

## INFORMACJE DODATKWE DO OCENY RYZYKA

### Zamawiający:

Nazwa: Politechnika Częstochowska

Adres siedziby: ul. Dąbrowskiego 69, 42-201 Częstochowa

Adresy innych lokalizacji objętych ubezpieczeniem:

1. ul. Armii Krajowej 17, 19, 19A, 19B, 19C, 21, 23/25, 36. 36B, Częstochowa
2. ul. Wały Dwernickiego 123, Częstochowa
3. ul. Brzeźnicka 60, 60A, Częstochowa
4. ul. Akademicka 1. 3, 3a, 5, Częstochowa
5. ul. Dąbrowskiego 69 do 75, Częstochowa
6. ul. Gombrowicza 1, Częstochowa
7. ul. Dekabrystów 26/30, Częstochowa
8. ul. Sowińskiego 40/48, Częstochowa

### INFORMACJE OGÓLNE

1. Data rozpoczęcia działalności: 30 listopada 1949
2. Rodzaj przeważającej działalności (z numerem PKD): Dydaktyka
3. Zamawiający nie wykonuje prac ziemnych i podziemnych.
4. Zamawiający nie wykonuje prac z użyciem młotów kafarów lub walców.
5. Liczba zatrudnionych pracowników: **1 220**
6. Budżet na 2019 rok: **149 570 000 zł**
7. Krótki opis/informacje dodatkowe: Politechnika Częstochowska jest państwową szkołą wyższą działającą na podstawie aktualnej ustawy o szkolnictwie wyższym
8. Zamawiający nie wynajmuje pomieszczeń od innych podmiotów TAK
9. Zamawiający wynajmuje pomieszczenia innym podmiotom TAK

- automaty sprzedające
- usługi kserograficzne
- gabinet stomatologiczny
- Telewizja Polska S.A.
- bankomat
- działalność gastronomiczna
- policealne STUDIUM OPTYCZNE
- Euronet Polska Sp. z o. o.
- sale sportowe
- telefonia komórkowa
- firma zajmująca się robotami drogowymi i budowlanymi
- firma zajmująca się działalnością logistyczną
- firma zajmująca się metalizacją próżniową

Wskazane w SIWZ lokalizacje nie znajdują się na terenie zalewowym.

Na terenach wymienionych w SIWZ począwszy od 1997 r. nie wystąpiła powódź.

## **Dodatkowe informacje dotyczące działalności w zakresie ryzyk cybernetycznych:**

Politechnika:

- Stosuje oprogramowanie antywirusowe i zapórę 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
- 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
- Stosuje 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
- Stosuje mechanizm blokowania dostępu do wybranych stron internetowych
- Nie ma podłączonych do sieci publicznych systemów operacyjnych, serwerów i sieci
- Stosuje ochronę sieci z podziałem na Vlany
- Nie wykorzystuje outsourcing usług teleinformatycznych
- Nie weryfikują 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
- Stosuje 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