KWESTIONARIUSZ CYBER – STAROSTWO POWIATOWE JAROSŁAW

1. Całkowita liczba rekordów (danych osobowych dot. osób fizycznych), za które Zamawiający jest prawnie odpowiedzialny (gromadzi je, przechowuje, przetwarza) 100.000, w podziale na:

1)	Informacje o kartach płatniczych	
2)	Dane o dokumentach tożsamości, numery identyfikacji podatkowej lub PESEL	100.000
3)	Inne dane osobowe	
4)	Dane o stanie zdrowia	
5)	Inne dane finansowe (oprócz kart płatniczych)	

2. Przychody Zamawiającego za ostatni rok obrotowy (2023) **– 70.810.716,67 zł**

3. Zamawiający jest jednostką samorządu terytorialnego. ☒ TAK ☐ NIE
4. Przychody uzyskiwane rocznie z USA nie przekraczają 25% całkowitego rocznego przychodu Zamawiającego NIE DOTYCZY
5. Całkowita liczba rekordów (danych osobowych dot. osób fizycznych), za które Zamawiający jest prawnie odpowiedzialny (gromadzi je, przechowuje, przetwarza) **nie przekracza 100.000.** ☒ TAK ☐ NIE
6. Zamawiający stosuje zapory sieciowe (firewall) przeznaczone do użytku komercyjnego, na wszystkich zewnętrznych bramach sieciowych oraz aplikacje antywirusowe przeznaczone do użytku komercyjnego, w całej sieci włączając w to serwery lub punkty końcowe oraz urządzenia przenośne. ☒ TAK ☐ NIE
7. Zamawiający lub jego dostawca usług w chmurze tworzy kopię zapasową istotnych danych co najmniej raz na 7 dni, a te zarchiwizowane dane są przechowywane w trybie offline w środowisku oddzielonym od pozostałej sieci, a ich integralność jest testowana co najmniej co 180 dni. ☒ TAK ☐ NIE
8. Zamawiający instaluje poprawki krytyczne oprogramowania uważane przez producenta za obowiązkowe w ciągu 30 dni od ich wydania. ☒ TAK ☐ NIE
9. Zamawiający zabezpiecza hasłem lub biometrycznie wszystkie swoje nośniki przenośne, w tym laptopy, smartfony i pendrive'y. ☒ TAK ☐ NIE
10. Zamawiający potwierdza, że nie wie o jakimkolwiek zdarzeniu, które może spowodować jakiekolwiek straty lub roszczenia, ani on sam nie poniósł żadnej straty, ani nie zostały wniesione przeciwko niemu żadne roszczenia, w związku z którymi można by uzyskać odszkodowanie w ramach polisy ubezpieczenia od ryzyk cybernetycznych. ☒ TAK ☐ NIE
11. Jak często Zamawiający (lub dostawca usług w chmurze) wykonuje kopie zapasowe danych niezbędnych do prowadzenia działalności (danych krytycznych)?

    ☐ raz na 5 dni ☒ inaczej, proszę podać jak: **co najmniej 5 dni w tygodniu**
12. Czy dane krytyczne przechowywane są w trybie offline w odseparowanym od sieci środowisku i testowane pod kątem integralności raz na:

    ☐ 30 dni, ☒ 90 dni, ☐ inaczej, proszę podać jak:
13. Czy wyłączono protokół RDP (Remote Desktop Protocol) na wszystkich punktach końcowych sieci, w tym na serwerach, na których protokół RDP nie jest wymagany? ☒ TAK ☐ NIE
14. Czy wszystkie dane osobowe w sieci są szyfrowane:

a) podczas przesyłania ☒ TAK ☐ NIE
b) podczas przechowywania na serwerach ☐ TAK ☒ NIE
c) podczas tworzenia kopii zapasowych ☐ TAK ☒ NIE
d) podczas przechowywania w urządzeniach przenośnych ☒ TAK ☐ NIE

15. Czy zdalny dostęp do sieci oraz danych osobowych jest zabezpieczony za pomocą co najmniej dwupoziomowego uwierzytelnienia? ☒ TAK ☐ NIE
16. Jak często aktualizowane są sygnatury wirusów?

    ☐ automatycznie ☒ codziennie ☐ co tydzień ☐ inaczej, proszę podać jak:
17. Jak często przeprowadzany jest zewnętrzny audyt bezpieczeństwa?

    ☐ raz w roku ☐ nigdy ☐ inaczej, proszę podać jak**: planowany w miarę możliwości finansowych**
18. Kto jest odpowiedzialny za zachowanie bezpieczeństwa sieci? **Administrator Danych, Administrator Systemów Informatycznych, Inspektor Ochrony Danych**
19. Jak często przeprowadzane są istotne aktualizacje?

    ☒ automatycznie ☐ co tydzień ☐ inaczej, proszę podać jak:
20. Czy Zamawiający wdrożył politykę audytowania i zarządzania kontami użytkowników? ☒ TAK ☐ NIE
21. Czy Zamawiający wymaga zmiany haseł co najmniej raz na trzy miesiące? ☒ TAK ☐ NIE
22. Czy dostęp do wrażliwych danych jest ograniczony zgodnie z wymogami użytkownika? ☒ TAK ☐ NIE
23. Czy Zamawiający stosuje się do aktualnych krajowych i międzynarodowych przepisów regulujących postępowanie z danymi osobowymi (np. RODO, APP)? ☒ TAK ☐ NIE
24. Jak często Zamawiający dokonuje przeglądu polityki bezpieczeństwa informacji? W ramach sprawdzeń i audytów

    ☒ raz w roku ☐ nigdy ☐ inaczej, proszę podać jak:
25. Czy Zamawiający posiada spisany plan zachowania ciągłości działalności, który jest poddawany corocznemu przeglądowi? ☐ TAK ☒ NIE
26. Czy plan zachowania ciągłości działalności firmy uwzględnia ocenę zagrożeń w cyberprzestrzeni? ☐ TAK ☒ NIE
27. Zależność sieciowa – po jakim czasie utrata połączenia z siecią zacznie oddziaływać na działalność?

    ☐ 6 h ☐ 12 h ☐ 24 h ☐ 48 h ☒ inaczej, proszę podać jak: **72 h**
28. Jak długo zajmie pełne odzyskanie kluczowych systemów?

    ☐ 6 h ☐ 12 h ☐ 24 h ☒ 48 h ☐ inaczej, proszę podać jak:
29. Czy Zamawiający dokonuje corocznych testów DRP (usuwania skutków awarii) / BCP (ciągłości biznesowej)? ☐ TAK ☒ NIE
30. Czy Zamawiający (lub partner zewnętrzny/dostawca usług w chmurze) dokonał konfiguracji sieci w celu zapewnienia wysokiej dostępności lub przejmowania funkcji przez system rezerwowy w odniesieniu do strony internetowej i innych istotnych aplikacji? ☒ TAK ☐ NIE
31. Jak często przeprowadzane są testy integralności danych?

    ☐ co tydzień ☐ co miesiąc ☒ rocznie ☐ nigdy ☐ inaczej, proszę podać jak:
32. Czy w ciągu ostatnich 24 miesięcy Zamawiający doznał awarii (nie dotyczy awarii zasilania) trwającej ponad 4 godziny lub jakiegokolwiek naruszenia, które mogłoby prowadzić do straty lub wniesienia roszczenia gdyby polisa cyber obowiązywała? Jeżeli tak, proszę podać szczegółowe informacje. ☐ TAK ☒ NIE
33. Czy w ciągu ostatnich 36 miesięcy dane wrażliwe lub osobowe, za które Zamawiający ponosi prawną odpowiedzialność, były narażone na atak lub utracone? Jeżeli tak, proszę podać szczegółowe informacje. ☐ TAK ☒ NIE