|  |  |  |  |
| --- | --- | --- | --- |
| **L.p.** | **TAK/NIE** | **W przypadku braku zabezpieczenia należy uzasadnić** | **Wdrożone środki bezpieczeństwa** |
| **I. Środki ochrony fizycznej** |
|  |  |  | Serwery zlokalizowane są na terytorium Europejskiego Obszaru Gospodarczego. |
|  |  |  | Serwery zlokalizowane są w pomieszczeniach z dostępem wyłącznie dla osób posiadających nadane uprawnienia (System Kontroli Dostępu – SKD, System Zarzadzania Kluczami - SZK). |
|  |  |  | Służba ochrony prowadzi całodobową, fizyczną ochronę budynku. |
|  |  |  | Hol główny i teren wokół budynku jest objęty monitoringiem wizyjnym (CCTV). |
|  |  |  | Dane osobowe Zamawiającego są przechowywane w pomieszczeniu zabezpieczonym drzwiami zwykłymi (nie wzmacnianymi, nie przeciwpożarowymi). |
|  |  |  | Dane osobowe Zamawiającego są przechowywane w pomieszczeniu zabezpieczonym drzwiami o podwyższonej odporności ogniowej. |
|  |  |  | Dane osobowe Zamawiającego są przechowywane w pomieszczeniu zabezpieczonym drzwiami o podwyższonej odporności na włamanie. |
|  |  |  | Dane osobowe Zamawiającego (w tym dane są przechowywane w pomieszczeniu, w którym okna zabezpieczone są za pomocą krat, rolet lub folii antywłamaniowej. |
|  |  |  | Pomieszczenia wyposażone są w system alarmowy przeciwwłamaniowy (SSWiN). |
|  |  |  | Dostęp do pomieszczeń objęty jest systemem kontroli dostępu (SKD). |
|  |  |  | Dostęp do pomieszczeń objęty jest zasadami zarządzania dostępem do kluczy do pomieszczeń (np. system zarzadzania kluczami, depozytory - SZK) |
|  |  |  | Dostęp do pomieszczeń kontrolowany jest przez system monitoringu z zastosowaniem kamer przemysłowych (CCTV). |
|  |  |  | Dostęp do pomieszczeń w czasie nieobecności zatrudnionych tam pracowników nadzorowany przez służbę ochrony. |
|  |  |  | Pomieszczenia są zabezpieczone przed skutkami pożaru za pomocą systemu przeciwpożarowego i / lub wolnostojącej gaśnicy. |
|  |  |  | Kopie zapasowe przechowywane są w różnych lokalizacjach, na różnych nośnikach. |
| **II. Środki sprzętowe infrastruktury informatycznej i telekomunikacyjnej** |
|  |  |  | Zastosowano urządzenia typu UPS, generator prądu i / lub wydzieloną sieć elektroenergetyczną, chroniące system informatyczny przed skutkami awarii zasilania. |
|  |  |  | Każdy pracownik otrzymuje imienny identyfikator do systemów informatycznych. |
|  |  |  | Dostęp do zasobów Zamawiającego zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła. |
|  |  |  | System informatyczny zapewnia wymuszenie na użytkowniku okresową zmianę hasła. |
|  |  |  | System informatyczny zapewnia zmianę hasła w razie zaistniałej potrzeby. |
|  |  |  | Zastosowano środki uniemożliwiające wykonywanie nieautoryzowanych kopii przy użyciu systemów informatycznych. |
|  |  |  | Zastosowano system rejestracji dostępu do systemu. |
|  |  |  | Zastosowano środki kryptograficznej ochrony danych przekazywanych drogą teletransmisji. |
|  |  |  | Dostęp do środków teletransmisji zabezpieczono za pomocą mechanizmów uwierzytelnienia. |
|  |  |  | Zastosowano środki ochrony przed szkodliwym oprogramowaniem, takim jak np. robaki, wirusy, konie trojańskie, rootkity. (oprogramowanie antywirusowe). |
|  |  |  | Oprogramowanie posiada licencje i jest na bieżąco aktualizowane. |
|  |  |  | Użyto system Firewall do ochrony dostępu do sieci komputerowej. |
|  |  |  | Użyto system IDS/IPS do ochrony dostępu do sieci komputerowej. |
|  |  |  | Zapewniono zdolność do szybkiego przywrócenia dostępności informacji i dostępu do nich w razie incydentu fizycznego i technicznego. |
|  |  |  | Dostęp do danych osobowych Zamawiającego zabezpieczony został przed nieautoryzowanym uruchomieniem za pomocą hasła BIOS. |
| **III. Środki ochrony w ramach narzędzi programowych i baz danych** |
|  |  |  | Wykorzystano środki pozwalające na rejestrację zmian wykonywanych na poszczególnych elementach danych. |
|  |  |  | Zastosowano środki umożliwiające określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanych informacji. |
|  |  |  | Dostęp do zasobów Zamawiającego wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła. |
|  |  |  | Dostęp do zasobów Zamawiającego wymaga uwierzytelnienia przy użyciu karty procesorowej oraz kodu PIN lub tokena. |
|  |  |  | Dostęp do zasobów Zamawiającego wymaga logowania/uwierzytelnienia poprzez uwierzytelnianie wielopoziomowe, np. 2FA (uwierzytelnianie dwuskładnikowe). |
|  |  |  | Dostęp do zasobów Zamawiającego wymaga uwierzytelnienia z wykorzystaniem technologii biometrycznej. |
|  |  |  | Zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych dla poszczególnych użytkowników systemu informatycznego. |
|  |  |  | Zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do zasobów Zamawiającego. |
|  |  |  | Zastosowano kryptograficzne środki ochrony danych. |
|  |  |  | Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe Zamawiającego. |
|  |  |  | Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania informacji Zamawiającego ( w tym danych osobowych) w przypadku dłuższej nieaktywności pracy użytkownika. |
| **IV. Środki organizacyjne** |
|  |  |  | Osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych. |
|  |  |  | Przeszkolono osoby zatrudnione przy przetwarzaniu danych osobowych w zakresie zabezpieczeń systemu informatycznego. |
|  |  |  | Cyklicznie doskonalona jest wiedza osób zatrudnionych przy przetwarzaniu informacji poprzez cykliczne szkolenia oraz inne działania podnoszące świadomość w przedmiotowym obszarze. |
|  |  |  | Wprowadzono/określono zasady ochrony danych osobowych przetwarzanych w systemach teleinformatycznych. |
|  |  |  | Osoby zatrudnione przy przetwarzaniu danych osobowych zobowiązane zostały do zachowania ich w tajemnicy. |
|  |  |  | Dostęp do pomieszczeń po godzinach pracy nie jest możliwy dla osób trzecich (np. firmy sprzątającej) bądź dostęp ten jest szczegółowo nadzorowany. |
|  |  |  | Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane. |
|  |  |  | Osoby zatrudnione przy przetwarzaniu danych osobowych zobowiązane zostały do zabezpieczania nieużywanych w danym momencie systemów poprzez blokadę ekranu lub w inny równoważny sposób – zgodnie z polityką czystego ekranu. |
|  |  |  | Określono zakres oraz częstotliwość tworzenia kopii zapasowych. |
|  |  |  | Określono procedury odtwarzania systemu po awarii oraz ich testowania. |
|  |  |  | Przeprowadzono szacowanie ryzyka dla aktywów w których będą przetwarzane będą dane osobowe Zamawiającego. |
|  |  |  | Wdrożenie wymogów dotyczących bezpieczeństwa informacji potwierdzone jest stosownymi certyfikatami. |
|  |  |  | Wdrażanie nowych rozwiązań odbywa się zgodnie z zasadą „privacy by design”. |
|  |  |  | Wdrażanie nowych rozwiązań odbywa się zgodnie z zasadą z zasadą „privacy by default”.” |
|  |  |  | Prowadzona jest ocena skutków dla ochrony danych. |
|  |  |  | Gwarantowana jest realizacja praw osób, których dane dotyczą. |
|  |  |  | Gwarantowane jest przestrzeganie procedury informowania Administratora o naruszeniu ochrony danych osobowych. |
|  |  |  | Prowadzony jest monitoring funkcjonującego systemu ochrony danych osobowych. |
|  |  |  | Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych. |
|  |  |  | Do przetwarzania danych osobowych dopuszczone są jedynie osoby posiadające upoważnienie do przetwarzania danych osobowych. |
|  |  |  | Wdrożona i stosowana jest polityka określającą zasady ochrony danych osobowych. |

Ponadto zastosowano dodatkowo inne poniżej wyszczególnione środki: …………………………………………………………………………………………………………..

……………………………………………………………………………………………………………

☐ wykazanie przestrzegania zasad dotyczących przetwarzania danych osobowych, jest możliwe m.in. poprzez przedstawienie obowiązujących procedur i dokumentacji ochrony danych osobowych.