MERCURY

إعداد سياسات نظام حماية البيانات الشخصية

15 – 19 أغسطس 2027

القاهرة (مصر)



Dubai - UAE: +971 4 450 5697
Istanbul - Türkiye: +90 539 599 1206
Amman - Jordan: +962 79 712 3347

MERCURY

إعداد سياسات نظام حماية البيانات الشخصية

المرجع: 148549_120984 **التاريخ:** 15 – 19 أغسطس 2027 **المكان:** القاهرة (مصر) **الرسوم:** Euro 4000

مقدمة:

في ظل تزايد التحديات المرتبطة بحماية البيانات الشخصية، أصبحت الحاجة ملحة لتطوير سياسات فعالة تضمن الامتثال للتشريعات الوطنية والدولية. تهدف هذه الدورة التدريبية في إعداد سياسات نظام حماية البيانات الشخصية، إلى تزويد المشاركين بالمعرفة المتخصصة والمهارات العملية لإعداد سياسات حماية البيانات الشخصية وفقًا لأفضل المعايير. سيتم التركيز على مراحل إعداد السياسات، وتحديد الأدوار والمسؤوليات، ومبادئ الشفافية والمساءلة.

كما تُعنى دورة إعداد سياسات نظام حماية البيانات الشخصية، بفهم طبيعة البيانات الشخصية الحساسة وآليات التحكم بها داخل المؤسسات. يتعرف المشاركون على أدوات التقييم وتحديد المخاطر المتعلقة بانتهاكات الخصوصية. كما تتناول الدورة تطبيق السياسات ضمن الأنظمة الإدارية والإجراءات التشغيلية اليومية. تسعى الدورة في النهاية إلى تعزيز ثقافة الامتثال والوعي المؤسسي بأهمية حماية البيانات الشخصية كجزء من الحوكمة الرشيدة.

الفئات المستهدفة:

تستهدف دورة إعداد سياسات نظام حماية البيانات الشخصية، الفئات والمحترفين الذين يسعون لاكتساب المعرفة والمهارات:

- مسؤولو حماية البيانات في المؤسسات.
- موظفو أقسام تقنية المعلومات.
- موظفو أقسام الحوكمة والامتثال.
- مدراء الأمن السيبراني.
- مستشارو الخصوصية وحماية البيانات.
- المحامون المتخصصون في القانون الرقمي.
- العاملون في القطاعات الحكومية والخاصة.
- موظفو الموارد البشرية الذين يتعاملون مع البيانات الحساسة.
- مدراء المخاطر المؤسسية.
- المطورون ومصممو الأنظمة التقنية.

Dubai - UAE: +971 4 450 5697
Istanbul - Türkiye: +90 539 599 1206
Amman - Jordan: +962 79 712 3347

MERCURY

أهداف الدورة التدريبية:

في نهاية هذا البرنامج التدريبي في إعداد سياسات نظام حماية البيانات الشخصية، سيكون المشاركون قادرين على:

- تحديد المفاهيم الأساسية لحماية البيانات الشخصية.
- تحليل الأنظمة القانونية المحلية والدولية ذات الصلة.
- تطوير سياسات مؤسسية تتوافق مع الإطار القانوني والتنظيمي.
- تقييم احتياجات المؤسسة من حيث البيانات الشخصية الحساسة.
- تطبيق منهجيات فعالة لصياغة السياسات واللوائح.
- تصميم إجراءات الامتثال الداخلي لمراقبة تنفيذ السياسات.
- تحسين القدرة على رصد الانتهاكات والرد عليها بفعالية.
- تطوير استراتيجيات إشراك الموظفين في تطبيق السياسات.
- استخدام أدوات التقييم الذاتي وتحليل الفجوات التنظيمية.
- تنفيذ آليات التوثيق والتحديث الدوري لسياسات الحماية.
- مراجعة الحالات الواقعية لتعزيز التطبيق العملي.
- إعداد تقارير واضحة تعكس مستوى الالتزام المؤسسي.
- توظيف الحلول التقنية لدعم حماية البيانات.
- مواءمة السياسات مع معايير الحوكمة المؤسسية.
- اكتساب مهارات تيسير ورش العمل حول الخصوصية داخل المؤسسة.

الكفاءات المستهدفة:

سيكتسب المشاركون الكفاءات التالية من خلال برنامج إعداد سياسات نظام حماية البيانات الشخصية:

- القدرة على إعداد سياسة حماية بيانات شاملة.
- الإلمام بالأنظمة والتشريعات الخاصة بالخصوصية.
- تحليل البيانات وتحديد المخاطر المرتبطة بها.
- صياغة اللوائح المؤسسية بلغة قانونية دقيقة.
- تطبيق أدوات التقييم الذاتي المؤسسي.
- استخدام النماذج التنظيمية لدعم السياسات.
- تطوير برامج توعية وتدريب داخلي.
- مراقبة وتحديث السياسات بشكل دوري.

Dubai - UAE: +971 4 450 5697
Istanbul - Türkiye: +90 539 599 1206
Amman - Jordan: +962 79 712 3347

MERCURY

محتوى الدورة التدريبية:

الوحدة الأولى: المبادئ الأساسية لحماية البيانات الشخصية:

- تعريف البيانات الشخصية والبيانات الحساسة.
- أهمية حماية الخصوصية في البيئة الرقمية.
- المعايير الدولية لحماية البيانات مثل GDPR.
- التشريعات الوطنية والإقليمية ذات الصلة.
- الحقوق الأساسية للأفراد في ما يخص بياناتهم.
- المسؤوليات القانونية للمؤسسات.
- مبادئ الشفافية والمساءلة.
- أثر حماية البيانات على سمعة المؤسسة.
- العلاقة بين حماية البيانات والأمن السيبراني.

الوحدة الثانية: تحليل المتطلبات المؤسسية وإعداد السياسات:

- إجراء تحليل فجوة الامتثال في المؤسسة.
- تحديد البيانات التي تتطلب حماية خاصة.
- تقييم دورة حياة البيانات داخل المؤسسة.
- إعداد سياسة واضحة لجمع ومعالجة البيانات.
- تحديد مسؤوليات الأطراف المعنية داخل المؤسسة.
- إعداد هيكلية تنظيمية لحوكمة البيانات.
- ضمان التوافق مع المعايير القانونية والتقنية.
- صياغة السياسات بلغة مفهومة لجميع العاملين.
- اعتماد السياسة من قبل الإدارة العليا.

Dubai - UAE: +971 4 450 5697
Istanbul - Türkiye: +90 539 599 1206
Amman - Jordan: +962 79 712 3347

MERCURY

الوحدة الثالثة: تنفيذ وتطبيق السياسات المؤسسية:

- إدماج السياسات ضمن العمليات التشغيلية.
- تطوير دليل إجراءات تنفيذ السياسات.
- تدريب الموظفين على تطبيق السياسات بفعالية.
- متابعة الالتزام والامتثال الداخلي.
- تنفيذ آليات التحقق والتدقيق.
- التعامل مع حوادث اختراق البيانات.
- إعداد تقارير تقييم الأداء والسياسات.
- تكوين فرق عمل لمراقبة الحماية المستمرة.
- التنسيق مع فرق تقنية المعلومات والدعم القانوني.

الوحدة الرابعة: المراجعة والتقييم والتحديث المستمر:

- إجراء تقييم دوري لفعالية السياسات.
- تطوير أدوات لقياس الامتثال المؤسسي.
- استخدام مؤشرات الأداء الرئيسية KPIs.
- تحليل الحوادث وتوصيف الفجوات التنظيمية.
- مراجعة القوانين الجديدة وتحديث السياسة بناءً عليها.
- تعزيز الثقافة المؤسسية في مجال حماية البيانات.
- إشراك أصحاب المصلحة في عملية التحسين
- تنفيذ سياسات قائمة على المخاطر.
- إعداد خطة لتحسين الامتثال والاستجابة للطوارئ.

Dubai - UAE: +971 4 450 5697
Istanbul - Türkiye: +90 539 599 1206
Amman - Jordan: +962 79 712 3347

MERCURY

الوحدة الخامسة: إدارة المخاطر والامتثال في سياسات حماية البيانات:

- تحليل المخاطر المرتبطة بالبيانات الشخصية.
- تطوير خطة استجابة للحوادث المحتملة.
- الربط بين تقييم المخاطر وصياغة السياسات.
- إدارة الموافقات والاتفاقيات مع الأطراف الخارجية.
- ضمان حماية البيانات عند مشاركة المعلومات.
- التقييم المستمر لمزودي الخدمات السحابية.
- التعامل مع الطلبات القانونية بخصوص البيانات.
- التكامل بين سياسات الامتثال والمخاطر.
- وضع استراتيجية حماية قائمة على سيناريوهات واقعية.

خلاصة وتوصيات الدورة التدريبية:

تؤكد هذه الدورة التدريبية في إعداد سياسات نظام حماية البيانات الشخصية، على أهمية إعداد سياسات فعّالة وشاملة لحماية البيانات الشخصية ضمن بيئة العمل الرقمية. توفر للمشاركين الأدوات والإجراءات اللازمة لضمان التوافق مع الأنظمة القانونية وتحقيق الامتثال المؤسسي. من خلال تطبيق المفاهيم المطروحة، ستتمكن المؤسسات من تحسين أمن البيانات ورفع مستوى الوعي الداخلي. يُوصى بتطبيق هذه السياسات بشكل متكامل مع ممارسات الحوكمة وإدارة المخاطر.