Zał. nr.6

INFORMACJE DODATKOWE DO OCENY RYZYKA

Zamawiający:
Nazwa: Politechnika Częstochowska
Adres siedziby: ul. Dąbrowskiego 69, 42-201 Częstochowa

INFORMACJE OGÓLNE

1. Data rozpoczęcia działalności: 30 listopada 1949
2. Rodzaj przeważającej działalności (z numerem PKD): Dydaktyka
3. Liczba zatrudnionych pracowników: 1 220
4. Budżet na 2019 rok: 149 570 000 zł
5. Politechnika Częstochowska do tej pory nie ubezpieczała się w zakresie ryzyk cybernetycznych. Brak informacji o szkodach w tym zakresie.

Dodatkowe informacje dotyczące działalności w zakresie ryzyk cybernetycznych:

Politechnika:
- Stosuje oprogramowanie antywirusowe i zaporę Firewall w całości sieci,
- Tworzy kopię zapasową istotnych danych co najmniej raz na 5 dni,
- Nie przetwarza danych kart płatniczych,
- Nie doznała przestoju sieci trwającego ponad 4 godz. lub jakiegokolwiek naruszenia, czy ataku przy użyciu wirusa lub złośliwego kodu w ciągu ostatnich 24 mies.
- Nie zostały utracone lub ujawnione dane osobowe, dane wrażliwe za które ponosi odpowiedzialność w ciągu ostatnich 36 mies.
- Nie prowadzi działalności w branżach: hazard, zakłady bukmacherskie, kontrola ruchu lotniczego, instytucje rządowe
- Odpowiedzialnym za bezpieczeństwo sieci i danych jest odpowiedzialny kierownik,
- Stosuje automatyczną aktualizację sygnatury wirusów
- Stosuje automatyczną aktualizację istotnych danych
- Stosowane są instrukcje zarządzania systemami informatycznymi.
- Wymaga zmiany haseł co najmniej raz na 3 miesiące
- Stosuje ograniczony dostęp do wrażliwych danych
- Dokonuje przeglądu polityki bezpieczeństwa raz w roku zgodnie z KRI
- Posiada możliwość odzyskania kluczowych systemów w ciągu 6h
- Posiada Centrum zapasowe w innym budynku dedykowanej serwerowni
- Nie posiada więcej niż 1 mln rekordów danych osobowych
- Nie są znane okoliczności które mogą stanowić podstawę do szkody z ryzyk cyber
- Nie otrzymała wypłaty odszkodowania z polisy cyber w ciągu ostatnich 3 lat
- Nie posiada polisy ryzyk cybernetycznych
- Nie prowadzi działalności i nie dostarcza produktów do krajów objętych sankcjami lub embargiem
- Sprawdza regularnie zmiany przepisów prawa oraz wytyczne dotyczące bezpieczeństwa i ochrony danych
- Stosuję oprogramowanie antywirusowe na wszystkich urządzeniach informatycznych, serwerach i systemach
- Spełnia wymogi ustawy o ochronie danych osobowych oraz rozporządzenia MSWiA w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i

organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczny służące do przetwarzania danych osobowych w zakresie systemu teleinformatycznego
- Nie posiada narzędzi teleinformatycznych, które pozwolą stwierdzić, że doszło do naruszenia środowiska teleinformatycznego
- Wyznaczono osobę za bezpieczeństwo teleinformatyczne
- Stworzona jest polityka ochrony danych osobowych, bezpieczeństwa informacji
- pracownicy są przeszkoleni w zakresie polityki ochrony danych osobowych, bezpieczeństwa informacji
- Posiada plan działania w przypadku wystąpienia incydentu naruszenia bezpieczeństwa danych osobowych
- Nie przetwarza danych za pośrednictwem chmury obliczeniowej
- Nie funkcjonuje klasyfikacja informacji
- Stosuję mechanizm blokowania dostępu do wybranych stron internetowych
- Nie ma podłączonych do sieci publicznych systemów operacyjnych, serwerów i sieci
- Stosuję ochronę sieci z podziałem na Vlany
- Nie wykorzystuje outsourcing usług teleinformatycznych
- Nie weryfikuję historii zatrudnienia i przeszłości (w tym kryminalną) wszystkich pracowników i niezależnych doradców
- Nie wymaga, by podwykonawcy zbierający, przetwarzający dane w imieniu Politechniki posiadali ubezpieczenie chroniące przed konsekwencjami ujawnienia, wycieku, utraty danych
- Stosuję uwierzytelnienie przy łączeniu się z wewnętrzną siecią komputerową lub systemem informatycznym
- Posiada i stosuje procedury dotyczące kopii bezpieczeństwa oraz odzyskiwania danych w systemach krytycznych i zasobach w których są przechowywane dane i informacje