الدورة التدريبية: أمن المعلومات القانوني والامتثال للتشريعات الرقمية

#CYB8448

الدورة التدريبية: أمن المعلومات القانوني والامتثال للتشريعات الرقمية

مقدمة الدورة التدريبية / لمحة عامة:

في ظل التطور المتسارع للتقنية، أصبحت التشريعات الرقمية وقوانين حماية البيانات من أهم التحديات التي تواجه المؤسسات. إن الفشل في الامتثال للوائح مثل اللائحة العامة لحماية البيانات) GDPR (أو قوانين الخصوصية المحلية يمكن أن يؤدي إلى غرامات باهظة، وفقدان ثقة العملاء، والإضرار بسمعة الشركة. تقدم هذه الدورة التدريبية المتخصصة لمتخصصي أمن المعلومات، المستشارين القانونيين، ومسؤولي الامتثال، المعرفة والمهارات اللازمة لـدمج الأمن السيبراني مع المتطلبات القانونية. سنتناول في هذه الدورة مفاهيم الأمن القانوني، أهم اللوائح الدولية والمحلية، وأفضل الممارسات لـتحقيق الامتثال. سيكتسب المشاركون القدرة على وضع سياسات أمنية تتوافق مع القوانين، تقييم المخاطر القانونية للبيانات، وبناء إطار حوكمة قوي. تهدف الدورة إلى بناء كوادر متخصصة في الأمن القانوني للبيانات، مما يضمن عمل المؤسسة ضمن الإطار القانوني. يستند المحتوى إلى أحدث المعايير وأفضل الممارسات الدولية، مع الاستفادة من إسهامات خبراء أكاديميين بارزين مثل البروفيسور دانيال ج. سولوف)Daniel J. Solove(، المعروف بأعماله في قانون الخصوصية وأمن المعلومات. يقدم BIG BEN Training Center هذه الدورة لتمكين المؤسسات من تحقيق التوازن بين الابتكار الرقمي والالتزام القانوني.

الفئات المستهدفة / هذه الدورة التدريبية مناسبة لـ:

- مديرو الأمن السيبراني.
- مسؤولو الامتثال والمخاطر.
- المستشارون القانونيون ومحامو الشركات.
- مديرو تقنية المعلومات.
- مسؤولو حماية البيانات (DPOs)
- الموظفون الإداريون في الأقسام التي تتعامل مع البيانات الحساسة.

القطاعات والصناعات المستهدفة:

- القطاع المالي والمصرفي.
- شركات التأمين.
- الرعاية الصحية.
- شركات التكنولوجيا.
- الجهات الحكومية وما في حكمها.
- الشركات متعددة الجنسيات.

الأقسام المؤسسية المستهدفة:

- إدارة الأمن السيبراني.
- الإدارة القانونية.
- إدارة الامتثال والحوكمة.
- إدارة تقنية المعلومات.
- إدارة المخاطر.

أهداف الدورة التدريبية:

بنهاية هذه الدورة التدريبية، سيكون المتدرب قد أتقن المهارات التالية:

- فهم العلاقة بين الأمن السيبراني والتشريعات القانونية.
- القدرة على تفسير اللوائح القانونية الرئيسية لحماية البيانات.
- تطبيق ضوابط أمنية تتوافق مع متطلبات الامتثال.
- وضع سياسات وإجراءات لحماية البيانات الحساسة.
- إجراء تقييم للمخاطر القانونية المتعلقة بأمن المعلومات.
- التعامل مع حوادث انتهاك البيانات من منظور قانوني.
- بناء إطار حوكمة قوي لأمن المعلومات.

منهجية الدورة التدريبية:

تعتمد هذه الدورة التدريبية منهجية تفاعلية وعملية، مصممة لربط المفاهيم القانونية بالواقع التقني لأمن المعلومات. سيتمكن المتدربون من خلال دراسات الحالة الواقعية لغرامات قانونية فرضت على مؤسسات بسبب انتهاكات أمنية، وورش العمل التطبيقية، من فهم كيفية صياغة سياسات أمنية تتوافق مع القوانين. تتضمن المنهجية مناقشات متعمقة حول التحديات القانونية للأمن السحابي والتحقيقات الجنائية الرقمية. سيتم التركيز على تحقيق الامتثال كعملية مستمرة، وليس مجرد إجراء لمرة واحدة. يقدم BIG BEN Training Center هذه الدورة لتمكين المؤسسات من بناء بيئة رقمية آمنة وممتثلة قانونيًا.

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: أساسيات الأمن القانوني للبيانات

- مقدمة إلى قوانين حماية البيانات والخصوصية.
- الفرق بين الأمن السيبراني والامتثال القانوني.
- أهمية الامتثال لتجنب العقوبات والمخاطر.
- التشريعات الدولية الرئيسية (GDPR, CCPA)
- التشريعات المحلية وقوانين الأمن السيبراني.
- مفاهيم البيانات الشخصية والبيانات الحساسة.
- الحقوق والالتزامات بموجب قوانين حماية البيانات.

الوحدة الثانية: إطار الحوكمة والأمن

- بناء إطار حوكمة لأمن المعلومات.
- وضع السياسات والإجراءات الأمنية.
- دور مسؤول حماية البيانات (DPO)
- إدارة المخاطر الأمنية من منظور قانوني.
- التدقيق الأمني والامتثال.
- تكامل الأمن السيبراني في استراتيجية الأعمال.
- تحديد الأدوار والمسؤوليات.

الوحدة الثالثة: الامتثال القانوني في الممارسات الأمنية

- متطلبات التشفير وتخزين البيانات.
- تأمين الوصول إلى البيانات الحساسة.
- التعامل مع سجلات المراقبة والبيانات.
- أمن العقود الرقمية والتوقيع الإلكتروني.
- الامتثال في الخدمات السحابية وموردي الطرف الثالث.
- حماية الملكية الفكرية الرقمية.
- أمن البريد الإلكتروني والاتصالات.

الوحدة الرابعة: الاستجابة للحوادث من منظور قانوني

- تطوير خطة الاستجابة للحوادث الأمنية.
- الإبلاغ عن انتهاكات البيانات إلى الجهات التنظيمية.
- التعامل مع حوادث الأمن وفقًا للقانون.
- التحقيقات الجنائية الرقمية وجمع الأدلة.
- التواصل مع العملاء بعد وقوع حادث.
- تجنب المسؤولية القانونية في حالة الحوادث.
- التعافي القانوني بعد وقوع الحادث.

الوحدة الخامسة: مستقبل التشريعات والأمن السيبراني

- التشريعات الناشئة في مجال الذكاء الاصطناعي.
- الامتثال في عالم إنترنت الأشياء(IoT)
- تحديات الأمن القانوني في العملات الرقمية.
- دور الذكاء الاصطناعي في الامتثال.
- التعاون بين الإدارة القانونية والأمن السيبراني.
- المرونة القانونية في بيئة الأعمال المتغيرة.
- تأثير الأمن القانوني على الابتكار.

الأسئلة المتكررة:

ما هي المؤهلات أو المتطلبات اللازمة للمشاركين قبل التسجيل في الدورة؟

لا توجد شروط مسبقة.

كم تستغرق مدة الجلسة اليومية، وما هو العدد الإجمالي لساعات الدورة التدريبية؟

تمتد هذه الدورة التدريبية على مدار خمسة أيام، بمعدل يومي يتراوح بين 4 إلى 5 ساعات، تشمل فترات راحة وأنشطة تفاعلية، ليصل إجمالي المدة إلى 20–25 ساعة تدريبية.

سؤال للتأمل:

في ظل التطور السريع للتقنيات والتشريعات الرقمية، كيف يمكن للمؤسسات أن تبتكر إطارًا قانونيًا وأمنيًا لا يقتصر على مجرد الامتثال للوائح الحالية، بل يُنشئ ثقافة حوكمة استباقية، ويُمكن المؤسسة من التكيف مع التغييرات القانونية المستقبلية، ويضمن حماية البيانات كأولوية قصوى لتعزيز الثقة والنمو المستدام؟

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

تتميز هذه الدورة بتركيزها المتخصص على التقاطع بين الأمن السيبراني والتشريعات القانونية، مما يوفر محتوى مصممًا خصيصًا لدمج هذين المجالين الحيويين. بدلاً من تناول كل مجال على حدة، نغوص في التطبيق العملي لتحقيق الامتثال، من صياغة السياسات الأمنية إلى التعامل مع الحوادث من منظور قانوني. تقدم الدورة دراسات حالة واقعية لانتهاكات بيانات أدت إلى عواقب قانونية، مع تحليل مفصل لنتائجها وكيفية تجنبها. نركز على بناء إطار حوكمة قوي يُمكن المؤسسة من حماية أصولها الرقمية مع الالتزام الكامل بالقوانين. إنها ليست مجرد دورة نظرية، بل هي برنامج تدريبي مكثف يهدف إلى بناء متخصصين في الأمن قادرين على العمل في إطار قانوني سليم.