المؤسسة العربية للاستشارات والتدريب وتطوير الأداء

AINFCT | info@ainfct.com | www.ainfct.com

Information Privacy Professional-CIPP

فكرة الدورة

أصبحت خصوصية المعلومات محوراً أساسياً في إدارة المخاطر الرقمية، مع تزايد الاعتماد على البيانات، وتوسع الخدمات الإلكترونية، وتطور المتطلبات التنظيمية لحماية البيانات الشخصية. وتحتاج المؤسسات إلى كوادر قادرة على فهم مبادئ الخصوصية، وتحليل الالتزامات التنظيمية، وتصميم ضوابط عملية تحافظ على الثقة وتدعم الامتثال.

يركز هذا البرنامج التدريبي من AINFCT على بناء فهم مهني متكامل لمجالات خصوصية المعلومات، بما يشمل مبادئ حماية البيانات، والأطر القانونية والتنظيمية، وحقوق الأفراد، وإدارة الموافقات، ونقل البيانات، وتقييمات أثر الخصوصية، وحوكمة برامج الخصوصية داخل المؤسسة. كما يربط البرنامج بين متطلبات الخصوصية وممارسات الأمن السيبراني وإدارة المخاطر وحوكمة البيانات.

يوفر البرنامج قيمة تطبيقية واضحة من خلال تحويل المفاهيم القانونية والتنظيمية إلى ممارسات تشغيلية قابلة للتنفيذ، مما يساعد المشاركين على دعم بيئات عمل أكثر التزاماً وشفافية في التعامل مع البيانات.

أهداف الدورة

فيما يلي الأهداف الرئيسية لهذا البرنامج التدريبي:

- تحليل مبادئ خصوصية المعلومات وحماية البيانات.
- تفسير الالتزامات التنظيمية المرتبطة بالبيانات الشخصية.
- تطبيق ضوابط إدارة الموافقات وحقوق الأفراد.
- تقييم أثر الخصوصية في العمليات والأنظمة.
- دعم حوكمة برامج الخصوصية داخل المؤسسة.
- ربط الخصوصية بالأمن السيبراني وإدارة المخاطر.

منهجية الدورة

- عروض تفاعلية تربط المفاهيم التنظيمية بالتطبيق العملي.
- تمارين تحليل تدفقات بيانات وسيناريوهات معالجة.
- دراسات حالة حول طلبات الأفراد وحوادث الخصوصية.
- مناقشات موجهة حول الامتثال وحوكمة البيانات.
- مراجعات معرفية قصيرة في نهاية المحاور الرئيسية.

أثر الدورة على المنظمة

يمكن تعزيز إدارة الخصوصية المؤسسية من خلال:

- رفع مستوى الامتثال لمتطلبات حماية البيانات.
- تحسين الثقة في معالجة البيانات الشخصية.
- تقليل مخاطر الانتهاكات التنظيمية والتشغيلية.
- دعم حوكمة البيانات والشفافية المؤسسية.

أثر الدورة على المتدربين

يساعد البرنامج المشاركين على:

- فهم مفاهيم الخصوصية بلغة مهنية دقيقة.
- تحليل متطلبات حماية البيانات داخل العمليات.
- تطبيق أدوات تقييم أثر الخصوصية.
- التعامل مع حقوق الأفراد بفعالية.

الشهادات

شهادة معتمدة من AINFCT

الفئة المستهدفة

يناسب هذا البرنامج المهنيين الذين يتعاملون مع البيانات الشخصية أو يشاركون في إدارة الامتثال والحوكمة والأمن. كما يفيد العاملين الراغبين في تطوير مسار مهني في مجال خصوصية المعلومات وحماية البيانات.

- مسؤولو الخصوصية وحماية البيانات.
- مختصو أمن المعلومات والأمن السيبراني.
- فرق الامتثال والمخاطر والحوكمة.
- مديرو البيانات والتحول الرقمي.
- المهتمون بمسار CIPP المهني.

موضوعات الدورة

اليوم الأول: مدخل إلى خصوصية المعلومات وحماية البيانات

- تطور مفهوم الخصوصية في الاقتصاد الرقمي.
- العلاقة بين الخصوصية وأمن المعلومات وحوكمة البيانات.
- أنواع البيانات الشخصية والحساسة وشبه المعرفة.
- المبادئ العامة لمعالجة البيانات بصورة مسؤولة.
- أدوار ومسؤوليات الجهات المعنية بالخصوصية.

اليوم الثاني: الأطر التنظيمية والمفاهيم القانونية الأساسية

- المفاهيم الأساسية في قوانين حماية البيانات.
- الجهة المتحكمة والمعالج وصاحب البيانات.
- أسس المعالجة القانونية ومبررات الاستخدام.
- مبادئ العدالة والشفافية وتحديد الغرض.
- العلاقة بين السياسات الداخلية والمتطلبات التنظيمية.

اليوم الثالث: دورة حياة البيانات الشخصية

- جمع البيانات وتوثيق أغراض المعالجة.
- استخدام البيانات ومشاركتها داخل المؤسسة.
- تخزين البيانات والاحتفاظ بها وفق الحاجة.
- الأرشفة والتخلص الآمن من البيانات.
- توثيق تدفقات البيانات بين الأنظمة والأطراف.

اليوم الرابع: حقوق الأفراد وإدارة الطلبات

- حقوق الوصول والتصحيح والحذف والاعتراض.
- إدارة طلبات أصحاب البيانات بطريقة منظمة.
- التحقق من هوية مقدم الطلب.

- مواعيد الاستجابة والتوثيق الداخلي.
- التوازن بين الحقوق والاستثناءات المشروعة.

اليوم الخامس: الشفافية والإشعارات والموافقات

- صياغة إشعارات الخصوصية بلغة واضحة.
- إدارة الموافقات الصريحة والضمنية.
- سحب الموافقة وتحديث تفضيلات الأفراد.
- إشعارات ملفات الارتباط والتتبع الرقمي.
- اختبار وضوح الإشعارات وقابليتها للفهم.

اليوم السادس: حوكمة برنامج الخصوصية

- مكونات برنامج الخصوصية المؤسسي.
- السياسات والإجراءات وسجلات المعالجة.
- أدوار مسؤول حماية البيانات والفرق الداعمة.
- نماذج المساءلة والتقارير الداخلية.
- مؤشرات قياس نضج برنامج الخصوصية.

اليوم السابع: تقييم أثر الخصوصية

- أهداف تقييم أثر حماية البيانات.
- متى يجب تنفيذ تقييم أثر الخصوصية.
- تحديد المخاطر المرتبطة بالمعالجة الجديدة.
- اختيار الضوابط التخفيفية المناسبة.
- توثيق النتائج ومتابعة خطط المعالجة.

اليوم الثامن: الخصوصية حسب التصميم والافتراض

- مبادئ الخصوصية حسب التصميم.
- تقليل البيانات وتحديد مدة الاحتفاظ.
- إخفاء الهوية والتعمية وتقليل التعريف.

- إعدادات الخصوصية الافتراضية الآمنة.
- دمج الخصوصية في المشاريع والأنظمة الجديدة.

اليوم التاسع: الأمن السيبراني وحماية البيانات الشخصية

- الضوابط الأمنية الداعمة للخصوصية.
- التحكم في الوصول إلى البيانات الشخصية.
- التشفير وإدارة المفاتيح وحماية التخزين.
- مراقبة الاستخدام غير المصرح به للبيانات.
- الربط بين الحوادث الأمنية وانتهاكات الخصوصية.

اليوم العاشر: إدارة الأطراف الثالثة ونقل البيانات

- تقييم مخاطر الموردين ومعالجي البيانات.
- بنود الخصوصية في العقود والاتفاقيات.
- ضوابط مشاركة البيانات مع أطراف خارجية.
- نقل البيانات عبر الحدود والاعتبارات التنظيمية.
- مراقبة التزام الأطراف الثالثة باستمرار.

اليوم الحادي عشر: التسويق الرقمي والخصوصية

- استخدام البيانات في الحملات والتواصل التسويقي.
- إدارة التفضيلات والاعتراض على التسويق.
- ملفات الارتباط وتقنيات التتبع والتحليلات.
- التمييز بين الضروري والتحليلي والتسويقي.
- مخاطر التنميط واتخاذ القرار الآلي.

اليوم الثاني عشر: الذكاء الاصطناعي وتحليلات البيانات

- مخاطر الخصوصية في نماذج التحليل المتقدمة.
- تقليل البيانات في مشروعات الذكاء الاصطناعي.
- الشفافية في المعالجة الخوارزمية.

- التحيز والإنصاف واستخدام البيانات الحساسة.
- حوكمة الاستخدام المسؤول للبيانات.

اليوم الثالث عشر: إدارة حوادث الخصوصية

- تمييز حادث الخصوصية عن الحادث الأمني العام.
- تقييم نطاق الحادث والبيانات المتأثرة.
- إجراءات الإخطار الداخلي والخارجي.
- توثيق قرارات الاستجابة للحوادث.
- تحسين الضوابط بعد الحادث.

اليوم الرابع عشر: التدقيق والمراقبة والتحسين المستمر

- مراجعة الامتثال الداخلي لمتطلبات الخصوصية.
- تدقيق سجلات المعالجة والسياسات والإجراءات.
- اختبار الضوابط التشغيلية لحماية البيانات.
- مؤشرات الأداء والمخاطر في برنامج الخصوصية.
- خطط التحسين المستمر ونضج الخصوصية.

اليوم الخامس عشر: تطبيقات عملية ومراجعة شاملة

- تحليل سيناريوهات معالجة بيانات متعددة.
- إعداد نموذج مبسط لتقييم أثر الخصوصية.
- مراجعة حقوق الأفراد وإدارة الموافقات.
- ربط الخصوصية بالأمن والحوكمة والمخاطر.
- بناء خطة تطوير مهني في مجال الخصوصية.

course_daily_schedule

يمتد البرنامج لمدة 15 يوماً تدريبياً، بواقع 4 ساعات تدريبية يومياً. يبدأ كل يوم بمراجعة موجزة للمفاهيم السابقة، ثم عرض للمحور الرئيسي، يتبعه نقاش تطبيقي أو تمرين عملي قصير، وينتهي اليوم بخلاصة مركزة تربط الموضوعات بسياقات العمل الفعلية. يتم توزيع الوقت بما يوازن بين الشرح، والنقاش، والتطبيق، والمراجعة المعرفية.

course_assessment

يعتمد التقييم على المشاركة الفعالة، والتمارين التطبيقية، وتحليل السيناريوهات، والمراجعات القصيرة المرتبطة بمحاور البرنامج. يحصل المشاركون في نهاية البرنامج على شهادة حضور/إتمام من AINFCT وفق متطلبات الحضور والمشاركة المعتمدة.

course_key_competencies

- حوكمة خصوصية المعلومات.
- حماية البيانات الشخصية.
- إدارة حقوق الأفراد.
- تقييم أثر الخصوصية.
- إدارة الامتثال التنظيمي.
- حوكمة الأطراف الثالثة.

مكتب القاهرة الرئيسي
القاهرة، جمهورية مصر العربية
7 شارع وهران، الطيران، مدينة نصر
+201152466358
info@ainfct.com
ainfct.com
رقم التسجيل الضريبي: 472920235
مكتب مدريد الفرعي
مدريد، إسبانيا

شارع الصحة 3، وسط المدينة، 28013 مدريد
training@ainfct.com
ainfct.com