-Master" القدوة: من إدارة الأوعية إلى هندسة السيادة المعلوماتية الشاملة

#### هندسة "النبض الاستراتيجي" والرشاقة السيادية في إدارة السجلات

- مصفوفة "النبض اللحظي" للذاكرة الرقمية: تصميم نظام رصد سيادي يعتمد على الذكاء الاصطناعي لتحويل تدفق السجلات والوثائق إلى نبضات استراتيجية تظهر للقائد فوراً. يهدف هذا النظام إلى تصفير زمن "البحث عن الحقيقة المعلوماتية" وضمان سلامة الأصول الوثائقية بنزاهة ومصداقية تامة، بعيداً عن الركود الإداري أو الضياع المعرفي.
- بروتوكول "الرشاقة السيادية" للوصول المعلوماتي الفوري: هندسة مسار قرار "صفري الإجراءات" يسمح للأنظمة باسترجاع الوثائق الحساسة ومنح صلاحيات الاطلاع اللحظي آلياً فور رصد النبضة الاستراتيجية التي تؤكد "الحاجة المعرفية" المشروعة. يضمن هذا البروتوكول سرعة الإسناد للقرار القيادي دون قيود بيروقراطية أو مراسلات ورقية تعطل نبض الدولة.
- حوكمة "الأمانة المعلوماتية" في الأرشفة الذكية: وضع ضوابط أخلاقية تضمن ملكية الدولة الكاملة لسجلاتها الرقمية، وتفعيل ميثاق "النزاهة في التوثيق" لضمان خلو الأرشيف الوطني من أي تلاعب أو انحياز رقمي، والوضوح التام أمام صانع القرار بشأن تاريخ وحاضر الأصول المعلوماتية.
- مختبر "هندسة الحصانة ضد التسريب المعلوماتي": تمرين محاكاة متقدم لاختبار قدرة "Record-Master" على إدارة "نبضة أزمة وثائقية" ناتجة عن محاولة وصول غير مشروع، وكيفية تفعيل بروتوكولات "التشفير السيادي والتعافي" لحماية أسرار الدولة والسيادة المعلوماتية الشاملة.

#### المخرجات الرئيسية للدورة:

- امتلاك استراتيجيات حصانة معلوماتية تضمن نزاهة التعامل مع السجلات والبيانات الوطنية بنسبة 100%.
- القدرة على هندسة منظومات أرشفة رشيفة 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 للمعلومات يدعم اتخاذ القرار القيادي الآمن والمستدام.



## الفئة المستهدفة:

- القيادات العليا ومدراء إدارات تكنولوجيا المعلومات، والأرشفة، والتميز المؤسسي.
- مسؤولو أمن المعلومات (CISO) وفرق تصفير البيروقراطية في الجهات السيادية والاتحادية.
- خبراء الحوكمة والنزاهة والرقابة الإدارية المعنيون بصحة السجلات والوثائق الوطنية.
- رؤساء مكاتب التحول الرقمي ومحلولو المخاطر المعلوماتية في المؤسسات الحكومية والوطنية.

## 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)