Procedura wewnętrzna Stowarzyszenia Lokalna Grupa Rybacka Bielska Kraina w zakresie polityki bezpieczeństwa oraz przetwarzania danych w CST2021 oraz portalu Fundusze Europejskie, w zakresie naborów ogłaszanych przez RLGD

§ 1
Przedmiot i zakres Procedury

1. Niniejsza Procedura wewnętrzna reguluje zasady bezpieczeństwa związane z korzystaniem z portalu CST 2021 oraz Portalu Fundusze Europejskie w związku z naborami ogłaszanymi przez stowarzyszenie Lokalna Grupa Rybacka Belska Kraina w ramach wdrażania strategii rozwoju lokalnego kierowanego przez społeczność, o której mowa w przepisach ustawy z dnia 26 maja 2023 r. *o wspieraniu zrównoważonego rozwoju sektora rybackiego z udziałem Europejskiego Funduszu Morskiego, Rybackiego i* Akwakultury.
2. Niniejsza Procedura powstała w związku z wymaganiami wynikającymi z § 6 ust. 1 pkt 2 lit. b tiret piąte umowy nr 5/2025 z dnia 05.03.2025 r. *o warunkach i sposobie realizacji strategii rozwoju lokalnego kierowanego przez społeczność, w ramach programu Fundusze Europejskie dla Rybactwa na lata 2021-2027 ze środków Europejskiego Funduszu Morskiego, Rybackiego i Akwakultury*, zawartej przez stowarzyszenie Lokalna Grupa Rybacka Bielska Kraina z Ministrem Rolnictwa i Rozwoju Wsi.
3. Postanowienia niniejszej Procedury pozostają bez uszczerbku dla obowiązujących w stowarzyszeniu Lokalna Grupa Rybacka Bielska Kraina zasad regulujących bezpieczeństwo informacji oraz przetwarzania danych osobowych, w szczególności określonych w Polityce przetwarzania danych osobowych przez Stowarzyszenie Lokalna Grupa Rybacka Bielska Kraina. W szczególności, ilekroć w tych dokumentach przewidziane są wyższe wymagania dotyczące zachowania poufności, integralności i bezpieczeństwa informacji od środków wynikających z niniejszej Procedury, należy stosować wymagania z tamtych dokumentów.

§ 2
Słownik

Użyte w niniejszej Procedurze określenia oznaczają:

1) **CST2021** – system teleinformatyczny, o którym mowa w art. 2 pkt 5 ustawy EFMRiA;
2) **Incydent** – pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji lub zmniejszeniem poziomu usług systemowych, które stwarzają znaczne prawdopodobieństwo zakłócenia działania Systemu i zagrażają bezpieczeństwu informacji, w tym danych osobowych przetwarzanych w Systemie;

3) **LSR** – strategia rozwoju lokalnego kierowanego przez społeczność, o której mowa w art. 1 pkt 3 ustawy o EFMRiA, opracowana przez RLGD i realizowana na podstawie umowy ramowej zawartej przez RLGD z Instytucją Zarządzającą;

4) **Podatność** – luka (słabość) aktywu lub grupy aktywów, która może być wykorzystana przez co najmniej jedno zagrożenie, rozumiane jako potencjalna przyczyna Incydentu, który może wywołać szkodę w Systemie;

5) **Portal Fundusze Europejskie** – strona internetowa, określona w art. 1 ust. 1 pkt 19 ustawy z dnia 28 kwietnia 2022 r. o *zasadach realizacji zadań finansowanych ze środków europejskich w perspektywie finansowej 2021-2027*, dostępna pod adresem: https://www.funduszeeuropejskie.gov.pl;

6) **Procedura** – niniejszy dokument;

7) **RLGD** – stowarzyszenie Lokalna Grupa Rybacka Bielska Kraina;

8) **System** – zarówno CST, jak i Portal;

9) **Użytkownik** - osoba mająca dostęp do Systemu, wyznaczona przez Zarząd RLGD, której uprawnienia w Systemie nadała właściwa instytucja administrująca Systemem; Użytkownik jest uprawniony do wykonywania w Systemie, w imieniu RLGD, czynności związanych z realizacją LSR, takich jak odbieranie i nadawanie pism, opracowywanie dokumentów, kontakt z wnioskodawcami;

10) **ustawa o EFMRiA** – ustawa z dnia 26 maja 2023 r. *o wspieraniu zrównoważonego rozwoju sektora rybackiego z udziałem Europejskiego Funduszu Morskiego, Rybackiego i* Akwakultury;

11) **Zdarzenie związane z bezpieczeństwem informacji** – stan Systemu, usługi lub sieci, wskazujący na możliwe naruszenie zasad korzystania z niego, błąd zabezpieczenia lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem.

§ 3
Ogólne zasady związane z korzystaniem z Systemu

1. Pracownicy RLGD i członkowie organów RLGD, upoważnieni do korzystania z Systemu w związku z przeprowadzeniem naborów zgodnie z przepisami ustawy o EFMRiA, posługują się indywidualnymi loginami i hasłami przyznanymi im przez administratorów tych Systemów.
2. Na każdorazowe polecenie wygenerowane przez System lub na żądanie administratorów tego Systemu, Użytkownicy dokonują zmiany hasła, spełniającego wymagania określone w Systemie oraz zgodnego z zasadami określonymi w Procedurze.
3. Użytkownik jest zobowiązany do zapoznania się i zaakceptowania regulaminu Systemu, co potwierdza w sposób określony w tym Systemie.
4. Złożenie oświadczenia, o którym mowa w ust. 3, jest warunkiem uzyskania dostępu do Systemu.

5. Użytkownik ponosi odpowiedzialność za skutki swoich działań lub zaniechań w Systemie. Nie zwalnia to z odpowiedzialności wobec osób trzecich RLGD za ewentualne skutki działań lub zaniechań Użytkownika.
6. Użytkownik wykonuje tylko takie działania w Systemie, które są zgodne z innymi dokumentami wewnętrznymi RLGD, w szczególności z Procedurą wyboru i oceny operacji w ramach LSR przez Stowarzyszenie Lokalna Grupa Rybacka Bielska Kraina.
7. Jeżeli wysłanie pisma w Systemie zgodnie z tymi dokumentami stanowi wynik uchwały podjętej przez organ RLGD albo rezultat innego rodzaju zdarzenia, niedopuszczalne jest zrealizowanie takiego działania bez lub wbrew treści takiej uchwały lub pomimo niewystąpienia takiego zdarzenia.
8. Użytkownik jest zobowiązany do przestrzegania regulaminu Platformy lub CST.

§ 4.
Hasła i zabezpieczenia Systemu

1. Korzystanie z Sytemu możliwe jest po zalogowaniu się do niego i wpisaniu hasła. Hasło do Systemu powinno się składać się z minimum 10 znaków i powinno zawierać wielkie i małe litery oraz cyfry i znaki specjalne. Jeżeli System ustanawia dalej idące wymagania dotyczące hasła, stosuje się te wymagania.
2. Hasło, o którym mowa w ust. 1, nie może zawierać w sobie loginu użytkownika ani nie może być identyczne z hasłem do komputera służbowego.
3. Nowe hasło musi różnić się od wszystkich haseł archiwalnych. Zaleca się, by nowe hasła nie były wariacjami poprzednich haseł (np. poprzez dodanie do starego hasła kolejnej cyfry).
4. Hasła nie mogą być ujawniane przez Użytkowników innym osobom, w tym innym Użytkownikom, nawet jeżeli są pracownikami RLGD lub zwierzchnikami Użytkownika. Zabronione jest zapisywanie haseł na tablicach, zapisywanie ich na karteczkach przylepianych do monitora i innego rodzaju zachowania, które mogłoby ujawnić hasło do Systemu.
5. Zabronione jest korzystanie z Systemu z użyciem danych dostępowych innego Użytkownika.
6. W przypadku nieumyślnego ujawnienia hasła do Systemu osobie nieuprawnionej lub podejrzenia ujawnienia, należy bezzwłocznie dokonać zmiany hasła na nowe.
7. W przypadku braku możliwości dokonania przez Użytkownika zmiany hasła do Systemu (braku działania odpowiedniej funkcjonalności w CST lub Platformie) należy niezwłocznie skontaktować się z administratorem Systemu.
8. Użytkownik jest zobowiązany do ustawienia ekranu monitora w taki sposób, aby uniemożliwić osobom postronnym wgląd lub spisanie informacji aktualnie wyświetlanej na ekranie monitora, w czasie, gdy Użytkownik korzysta z Systemu.
9. Komputer Użytkownika powinien zostać ustawiony w taki sposób, aby osoby postronne miały utrudniony dostęp do portów zewnętrznych lub przynajmniej dostęp do portów zewnętrznych był pod kontrolą wizualną Użytkownika.

10. Użytkownik jest zobowiązany do przestrzegania zasady czystego biurka. W szczególności przed opuszczeniem stanowiska pracy Użytkownik powinien schować wszelkie dokumenty związane z używanym Systemem oraz informatyczne nośniki danych (dyskietki, płyty CD, DVD, BD, pendrive itp.).
11. Komputer Użytkownika powinien blokować się w przypadku braku aktywności Użytkownika dłuższej niż 5 minut (tj. zablokowanie pulpitu lub włączenie wygaszacza ekranu). Odblokowanie komputera powinno wymagać wpisania hasła.
12. Komputer Użytkownika nie powinien zachowywać zapisanego hasła do Systemu – hasło powinno być każdorazowo wpisywane w całości przez Użytkownika.
13. Komputer Użytkownika powinien posiadać oprogramowanie antywirusowe, którego sygnatury wirusów powinny być aktualizowane nie rzadziej niż raz na tydzień, a także oprogramowanie typu firewall.
14. Sieć RLGD powinna być zabezpieczona oprogramowaniem uniemożliwiającym jej penetrację przez zewnętrznych, nieautoryzowanych użytkowników.
15. Oprogramowanie, o którym mowa w ust. 13, powinno być stale aktywne na komputerach Użytkowników.
16. Użytkownik powinien monitorować komunikaty pochodzących z oprogramowania, o którym mowa w ust. 13, zainstalowanego na stacji roboczej i reagowania na nie.
17. Podczas pracy z Systemem na komputerze Użytkownika nie powinien być uruchomiony żaden serwer, w szczególności nie powinien być uruchomiony serwer WWW oraz FTP (TFTP).
18. Sprzęt i oprogramowanie, z którego korzysta Użytkownik, powinny być regularnie aktualizowane zgodnie z wytycznymi producentów.
19. Przeglądarkę internetową, z której korzysta Użytkownik, należy skonfigurować w ten sposób, aby miała włączoną obsługę protokołu OCSP (Online Certificate Status Protocol), umożliwiającego przeprowadzenie weryfikacji ważności certyfikatu Systemu.
20. Użytkownik nie może korzystać z niezabezpieczonych sieci WIFI.
21. Korzystanie z Systemu w ramach publicznych sieci (np. w bibliotece, kawiarni, hotelu) jest zabronione.

§ 5
Akty staranności podczas codziennej pracy w Systemie

1. Użytkownik podczas logowania się do Systemu jest zobowiązany sprawdzić czy:
   1) w pasku adresowym przeglądarki adres zaczyna się od https;
   2) w obrębie okna przeglądarki znajduje się mała kłódka informująca o bezpieczeństwie;
   3) po kliknięciu na kłódkę pojawia się informacja o tym, że dla danego Systemu został wydany certyfikat i jest on ważny.
2. Połączenie do Systemu powinno być jest szyfrowane.

3. W celu chwilowego zawieszenia pracy w Systemie, należy zablokować ekran, tj. zablokować pulpit lub włączyć wygaszacz ekranu zabezpieczony hasłem. Jeśli komputer Użytkownika nie pozwala na zabezpieczenie ekranu hasłem, należy wylogować się z Systemu.
4. Po zakończeniu pracy należy wylogować się z Systemu poprzez wybranie funkcji "Wyloguj". Nie należy kończyć pracy poprzez samo tylko zamknięcie okna przeglądarki znakiem „X”.

§ 6
Naruszenia zasad bezpieczeństwa

1. W przypadku:
   1) zauważenia Podatności przez Użytkownika lub któregokolwiek innego pracownika lub członka Stowarzyszenia,
   2) wystąpienia Zdarzenia związanego z bezpieczeństwem informacji,
   3) pojawienia się Incydentu,
   4) zauważenia, że stan sprzętu komputerowego, zawartość zbioru danych osobowych w Systemie, ujawnione metody pracy, sposób działania Systemy lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenie bezpieczeństwa danych przetwarzanych w Systemie

   – osoba, która stwierdzi jedną z powyższych sytuacji (w tym Użytkownik), jest zobowiązana do niezwłocznego powiadomienia Zarządu RLGD oraz administratora Systemu. Jeżeli okoliczności wskazują na prawdopodobieństwo naruszenia zasad ochrony danych osobowych stosuje się ponadto procedurę opisaną w Polityce przetwarzania danych osobowych przez Stowarzyszenie Lokalna Grupa Rybacka Bielska Kraina.
2. Wszelkie czynności podejmowane w związku z jednym ze zdarzeń, o których mowa w ust. 1, powinny być dokumentowane, tak by można było odtworzyć działania podejmowane przez Stowarzyszenie, zgodnie z zasadą rozliczalności.