|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Miejscowość: |  | Data: |  | Nr wniosku: |  |

**Wniosek o nadanie/modyfikację uprawień do NSW / SWIBŻ\* dla podmiotu zewnętrznego**

\* zaznaczyć właściwy system

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Część A – wypełnia wnioskodawca** | | | | | |
| **Dane wnioskodawcy** | | | | | |
| Nazwa podmiotu: | |  | | | |
| Adres podmiotu: | |  | | | |
| Adres email (operacyjny) | |  | | | |
| Telefon (operacyjny) | |  | REGON / NIP |  | |
| **Dane kierownika podmiotu zewnętrznego** | | | | | |
| Imię: | |  | Nazwisko: |  | |
| Telefon kontaktowy: | |  | Służbowy e-mail: |  | |
| Nadanie uprawnień: | |  | Modyfikacja uprawnień: | |  |
| **Uprawnienia do systemu** | | | | | |
| **Niniejszym wnioskuję o nadanie/modyfikację uprawnień dla niżej wymienionych użytkowników i poniższym podpisem zobowiązuję się, że zostaną oni zobowiązani do stosowania następujących zasad korzystania z systemu:**   1. Użytkownik ma prawo do wykonywania w systemie tylko tych czynności, które wynikają z wnioskowanego zakresu. Wszelkie przekroczenia lub próby przekroczenia przyznanych uprawnień traktowane będą jako incydent bezpieczeństwa i spotkają się z reakcją przewidzianą przez Politykę Bezpieczeństwa Informacji Urzędu Morskiego w Gdyni. 2. Użytkownik ma obowiązek niezwłocznie odnotowywać i zgłaszać wszelkie zaobserwowane lub podejrzewane słabości związane z bezpieczeństwem informacji w systemie. 3. Poświadczenia logowania do systemu muszą być każdorazowo wpisywane (na etapie logowania) przez ich właściciela. W szczególności zabrania się zapisywanie poświadczeń do logowania w pamięci przeglądarki internetowej. 4. Zabrania się ujawniania danych dostępowych (identyfikatora i hasła) do systemu informatycznego. 5. Użytkownik ponosi odpowiedzialność za wszelkie operacje wykonywane przy użyciu jego identyfikatora i hasła. 6. Użytkownik jest odpowiedzialny za zachowanie poufności swoich haseł. 7. Użytkownik systemu informatycznego musi realizować następującą politykę haseł:    1. Hasło musi składać się z co najmniej 8 znaków,    2. Hasło musi stanowić kombinację, co najmniej liter i liczb,    3. Hasło nie może być łatwe do odgadnięcia,    4. Hasło musi być zmieniane, co najmniej co 30 dni,    5. Po zresetowaniu hasła przez pracownika Wydziału Informatyki i Łączności użytkownik musi niezwłocznie zmienić hasło na nowe,    6. W swojej strukturze hasło nie może posiadać nazwy identyfikatora,    7. Zabrania się zapisywania haseł w łatwo dostępnych miejscach w szczególności w obrębie miejsca pracy. 8. W przypadku podejrzenia utraty poufności danych do logowania użytkownik musi je zmienić (lub zgłosić potrzebę zmiany do administratora systemu – pracownika Wydziału Informatyki i Łączności) i powiadomić o tym fakcie Wydział Informatyki i Łączności. 9. Podczas pracy w systemie, użytkownik zobowiązany jest chronić wyświetlane na monitorze informacje przed wglądem osób nieupoważnionych. 10. Każdorazowa przerwa w pracy w systemie informatycznym połączona z opuszczeniem stanowiska pracy lub zakończenie pracy rodzi obowiązek wylogowania się z systemu. 11. Urządzenie, z którego realizowana jest praca w systemie informatycznym musi być wyposażone w:     1. oprogramowanie antywirusowe z aktualną definicją wirusów,     2. zaktualizowany system operacyjny, który jest objęty wsparciem jego producenta. 12. Zabrania się pracy w systemie z wykorzystaniem nieznanych sieci bezprzewodowych w szczególności z sieciami publicznymi o niezweryfikowanych nazwach (SSID) oraz z wykorzystaniem protokołu innego niż WPA2 z szyfrowaniem AES. | | | | | |
| **Dane użytkowników** | | | | | |
| Nazwisko | Imię | | Nr telefonu | Adres e-mail (unikalny) | |
|  |  | |  |  | |
|  |  | |  |  | |
|  |  | |  |  | |
|  |  | |  |  | |
|  |  | |  |  | |
|  |  | |  |  | |
|  |  | |  |  | |
|  |  | |  |  | |
| Ograniczenie uprawnień do portów\*  \*tylko instytucjonalni odbiorcy danych NSW | | |  | | |
| Data i podpis kierownika podmiotu zewnętrznego | | |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Część B – wypełnia Urząd Morski w Gdyni** | | | |
| Opinia Inspektora Danych Osobowych (IOD):[[1]](#footnote-1) | | Pozytywna / Negatywna[[2]](#footnote-2) | |
| Uwagi |  | Data i podpis IOD |  |
| Opinia Administratora Systemu (AS): | | Pozytywna / Negatywna[[3]](#footnote-3) | | |
| Uwagi |  | Data i podpis AS |  | |
|  | | | |
| ZEZWALAM \ NIE ZEZWALAM[[4]](#footnote-4) NA REALIZACJĘ WNIOSKU | | | |
| Data i podpis Dyrektora Urzędu Morskiego w Gdyni lub Koordynatora SafeSeaNet | | |  |

1. Jeśli system przetwarza dane osobowe [↑](#footnote-ref-1)
2. Niepotrzebne skreślić [↑](#footnote-ref-2)
3. Niepotrzebne skreślić [↑](#footnote-ref-3)
4. Niepotrzebne skreślić [↑](#footnote-ref-4)