AKADEMIA B&B

OCHRONA DANYCH I BEZPIECZEŃSTWO INFORMACJI PODCZAS PRACY ZDALNEJ

Organizuj pracę zdalną bezpiecznie i zgodnie z prawem! Ogranicz ryzyka, wyeliminuj błędy, bądź świadomy zagrożeń.

Warto zweryfikować, czy dotychczas stosowane rozwiązania są zgodne z obowiązującymi wytycznymi i przepisami prawa, w szczególności przepisami ochrony danych osobowych. Otoczenie w jakim pracujemy ma niewątpliwie ogromny wpływ na bezpieczeństwo informacji, a praca zdalna niesie za sobą zwiększoną podatność na ewentualny atak.

Cel szkolenia?

Nowe przepisy regulujące zasady pracy zdalnej określają obszary, na których należy się skupić, umożliwiając pracownikowi pracę na jasno określonych zasadach. Podczas szkolenia uczestnicy dowiedzą się nie tylko w jaki sposób zorganizować pracę zdalną, aby była zgodna z RODO, ale także w jaki sposób postępować, by zminimalizować ryzyko wycieku danych.

Omówimy przykłady nieświadomego naruszenia bezpieczeństwa informacji, zasady użytkowania sprzętu służbowego i prywatnego oraz sposoby ochrony sieci domowej. Na co zwracać uwagę podczas telekonferencji, co z hasłami i dostępem do dokumentów, ze wskazaniem na szyfrowanie i bezpieczeństwo danych, zarówno tych w formie elektronicznej, jak i papierowej wyniesionej poza siedzibę firmy.

Szkolenia dedykowane są dla klientów biznesowych i instytucjonalnych, włączając w to MŚP, duże przedsiębiorstwa, jak również administrację publiczną.

Jak szkolimy?

Szkolenie realizowane jest w formie mini wykładu. Łączy w sobie wiedzę merytoryczną z praktycznymi przykładami jej wykorzystania w środowisku pracy.

Pozwalamy naszym klientom mieć realny wpływ na kształt i merytoryczną zawartość szkolenia. Na wstępie przeprowadzimy badania ankietowe online z wiedzy o podstawowych aspektach cyberbezpieczeństwa i stosowanych procedurach IT. Wyniki ankietyzacji uwypuklą obszary, na których się skupimy i które omówimy w trakcie szkolenia

Informacje ogólne

Szkolenia mogą być prowadzone w formule otwartej i zamkniętej.

Szkolenie będzie prowadzone w języku polskim.

Szkolenia trwają ok. 6 h.

W przypadku szkoleń trwających do 3 godzin, przewiduje się jedną przerwę trwającą 15 minut. W przypadku szkoleń trwających powyżej 3 godzin, organizowane będą dwie przerwy trwające 15 minut każda.

Dysponujemy potencjałem dydaktycznym i rozbudowanym zapleczem technicznym – mobilna pracownia komputerowa oraz sprzęt komputerowy dla prowadzących umożliwiający przeprowadzenie szkolenia wraz ekran i projektorem.

Mogą się odbywać stacjonarnie, na zamówienie Klienta, w miejscu przez niego wyznaczonym lub w naszej Siedzibie. Szkolenie przeprowadzone powinno być w grupach liczących do 25 pracowników.

Jesteśmy ponadto otwarci i przygotowani na realizację szkolenia w formie online. Liczba uczestników do ustalenia.

Niezależnie od formy, zobowiązujemy się do prowadzenia dokumentacji wszystkich szkoleń w jednakowy sposób – na dokumentację szkolenia składają się:

- lista obecności uczestników szkolenia (w przypadku szkolenia online – raport uczestnictwa i raport końcowy po spotkaniu),
- ankiety satysfakcji sporządzone po każdym szkoleniu wraz z raportem.

Kto prowadzi szkolenia?

Szkolenia prowadzone są przez praktyków, którzy na co dzień mają styczność z szeroko rozumianym bezpieczeństwem informacji i bezpieczeństwem w cyberprzestrzeni. Dostarczają rzetelną wiedzę, która daje uczestnikom przewagę w szybko zmieniającym się świecie cyberbezpieczeństwa i sprawnie wykorzystują swoje doświadczenie zebrane podczas spotkań z pracownikami wszystkich szczebli w administracji publicznej i sektora prywatnego.

KATARZYNA GLIB

Inspektor Ochrony Danych, Certyfikowany Audytor Wiodący normy ISO 27001, szkoleniowiec

Odpowiedzialna za tworzenie i wdrażanie Systemów Zarządzania Bezpieczeństwem Informacji, z uwzględnieniem zasad ochrony danych osobowych oraz audytowanie w/w obszarów w podmiotach publicznych i prywatnych. Wykonuje opracowania z zakresu bezpieczeństwa informacji, badania zgodności z normami, przepisami prawa i ładu korporacyjnego.

Realizuje audyty z zakresu ochrony danych osobowych, bezpieczeństwa informacji oraz KRI, KSC.

ADRIAN KAMIZELA

Certyfikowany Audytor Wiodący normy ISO 27001, szkoleniowiec

Wyspecjalizowany w zakresie szeroko pojętej technologii IT, w tym sieci komputerowych i bezpieczeństwa systemów komputerowych oraz komputerowych systemach zarządzania i sterowania. Realizuje audyty bezpieczeństwa danych w systemach informatycznych i sieci ICT oraz KRI i KSC. Bierze pod lupę aspekty techniczne analizując oprogramowanie, serwisy WWW i pocztowe. Weryfikuje wszelkie ustanowione zabezpieczenia informacji przed nieuprawnionym dostępem.

Trenerzy pracujący w Akademii BB są pasjonatami symulacji biznesowych jako narzędzi do praktycznej nauki oraz angażowania uczestników szkoleń, dzięki którym zdobywają oni wyłącznie umiejętności przydatne w życiu, tym zawodowym, jak i prywatnym. Posiadają wszechstronną wiedzę, wielokierunkowe wykształcenie, praktyczne doświadczenie. Kładą nacisk na praktyczne podejście dostosowując je do aktualnej grupy odbiorców jego szkoleń.

Trenerzy w pełni odpowiadają za zawartość merytoryczną szkoleń, ich zakres i dobór materiałów.

Agenda szkolenia**:

1	Czym jest bezpieczeństwo informacji?
2	Czym jest dana osobowa? Podstawowe zasady ochrony danych osobowych.
3	Ochrona informacji i danych osobowych. Kiedy informacje nie są danymi osobowymi?
4	Bezpieczna praca zdalna: prawa i obowiązki pracownika.
5	Zabezpieczenia fizyczne. Zasady czystości w bezpieczeństwie danych i informacji.
6	Jakie kryteria, w tym techniczne i organizacyjne, wpływają na poziom bezpieczeństwa?
7	Praca na urządzeniu służbowym i prywatnym, a bezpieczeństwo danych firmowych.
8	Dobre praktyki porozumiewania się na odległość.
9	Wynoszenie dokumentów i nośników zawierających dane osobowe poza miejsce przetwarzania. Zasady korzystania z elektronicznych nośników informacji.
10	Metody i środki uwierzytelnienia.
11	Bezpieczne hasła, menedżer haseł, autoryzacja dwuetapowa, klucze sprzętowe.
12	Sieć domowa, a zaufane dostępy do sieci.
13	Zarządzanie tożsamością i uprawnieniami w systemach informatycznych do przetwarzania danych.
14	Bezpiecznie przetwarzanie danych: szyfrowanie, przechowywanie, udostępnianie, komunikacja.
15	Zdalny dostęp do zasobów jednostki oraz związane z tym potencjalne zagrożenia.
16	Zasady korzystania z poczty elektronicznej.
17	Bezpieczeństwo danych w chmurze.
18	Bezpieczeństwo podczas korzystania z przeglądarek internetowych.

19	Incydenty bezpieczeństwa informacji i zasady sprawnego zarządzania.
20	Prywatność w sieci czyli: trackery, ciastka, tryb incognito.
21	Ataki sieciowe i komputerowe. Omówienie zagrożeń takich jak phishing, ransomware, malware, socjotechnika, atak telefoniczny, spoofing.

**

Zakres szkolenia może być dowolnie konfigurowany w zależności od rodzaju działalności i procesów w niej zachodzących.

Co po szkoleniu?

Szkolenie zakończone testem zdobytej wiedzy – test przeprowadzony z wykorzystaniem urządzeń mobilnych (każdy uczestnik szkolenia otrzyma link).

Uczestnik szkolenia otrzyma pakiet materiałów szkoleniowych w formie elektronicznej.

Szkolenie jest certyfikowane. Uczestnik po zakończeniu szkolenia otrzyma stosowne zaświadczenie ukończenia szkolenia. W przypadku przeszkolenia wszystkich pracowników, certyfikat uzyska dana Instytucja.

Jesteś zainteresowany ofertą?

Jeśli masz dodatkowe pytania lub chcesz zapoznać się z naszą ofertą zapraszamy do kontaktu z opiekunami handlowymi.