تسخير تقنيات إنترنت الأشياء والأجهزة القابلة للارتداء لسلامة الموظفين

الإمارات العربية المتحدة - دبي

15 – 19/ 02 / 2026

مقدمة:

في إطار التوجه الاستراتيجي نحو السيادة الرقمية وتطبيق مبدأ تصفير البيروقراطية، يتحول مفهوم السلامة المهنية من الرقابة التقليدية إلى "الحماية اللحظية الذكية". تهدف هذه الدورة إلى تمكين القادة من توظيف تقنيات إنترنت الأشياء (IoT) والمستشعرات القابلة للارتداء (Wearables) لخلق بيئة عمل "مؤمنة رقمياً". يركز البرنامج على كيفية حوكمة تدفق البيانات الحيوية والبيئية لضمان النزاهة المطلقة وحماية خصوصية المورد البشري السيادي، مما يضمن ريادة المؤسسة وقدرتها على تصفير الحوادث عبر التنبؤ الذكي والتدخل الاستباقي.

أهداف الدورة:

- استيعاب مفاهيم **الربط السيادي** وعلاقتها بالرشاقة المؤسسية وتصفير البيروقراطية الإجرائية.
- تطوير مهارات هندسة منظومات السلامة المعتمدة على المستشعرات الذكية لرصد المخاطر في الوقت الفعلي.
- إتقان فن إدارة البيانات الضخمة الناتجة عن الأجهزة القابلة للارتداء لتحسين اتخاذ القرار الوقائي.
- حوكمة استخدام التقنيات الغامرة والملبوسة لضمان النزاهة والامتثال للمعايير الأخلاقية والوطنية.
- اكتساب مهارات **تصفير زمن الاستجابة للطوارئ** عبر أتمتة التنبيهات والخرائط الحرارية للمخاطر.
- تعزيز السيادة الرقمية من خلال تأمين سحابة بيانات السلامة ومنع التدخلات الخارجية.
- تطبيق استراتيجيات "التلعيب (Gamification) "لتعزيز الالتزام بمهمات السلامة عبر الأجهزة الذكية.
- تطوير مهارات إدارة المعضلات الأخلاقية المرتبطة بمراقبة الموظفين والحق في الخصوصية.
- صياغة خارطة طريق شاملة لتحويل بيئة العمل إلى "منشأة ذكية وآمنة" تدعم الريادة العالمية.

محتويات الورشة:

اليوم الأول:

فلسفة "إنترنت السلامة" في عصر تصفير البيروقراطية

من "التفتيش اليدوي" إلى "الحصانة الرقمية اللحظية"

- مفهوم إنترنت الأشياء (IoT) في السلامة الحكومية: كيف تصبح البيئة هي الحارس للموظف؟
- مواءمة الـ IoT مع استراتيجية تصفير البيروقراطية: إلغاء سجلات الحضور والغياب والمخاطر الورقية.
- تحليل العلاقة بين "التدفق اللحظي للبيانات" وبين بناء الثقة والمصداقية الوطنية.
- تمرين "هندسة المسار الآمن": تصميم رحلة موظف في منشأة ذكية تصفّر المخاطر إجرائياً بنزاهة.

النزاهة والسيادة في بناء "الدرع الرقمي للموظف"

- مفهوم "السيادة المعلوماتية الحيوية": حماية البيانات الصحية للموظفين من التلاعب أو الاستغلال.
- دور القائد في حماية صورة المؤسسة عبر ممارسات النزاهة في استخدام تقنيات التتبع.
- سيكولوجية الأمان التقني: بناء المصداقية عبر الشفافية في توضيح "ماذا نرصد ولماذا؟".
- صياغة ميثاق "أخلاقيات الملبوسات التقنية" لضمان توافقها مع الكرامة الإنسانية والسيادة الوطنية.

اليوم الثاني:

الهندسة التقنية والسيادة المعلوماتية للأجهزة

الربط البيني الآمن وإدارة الهوية الرقمية للأجهزة

- أنواع المستشعرات (نبض القلب، السقوط، جودة الهواء، التعب) وكيفية دمجها في نظام موحد بنزاهة.
- الأمان الرقمي كركيزة للـ IoT: حماية الأجهزة القابلة للارتداء من الاختراق أو "التزييف البيومتري."
- إدارة الهوية الرقمية (UAE Pass) وأثرها على موثوقية الدخول للمناطق الخطرة وتصفير الأخطاء.
- تمرين تقني: تصميم بروتوكول "التحقق المزدوج" لضمان نزاهة البيانات الصادرة من الأجهزة الميدانية.

أخلاقيات التفاعل مع أنظمة "التحذير الآلي"

- حدود استخدام الذكاء الاصطناعي في "التدخل القسري" (مثل إيقاف الآلات) لضمان السلامة السيادية.
- حوكمة مخرجات أنظمة "توقع الإجهاد": الضمان الأخلاقي لعدم استخدام البيانات ضد الموظف بنزاهة.
- مفهوم "الأمانة في الرصد": تجنب الاعتماد الكلي على الآلة دون وجود "حكمة قيادية" بشرية.
- ورشة عمل: وضع ضوابط أخلاقية لاستخدام البيانات الضخمة في "تحسين تصميم بيئة العمل."

اليوم الثالث:

الحياد والعدالة في إدارة "البيانات الحساسة"

النزاهة الرقمية ومكافحة الانحياز في الرصد البيومتري

- أخلاقيات "العدالة الرقمية": ضمان دقة المستشعرات لجميع الفئات دون تمييز أو انحياز تقني.
- الرقابة الأخلاقية على أنظمة "الخرائط الحرارية": كيف نضمن الشفافية والنزاهة في توزيع المهام؟
- تطبيق قاعدة "الإرادة البشرية القيادية": التدخل لتفسير "تنبيه صحي" قد يكون ناتجاً عن ظرف عارض.
- حساب معامل الثقة في أنظمة الـ IoT لتقليل احتمالات الخطأ الناتج عن "الهلوسة الرقمية" للبيانات.

حوكمة المسؤولية عن مخرجات "السلامة المؤتمتة"

- المسؤولية المهنية للقائد عند فشل مستشعر في إرسال "نداء استغاثة" أو حدوث عطل في الشبكة.
- إدارة العلاقة مع مزودي حلول "Smart Safety": ضمان السيادة والشفافية في معالجة البيانات.
- بناء أنظمة "التحقق المزدوج" لضمان عدم غياب الحكمة البشرية في قراءة الإنذارات الخطرة.
- تمرين محاكاة: إدارة أزمة تواصل ناتجة عن "عطل تقني" في أجهزة السلامة وكيفية علاجه بنزاهة.

اليوم الرابع:

المسؤولية المهنية وإدارة السمعة في الأزمات التقنية

القيادة الاتصالية وحماية السمعة في البيئات الذكية

- أخلاقيات إدارة أزمات "تسريب البيانات الصحية": الموازنة بين الشفافية والسيادة والخصوصية.
- الرقابة على "البصمة الرقمية للأجهزة" وأثرها على حيادية ومصداقية القرار السيادي والقانوني.
- بناء نظام "الإفصاح الاستباقي للجاهزية": ضمان الشفافية لتصفير فرص انتشار الشائعات حول السلامة.
- التدقيق الأخلاقي على سلاسل "التوريد التقني" لضمان خلوها من الممارسات غير العادلة أو المحفوفة بالمخاطر.

أخلاقيات الاستجابة للانتهاكات والاختراقات السيبرانية للأجهزة

- المسؤولية الأخلاقية في التبليغ عن الثغرات التقنية التي قد تؤدي لتعطيل "أنظمة حماية الموظفين."
- فن التواصل الأخلاقي أثناء تعطل أنظمة الـ IoT: حماية الثقة عبر بيانات صادقة ونزيهة دون تضليل.
- إدارة "التعافي المؤسسي": إجراءات إعادة بناء الصورة بعد رصد انحراف في دقة الأجهزة القابلة للارتداء.
- بناء خطة "الحصانة الرقمية الشاملة": تحصين منظومة السلامة ضد الهجمات أو الإهمال الممنهج.

اليوم الخامس:

هندسة الحماية اللحظية وتصفير البيروقراطية في توظيف إنترنت الأشياء (IoT) لسلامة الموظفين والسيادة الحيوية

مختبر "النبض الرقمي السيادي" وإدارة السلامة الوقائية عبر المستشعرات الملبوسة

- محاكاة "الاستجابة الحيوية الحرجة" والسيادة المعلوماتية: وضع القادة في سيناريو يحاكي رصد "إجهاد حراري أو أزمة صحية مفاجئة" لموظف في موقع ميداني عبر جهازه القابل للارتداء، واختبار قدرة المنظومة على تفعيل بروتوكول "التدخل الاستباقي" بنزاهة ووضوح تام لضمان حماية المورد البشري السيادي دون انتهاك خصوصيته الرقمية.
- تصفير البيروقراطية في "هندسة الطوارئ المؤتمتة": تطبيق مسار قرار صفري الإجراءات لإيقاف العمليات الميكانيكية أو إخلاء الموقع بناءً على تنبيهات المستشعرات (IoT) اللحظية، لضمان حماية الأرواح في الزمن الحقيقي دون انتظار الاعتمادات الإدارية التقليدية أو البلاغات الورقية التي قد تتسبب في تأخر الإنقاذ، مع الحفاظ على الحصانة الرقمية والريادة العالمية الشاملة.
- هندسة "النزاهة والخصوصية الحيوية" والتحقق المزدوج: اختبار مهارة القائد في الموازنة بين مخرجات أنظمة "توقع الإجهاد" وبين "الحكمة البشرية السيادية" لضمان عدم استخدام البيانات الصحية ضد الموظف في تقييمات الأداء، ومنع أي انحيازات خوارزمية قد تسيء فهم الحالة الفسيولوجية، مما يعزز ريادة الدولة كبيئة عمل إنسانية وآمنة تقنياً.
- ورشة "تفكيك صوامع بيانات السلامة والربط السيادي": مراجعة فورية لنتائج المحاكاة لتحديد الفجوات في "منظومة الربط البيني" بين الأجهزة القابلة للارتداء وغرف العمليات، وتطوير حلول هندسية استباقية تمنع تضارب البيانات أو الاختراقات السيبرانية للأجهزة، مما يحقق التميز في الأداء الوطني والوضوح التام أمام صانع القرار لبناء "رادار سلامة وطني موحد".

المخرجات الرئيسية للدورة:

- امتلاك استراتيجية "حصانة رقمية" تضمن نزاهة التعامل مع بيانات الموظفين بنسبة 100.%
- القدرة على هندسة منظومات سلامة "ذكية ومترابطة" بمرونة وتوافق مع متطلبات السيادة والريادة.
- إتقان أدوات الرقابة الأخلاقية على الأنظمة الذكية لضمان الشفافية وتصفير مخاطر الانحياز الرقمي.
- بناء سجل ممارسات فضلى في إدارة "إنترنت السلامة" يدعم اتخاذ القرار القيادي الآمن والمستدام.
- تحقيق جاهزية كاملة للمؤسسة والمسؤول للمنافسة في فئات التميز والريادة في السلامة والابتكار.

الفئة المستهدفة:

- القيادات والمدراء في إدارات السلامة والصحة المهنية، التحول الرقمي، والعمليات.
- مسؤولو التميز المؤسسي، مهندسو النظم، وخبراء الاستراتيجية في الجهات السيادية.
- مستشارو التكنولوجيا الناشئة، مدراء السعادة وجودة الحياة، وفرق الاستجابة للطوارئ.
- رؤساء فرق مشاريع تصفير البيروقراطية وتطوير الخدمات الحكومية الذكية.
- الكوادر الطموحة الساعية لامتلاك جدارات "قائد السلامة الرقمية المعززة بالـ"IoT.

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)