



الرصد الاستباقي للمخاطر الصحية المهنية باستخدام أجهزة الاستشعار الذكية



الإمارات العربية المتحدة - دبي

2026 / 04 / 23 – 19



مقدمة:

في إطار التوجه الاستراتيجي نحو السيادة الرقمية وتطبيق مبدأ تصفير البيروقراطية، يتحول الرصد الصحي من مجرد "فحوصات دورية" إلى "حماية لحظية مستمرة". تهدف هذه الدورة إلى تمكين القادة من توظيف تقنيات إنترنت الأشياء (IoT) والمستشعرات القابلة للارتداء لرصد العوامل الحيوية والبيئية في الوقت الفعلي. يركز البرنامج على حوكمة تدفق البيانات الصحية لضمان النزاهة المطلقة وحماية الخصوصية السيادية للمورد البشري، مما يضمن قيادة المؤسسة وقدرتها على التنبؤ بالأمراض المهنية وتصفير مخاطرها قبل وقوعها.

أهداف الدورة:

- استيعاب مفاهيم الرصد السيادي وعلاقتها بالرشاقة المؤسسية وتصفير البيروقراطية الإجرائية.
- تطوير مهارات هندسة منظومات الاستشعار الذكية لرصد غازات بيئة العمل، الضجيج، والجهد البدني.
- إتقان فن تحليل البيانات الحيوية (Biometrics) باستخدام الذكاء الاصطناعي للتنبؤ بحالات الإجهاد والاحتراق.
- حوكمة استخدام الأجهزة القابلة للارتداء لضمان النزاهة والامتثال للمعايير الأخلاقية والوطنية.
- اكتساب مهارات تصفير الفجوة الاستجابية عبر أنظمة التنبيه اللحظي للمخاطر الصحية.
- تعزيز السيادة الرقمية من خلال تأمين سحابة بيانات الصحة المهنية ومنع التدخلات الخارجية.
- تطبيق استراتيجيات "الوقاية الرقمية المخصصة" بناءً على البصمة الحيوية لكل موظف بنزاهة تامة.
- تطوير مهارات إدارة المعضلات الأخلاقية المرتبطة بمراقبة الحالة الصحية مقابل الحرية الشخصية.
- صياغة خارطة طريق شاملة لتحويل الرصد الصحي إلى "أصل استراتيجي" يدعم جودة الحياة والريادة.



محتويات الورشة:

اليوم الأول:

فلسفة الرصد الاستباقي في عصر الرشاقة الرقمية

من "التشخيص المتأخر" إلى "التنبؤ اللحظي والرشاقة"

- مفهوم الرصد الاستباقي السيادي: لماذا تُعد البيانات الحيوية خط الدفاع الأول عن المورد البشري؟
- موازنة الرصد مع استراتيجية تصفير البيروقراطية: إلغاء التقارير الطبية الورقية والاعتماد على التدفق الرقمي.
- تحليل العلاقة بين "الأمان الصحي الرقمي" وبين بناء الثقة والمصادقية الوطنية عالمياً.
- تمرين "هندسة المناعة الرقمية": تصميم نظام رصد يصفّر التعرض للمخاطر المهنية إجرائياً بنزاهة.

النزاهة والسيادة في بناء "سجل الصحة الرقمي"

- مفهوم "السيادة المعلوماتية الحيوية": حماية البيانات الطبية للموظفين من التلاعب أو الاستغلال.
- دور القائد في حماية صورة المؤسسة عبر ممارسات النزاهة في استخدام تقنيات الاستشعار.
- سيكولوجية الثقة في الرصد: بناء المصادقية عبر الشفافية في توضيح أهداف جمع البيانات الحيوية.
- صياغة ميثاق "أخلاقيات الرصد الصحي" لضمان توافقه مع الكرامة الإنسانية والسيادة الوطنية.

اليوم الثاني:

الهندسة التقنية لأجهزة الاستشعار والملبوسات

الربط البيئي السيادي وإدارة الهوية الرقمية للأجهزة

- أنواع أجهزة الاستشعار (الرقع الجلدية، الساعات الذكية، مستشعرات البيئة) وتكاملها بنزاهة.
- الأمان الرقمي كركيزة للرصد: حماية الأجهزة القابلة للارتداء من الاختراق أو "التزييف الحيوي".
- إدارة الهوية الرقمية (UAE Pass) وأثرها على موثوقية السجلات الصحية وتفسير مخاطر انتحال الشخصية.
- تمرين تقني: تصميم بروتوكول "التدفق الآمن للمعلومات" من المستشعر إلى منصة اتخاذ القرار.



أخلاقيات التفاعل مع أنظمة "التحذير الصحي الآلي"

- حدود استخدام الذكاء الاصطناعي في "التوصيات الطبية" دون انتهاك السرية أو فقدان الحكمة البشرية.
- حوكمة مخرجات أنظمة "توقع الإجهاد": الضمان الأخلاقي لعدم استخدام البيانات كأداة للضغط المهني.
- مفهوم "الأمانة في الرصد": تجنب الاعتماد الكلي على الآلة دون وجود "رقابة قيادية" بشرية ونزيهة.
- ورشة عمل: وضع ضوابط أخلاقية لاستخدام البيانات الضخمة في "تحسين جودة حياة الموظف".

اليوم الثالث:

الحياد والعدالة في إدارة البيانات الصحية الضخمة

النزاهة الرقمية ومكافحة الانحياز في التحليل الحيوي

- أخلاقيات "العدالة الرقمية": ضمان دقة المستشعرات لجميع الفئات وتجنب الانحياز الخوارزمي.
- الرقابة الأخلاقية على أنظمة "تقييم اللياقة": كيف نضمن الشفافية والنزاهة في توزيع المهام؟
- تطبيق قاعدة "الإرادة البشرية القيادية": التدخل لتفسير "تنبيه صحي آلي" قد يساء فهمه برمجياً.
- حساب معامل الثقة في أنظمة الاستشعار لتقليل احتمالات الخطأ الناتج عن "الهلوسة الرقمية" للبيانات.

حوكمة المسؤولية عن مخرجات "أنظمة الرصد الذكية"

- المسؤولية المهنية للقائد عند فشل مستشعر في إرسال "إنذار خطر" أو حدوث عطل في الشبكة السيادية.
- إدارة العلاقة مع مزودي حلول "Health-Tech" ضمان الشفافية والسيادة في معالجة البيانات.
- بناء أنظمة "التحقق المزدوج" لضمان عدم غياب الحكمة البشرية في قراءة الإنذارات الصحية الحساسة.
- تمرين محاكاة: إدارة أزمة تواصل ناتجة عن "تسريب بيانات صحية" وكيفية علاجها بنزاهة وشفافية.



اليوم الرابع:

المسؤولية المهنية وإدارة السمعة والخصوصية

القيادة الاتصالية وحماية السمعة في البيئة الذكية

- أخلاقيات إدارة أزمات "الخصوصية الصحية": الموازنة بين الشفافية والسيادة والوقار الحكومي.
- الرقابة على "البصمة الرقمية الصحية" وأثرها على حيادية ومصداقية القرار السيادي والقانوني.
- بناء نظام "الإفصاح الاستباقي للجهازية": ضمان الشفافية لتصفير فرص انتشار الشائعات حول بيئة العمل.
- التدقيق الأخلاقي على سلاسل "التوريد التقني" لضمان خلوها من الممارسات غير العادلة أو الضارة.

أخلاقيات الاستجابة للانتهاكات السيبرانية لأنظمة الاستشعار

- المسؤولية الأخلاقية في التبليغ عن الثغرات التقنية التي قد تؤدي لتشويه "الهوية الصحية" للموظف.
- فن التواصل الأخلاقي أثناء تعطل أنظمة الرصد: حماية الثقة عبر بيانات صادقة ونزيهة دون تضليل.
- إدارة "التعافي المؤسسي": إجراءات إعادة بناء الصورة بعد رصد انحراف في دقة أجهزة الاستشعار.
- بناء خطة "الحصانة الرقمية الصحية": تحصين منظومة الرصد ضد الهجمات أو الإهمال الممنهج.

اليوم الخامس:

هندسة الاستجابة الفورية وتصفير البيروقراطية في مواجهة المخاطر الصحية والمهنية الذكية

مختبر "النابض الحيوي" وإدارة الإنذارات الصحية الاستباقية تحت الضغط

- محاكاة "الانهيار الصامت" والسيادة الحيوية: وضع القادة في سيناريو معقد يحاكي تسرب غاز غير مرئي أو إجهاد حراري حاد يكتشفه نظام الاستشعار قبل أن يشعر به الموظفون، واختبار قدرتهم على قراءة "التوأم الرقمي الصحي" وتفعيل بروتوكولات العزل والوقاية بنزاهة ووضوح تام لضمان صفر إصابات.
- تصفير البيروقراطية في التدخل الوقائي: تطبيق مسار قرار "صفري الإجراءات" لإرسال الدعم الطبي أو أوامر الإخلاء الفوري بناءً على البيانات الحيوية اللحظية (Biometrics)، لضمان حماية المورد البشري دون انتظار التسلسل الإداري التقليدي، مع الحفاظ على الحصانة المعلوماتية للبيانات الصحية السيادية والريادة العالمية الشاملة.
- هندسة "الثقة البيومترية" تحت الأزمة: اختبار مهارة القائد في الموازنة بين تحليلات الذكاء الاصطناعي للحالة الصحية وبين "الإرادة البشرية القيادية" لضمان عدم إساءة فهم الإنذارات أو تحويل الرصد إلى أداة ضغط، وضمان استمرارية العمل بنزاهة تامة ودون المساس بجودة الحياة أو الخصوصية الشخصية للموظف.



المخرجات الرئيسية للدورة:

- امتلاك استراتيجيات "حصانة صحية رقمية" تضمن نزاهة التعامل مع بيانات الموظفين بنسبة 100%.
- القدرة على هندسة منظومات رصد "حظية وسيادية" بمرونة وتوافق مع متطلبات الريادة والتميز.
- إتقان أدوات الرقابة الأخلاقية على أنظمة الاستشعار لضمان الشفافية وتصفير مخاطر الانحياز.
- بناء سجل ممارسات فضلى في إدارة "البيانات الحيوية" يدعم اتخاذ القرار القيادي الآمن والمستدام.
- تحقيق جاهزية كاملة للمؤسسة والمسؤول للمنافسة في فئات التميز والريادة في جودة الحياة.

الفئة المستهدفة:

- القيادات والمدراء في إدارات السلامة والصحة المهنية، التحول الرقمي، والموارد البشرية.
- مسؤولو التميز المؤسسي، الأطباء المهنيون، وخبراء الاستراتيجية في الجهات السيادية.
- مستشارو التكنولوجيا الناشئة، مدراء السعادة وجودة الحياة، وفرق إدارة المخاطر.
- رؤساء فرق مشاريع تصفير البيروقراطية وتطوير الخدمات الحكومية الذكية.
- الكوادر الطموحة الساعية لامتلاك جدارات "خبير الرصد الصحي الذكي والنزاهة الرقمية".

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)