Regulamin Systemu Operatora

Rozdział I

Słownik pojęć

Ilekroć w niniejszym Regulaminie jest mowa o:

1. Administratorze – należy przez to rozumieć Użytkownika o specjalnych uprawnieniach, które pozwalają mu na zarządzanie kontami Użytkowników. Funkcję Administratora pełnią wyznaczeni pracownicy Lidera Projektu tj. Agencja Rozwoju Regionalnego ARLEG S.A. (zwana dalej ARR ARLEG S.A.); ul. Macieja Rataja 26, 59-220 Legnica,
2. Administratorze danych osobowych – należy przez to rozumieć osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych zgodnie z art. 4 pkt 7) RODO;
3. IP – należy przez to rozumieć Instytucję Pośredniczącą , o której mowa w art. 2 pkt 10 Ustawy;
4. IZ – należy przez to rozumieć Instytucję Zarządzającą, o której mowa w art. 2 pkt 12 Ustawy;
5. Koncie – należy przez to rozumieć zespół cech identyfikujących Użytkownika, z których wynika możliwość dostępu do usług po podaniu identyfikatora użytkownika oraz hasła;
6. Partnerzy Projektu – podmioty współrealizujące projekt wraz z Liderem Projektem, tj.
   - Dolnośląską Agencją Współpracy Gospodarczej Sp. z o.o., Al. Kasztanowa 3A-5, 53-125 Wrocław,
   - Karkonoska Agencja Rozwoju Regionalnego S.A., ul. 1 Maja 27, 58-500, Jeleniej Góra,
   - Dolnośląską Agencją Rozwoju Regionalnego Spółka Akcyjna., ul. Szczawieńska 2, 58-310 Szczawno-Zdrój;
   - Wrocławska Agencja Rozwoju Regionalnego S.A., ul. Karmelkowa 29, 52-437 Wrocław,
   - Dolnośląski Park Innowacji i Nauki S.A., ul. Eugeniusza Kwiatkowskiego 4, 52-407 Wrocław.
7. Regulaminie – należy przez to rozumieć niniejszy dokument określający w szczególności warunki korzystania z Systemu, prawa i obowiązki korzystających z niego Użytkowników, warunki i zasady ochrony danych osobowych, jak również zakres odpowiedzialności Użytkowników;

8. RODO – należy przez to rozumieć Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych);
9. Roli – należy przez to rozumieć zespół praw i obowiązków wynikających ze statusu Użytkownika w Systemu;
10. Rozporządzenie ogólne - rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/1060 z dnia 24 czerwca 2021 r. ustanawiające wspólne przepisy dotyczące Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego Plus, Funduszu Spójności, Funduszu na rzecz Sprawiedliwej Transformacji i Europejskiego Funduszu Morskiego, Rybackiego i Akwakultury, a także przepisy finansowe na potrzeby tych funduszy oraz na potrzeby Funduszu Azylu, Migracji i Integracji, Funduszu Bezpieczeństwa Wewnętrznego i Instrumentu Wsparcia Finansowego na rzecz Zarządzania Granicami i Polityki Wizowej (Dz. Urz. UE L 231 z dn. 30 czerwca 2021 r.);
11. Ustawa – ustawa z dnia 28 kwietnia 2022 r. o zasadach realizacji zadań finansowanych ze środków europejskich w perspektywie finansowej 2021–2027 (Dz. U. z 2022 r. poz. 1079);
12. Użytkowniku – należy przez to rozumieć osobę, która posiada dostęp do Systemu Operatora, wyznaczona przez Przedsiębiorcę do wykonywania w jej imieniu czynności związanych z realizacją projektu lub do wykonywania w jego imieniu czynności związanych z realizacją projektu.

Rozdział II

Postanowienia ogólne

1. Niniejszy Regulamin określa warunki i zasady korzystania z Systemu Operatora, a w szczególności uprawnienia i obowiązki Użytkowników.
2. Użytkownik jest zobowiązany do przestrzegania Regulaminu.
3. Dostęp do Systemu Operatora jest bezpłatny.
4. Właścicielem Systemu Operatora jest ARR ARLEG S.A.
5. ARR ARLEG S.A zastrzega sobie prawo dowolnej modyfikacji usług, sposobu działania Systemu Operatora oraz podjęcia wszelkich dozwolonych przez prawo czynności związanych z obsługą i konserwacją Systemu Operatora.
6. ARR ARLEG S.A zastrzega sobie prawo do zablokowania Konta w przypadku stwierdzenia naruszania niniejszego Regulaminu.
7. Użytkownik, który wprowadza dane do Systemu Operatora, jest zobowiązany do zapewnienia ich jakości, w szczególności prawdziwości oraz zgodności ze strukturą danych oczekiwaną przez System Operatora.

Rozdział III

Cele Systemu Operatora

System Operatora jest aplikacją umożliwiającą złożenie dokumentów, w tym między innymi formularza zgłoszeniowego, umowy, wniosku o rozliczenie do projektu „Dotacje na usługi rozwojowe dla dolnośląskich firm" dofinansowanego ze środków Europejskiego Funduszu Społeczny PLUS w ramach programu Fundusze Europejskie dla Dolnego Śląska 2021-2027, Priorytet 7 Fundusze Europejskie na rzecz rynku pracy i włączenia społecznego na Dolnym Śląsku, Działanie 7.4 Adaptacja do zmian na rynku pracy, Typ 7.4.A Projekty w zakresie Podmiotowego Systemu Finansowania.

Rozdział IV

Warunki korzystania z Systemu Operatora

1. Do korzystania z Systemu Operatora wymagane jest posiadanie przez Użytkownika:
    a. dostępu do Internetu;
    b. dostępu do indywidualnego konta poczty elektronicznej e-mail;
    c. dostępu do przeglądarki internetowej spośród wymienionych Edge, Mozilla Firefox, Google Chrome, Opera w ich najwyższej, stabilnej wersji.
2. Podczas korzystania z Systemu Operatora niezbędnym wymogiem jest, by przeglądarka internetowa Użytkownika akceptowała pliki typu cookie.
3. System Operatora jest dostępny dla Użytkowników pod adresem www.74a.uslugi-rozwojowe.pl przez 24 godziny na dobę, 7 dni w tygodniu, z zastrzeżeniem ust.4.
4. ARR ARLEG S.A. zastrzega sobie możliwość wprowadzenia przerw w funkcjonowaniu Systemu Operatora niezbędnych do wykonania czynności związanych z prawidłowym jego funkcjonowaniem, w tym z przerwą konserwacyjną, z realizacją prac dotyczących administrowania lub modyfikacji funkcjonalności Systemu Operatora ze względów bezpieczeństwa lub innych przyczyn niezależnych od ARR ARLEG S.A. O planowanych przerwach związanych z prowadzeniem prac konserwacyjnych w Systemie Operatora ARR ARLEG S.A. informuje za pośrednictwem funkcjonalności systemu i na stronie www.arleg.eu.
5. ARR ARLEG S.A. nie ponosi kosztów związanych z uzyskaniem przez Użytkownika niezbędnego dostępu do Systemu Operatora dzięki korzystaniu z Internetu lub innych środków komunikowania się na odległość, a także właściwego oprogramowania do korzystania z dostępu do Systemu Operatora lub umożliwiającego odczytanie lub zapisanie danych. Zasady i koszty takiego

dostępu reguluje umowa zawarta przez Użytkownika z podmiotem udostępniającym takie usługi lub oprogramowanie.

6. ARR ARLEG S.A. nie ponosi odpowiedzialności za zakłócenia w funkcjonowaniu Systemu Operatora wywołane siłą wyższą, awarią sprzętu lub niedozwoloną ingerencją Użytkowników, nawet jeśli spowodowałyby one utratę danych na Kontach Użytkowników.
7. ARR ARLEG S.A. nie ponosi odpowiedzialności za czasową niemożność korzystania przez Użytkowników z Systemu Operatora z przyczyn niezależnych od ARR ARLEG S.A.
8. ARR ARLEG S.A. gromadzi informacje o adresie IP, z którego Użytkownik uwierzytelnia się w Systemu Operatora. ARR ARLEG S.A. gromadzi adresy IP wyłącznie w celu wykrywania prób naruszenia zabezpieczeń Systemu Operatora oraz prowadzenia audytu jego zabezpieczeń.
9. ARR ARLEG S.A nie odpowiada za szkody powstałe w związku z korzystaniem z Systemu Operatora, bądź w związku z niewłaściwym działaniem Systemu Operatora spowodowanym błędami, brakami, zakłóceniami, defektami, opóźnieniami w transmisji danych, wirusami komputerowymi, awariami łącza sieci Internet lub nieprzestrzeganiem postanowień Regulaminu.
10. ARR ARLEG S.A zastrzega sobie prawo do zawieszenia konta Użytkownika, który narusza prawo lub postanowienia Regulaminu.
11. ARR ARLEG S.A może trwale zablokować konto Użytkownika jeśli Użytkownik nie zaprzestanie działań sprzecznych z prawem lub postanowieniami Regulaminu. ARR ARLEG S.A poinformuje właściwy podmiot o zawieszeniu bądź zablokowaniu konta Użytkownika reprezentującego ten podmiot.

Rozdział V
Użytkownicy Systemu Monitorowania FST

1. Użytkownikiem może być każda osoba, która zarejestruje Konto w Systemu Operatora jednak poziom uprawnień uzależniony jest od pełnionej w systemie Roli.
2. Rejestrując Konto Użytkownik potwierdza spełnianie warunków korzystania z Systemu Operatora oraz wyraża zgodę na wszystkie postanowienia niniejszego Regulaminu i zobowiązuje się do ich przestrzegania, co potwierdza (przez złożenie oświadczenia na formularzu) podczas pierwszego logowania oraz po zmianie Regulaminu. Złożenie ww. oświadczenia, jest warunkiem uzyskania dostępu do Systemu Operatora.
3. Korzystanie z funkcjonalności Systemu Operatora jest możliwe pod warunkiem nadania Użytkownikowi Roli przez osobę uprawnioną do zarządzania Użytkownikami w podmiocie, w imieniu którego Użytkownik ma działać w Systemu Operatora.
4. Rejestrując Konto Użytkownik, wyraża zgodę na otrzymywanie na powiązany z kontem adres email komunikatów systemowych.

5. Zabrania się Użytkownikowi nieautoryzowanego monitorowania Systemu Operatora w tym jego zabezpieczeń oraz podejmowania wszelkich prób mających na celu naruszenie bezpieczeństwa danych przetwarzanych w Systemie Operatora, w tym prób przełamania zabezpieczeń Systemu Operatora.

Rozdział VI

Konto Użytkownika Systemu Operatora

1. Rozpoczęcie korzystania z Systemu Operatora wymaga rejestracji konta oraz w przypadku Przedsiębiorców kliknięcia linku aktywacyjnego wysłanego na adres e-mail podany podczas rejestracji Użytkownika.
2. Zrealizowanie w pełni procedury aktywacji Konta w Systemie Operatora możliwe jest wobec Użytkownika, który:
   a) zapoznał się i zaakceptował treść całego Regulaminu;
   b) oświadczył, że zapoznał się ze Szkoleniem z Bezpieczeństwa informacji przetwarzanych w Systemu Operatora (w załączeniu).
   c) podał wszystkie wymagane dane.
3. W przypadku stwierdzenia podania przez Użytkownika nieprawdziwych lub nieaktualnych danych, Administrator Systemu Operatora ma obowiązek:
   a) wezwać Użytkownika do natychmiastowego usunięcia nieprawidłowości, lub
   b) zablokować Konto Użytkownika do czasu wyjaśnienia sprawy.
4. W przypadku pojawienia się uzasadnionych wątpliwości, co do autentyczności wprowadzonych przez Użytkownika danych, Administrator Systemu Operatora może zażądać przedstawienia stosownych dokumentów potwierdzających te dane.
5. Dla każdego Użytkownika jest ustalany odrębny identyfikator użytkownika i hasło dostępu do Systemu Operatora.
6. Przydziału i zmiany haseł dokonuje się w następujący sposób:
   a. hasła powinny mieć co najmniej osiem znaków i muszą zawierać małe i wielkie litery, cyfry oraz znaki specjalne,
   b. nowe hasło nie powinno być identyczne z żadnym z 8 poprzednich,
7. Hasło powinno być zmieniane przez każdego z Użytkowników nie rzadziej niż raz na 90 dni,
   a. hasła nie powinny składać się z kombinacji znaków mogących ułatwić ich odgadnięcie lub odszyfrowanie przez osoby nieuprawnione (np.: imię, nazwisko Użytkownika);
   b. hasło powinno zostać zmienione przez Użytkownika niezwłocznie w przypadku powzięcia podejrzenia lub stwierdzenia, że mogły się z nim zapoznać osoby trzecie.

8. Użytkownik jest odpowiedzialny za wszystkie czynności wykonane przy użyciu identyfikatora, którym się posługuje.
9. Zabrania się udostępniania danych identyfikacyjnych swojego Konta innym osobom, a w szczególności hasła dostępu.
10. Zabrania się korzystania z Kont należących do innych osób.
11. Przy opuszczeniu miejsca pracy dostęp do Systemu Operatora powinien być blokowany przez wybranie co najmniej jednej z poniższych opcji:
    a. zastosowanie mechanizmu zawieszania pracy systemu operacyjnego;
    b. wylogowania się Użytkownika z Systemu Operatora.

Rozdział VII

Dane osobowe

1. Administratorami danych osobowych (administratorami) w rozumieniu przepisów RODO są podmioty wskazane w art. 87 ust. 1 ustawy z dnia 28 kwietnia 2022 r. o zasadach realizacji zadań finansowanych ze środków europejskich w perspektywie finansowej 2021–2027.
2. Administratorzy przetwarzają dane osobowe w celach określonych w art. 4 ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2021/1057 z dnia 24 czerwca 2021 r. ustanawiające Europejski Fundusz Społeczny Plus (EFS+).
3. Dane osobowe są przechowywane przez okres niezbędny do realizacji ww. celów, tj. do czasu rozliczenia programów na lata 2021-2027 oraz upływu okresów trwałości i zakończenia kontroli trwałości dla wszystkich projektów.
4. Użytkownik ma obowiązek zachować w tajemnicy przetwarzane dane osobowe oraz informacje o sposobach ich zabezpieczenia, zarówno w okresie korzystania z Systemu Operatora jak i po jego zakończeniu.
5. Użytkownik odpowiada za zgodność danych osobowych wprowadzonych przez siebie do Systemu Operatora z dokumentami źródłowymi.
6. Każdy Użytkownik ma prawo do wniesienia skargi do organu nadzorczego, którym jest Prezes Urzędu Ochrony Danych Osobowych.

Rozdział VIII

Polityka prywatności

1. ARR ARLEG S.A przywiązuje szczególną wagę do poszanowania prywatności Użytkowników korzystających z Systemu Operatora. Gromadzone w dziennikach logów dane są wykorzystywane wyłącznie do celów administrowania Systemu. Wszelkie dane Użytkowników uzyskane za

pośrednictwem Systemu Operatora przeznaczone są na użytek ARR ARLEG S.A, Partnerów Projektu lub innych instytucji systemu wdrażania Projektu w ramach Funduszy Europejskich dla Dolnego Śląska na lata 2021-2027.

2. Wszelkie dane pochodzące od Użytkowników uzyskiwane są podczas korzystania z Systemu Operatora – wśród nich mogą być:

a) informacje podawane dobrowolnie przez Użytkownika;

b) informacje uzyskiwane podczas korzystania– wśród nich mogą być:

- informacje w dziennikach serwerów – nasze serwery automatycznie zapisują takie dane, jak adres IP, data, czas, metoda HTTP, adres strony internetowej, aplikacja klienta;

3. Przeglądarka internetowa może przechowywać pliki cookies na dysku komputera. W plikach cookies znajdują się informacje niezbędne do prawidłowego funkcjonowania Systemu Operatora takie jak:
    a. numer sesji i identyfikator użytkownika
    b. zmiana kontrastu dla niepełnosprawnych
    c. zabezpieczenie formularzy csrf.
4. Zawartość plików cookies nie pozwala na identyfikację Użytkownika.
5. Za pomocą plików cookies nie są przetwarzane lub przechowywane dane osobowe Użytkowników Systemu Operatora.
6. Mechanizm cookies nie jest wykorzystywany do pozyskiwania jakichkolwiek informacji o Użytkownikach.
7. ARR ARLEG S.A przechowuje pliki cookies na komputerach Użytkowników w celu:

a) właściwego dopasowania Systemu Operatora do potrzeb Użytkowników;

b) zapamiętania preferencji i indywidualnych ustawień Użytkownika;

c) tworzenia statystyk oglądalności Systemu Operatora.

8. Użytkownik posiada możliwość takiego skonfigurowania przeglądarki internetowej, aby całkowicie lub częściowo wyłączyć przechowywanie plików cookies na dysku twardym komputera. Efektem zmiany może być utrata możliwości korzystania z niektórych funkcjonalności Systemu Operatora.
9. Dane zbierane w ramach Systemu Operatora służą do zapewnienia określonych usług Użytkownikom oraz do celów administracyjnych i statystycznych, a także do ochrony Systemu Operatora.
10. Dane te nie będą sprzedawane ani udostępniane innym instytucjom lub organizacjom ani osobom, które nie są pracownikami, współpracownikami ARR ARLEG S.A, Partnerów Projektu lub świadczą dla ARR ARLEG S.A usługi związane z utrzymaniem, wsparciem technicznym lub rozwojem Systemu Operatora. Jednakże dostęp do danych posiada także firma Google Inc. poprzez wykorzystywanie do celów statystycznych funkcjonalności Google Analytics.

11. ARR ARLEG S.A może sporządzać zbiorcze zestawienia statystyczne, które mogą być ujawniane osobom trzecim. Zestawienia takie nie zawierają jednak żadnych danych pozwalających na identyfikację pojedynczych Użytkowników.
12. ARR ARLEG S.A dokłada wszelkich starań, aby chronić Systemu Operatora przed nieuprawnionym dostępem osób trzecich. W tym celu stosowane są m.in. firewall, urządzenia zabezpieczające serwery, urządzenia szyfrujące oraz fizyczne środki bezpieczeństwa.

Rozdział IX

Korzystanie z Systemu Operatora

1. Każda stacja robocza, na której odbywa się praca w Systemie Operatora powinna posiadać aktualne oprogramowanie antywirusowe oraz zaporę sieciową. Oprogramowanie antywirusowe musi posiadać automatyczną aktualizację z sieci Internet lub z lokalnego repozytorium wykonywaną nie rzadziej niż raz w tygodniu.
2. Niedopuszczalne są działania mogące utrudniać lub zakłócać działanie Systemu Operatora. W przypadku stwierdzenia takich działań, Administrator wzywa Użytkownika do natychmiastowego wyjaśnienia sprawy, bądź blokuje bądź blokuje dostęp poprzez blokadę adresu IP lub dostęp do jego konta do czasu wyjaśnienia sprawy.
3. Zamieszczanie w Systemie Operatora treści bezprawnych, obraźliwych, nieprawdziwych, niezgodnych z prawem powszechnie obowiązującym w Polsce, propagujących przemoc, nagannych moralnie lub naruszających powszechnie uznane dobre obyczaje jest zabronione. Treści takie mogą zostać usunięte przez Administratora.
4. Użytkownicy są zobowiązani do ustawienia ekranów monitorów w taki sposób, aby uniemożliwić osobom postronnym wgląd lub spisanie zawartości aktualnie wyświetlanej na ekranie monitora.

Rozdział X

Odpowiedzialność

1. ARR ARLEG S.A nie ponosi odpowiedzialności za treści umieszczane w Systemu Operatora przez Użytkowników.
2. Zamieszczanie treści bezprawnych, obraźliwych, nieprawdziwych, niezgodnych z prawem powszechnie obowiązującym w Polsce, propagujących przemoc, nagannych moralnie lub naruszających powszechnie uznane dobre obyczaje jest

zabronione. Treści takie mogą zostać usunięte. W szczególności zabronione jest umieszczanie w systemie:
– treści, które zawierają słowa lub zwroty powszechnie uznawane za obraźliwe,
- materiałów o charakterze reklamowym oraz linków do tych materiałów,
- jakichkolwiek treści o charakterze bezprawnym, naruszających w jakikolwiek sposób obowiązujące prawo,
- wzywających do nienawiści rasowej, etnicznej, wyznaniowej, zawierających treści pornograficzne, pochwalających faszyzm, nazizm, komunizm, propagujących przemoc, obrażających uczucia religijne, -naruszających prawa innych osób,
– treści posiadających linki do szkodliwego oprogramowania lub zawierające (np. wirusy, robaki, trojany); – spamu, tj. wielokrotnego powtarzania tej samej lub zbliżonej treści.

3. ARR ARLEG S.A nie ponosi odpowiedzialności za skutki nieprawidłowego korzystania z przez użytkowników.
4. ARR ARLEG S.A nie ponosi odpowiedzialności za treści umieszczane przez użytkowników.
5. Użytkownik ponosi pełną odpowiedzialność za naruszenie prawa bądź szkodę wywołaną jego działaniami w Systemu Operatora, w szczególności podaniem nieprawdziwych danych ujawnieniem informacji niejawnych lub innych tajemnic ustawowo chronionych, naruszeniem dóbr osobistych lub praw autorskich oraz praw pokrewnych, a także przetwarzaniem danych osobowych przekazanych przez użytkowników niezgodnie z celami oraz zakresem danych przekazanych do przetwarzania lub z naruszeniem przepisów dot. ochrony danych osobowych.

Rozdział XI

Zgłoszenia problemów, uwag

Zakłócenia w funkcjonowaniu Systemu Operatora, problemy i uwagi związane ze świadczonymi w jego ramach usługami mogą być zgłaszane przez Użytkownika i są analizowane przez odpowiednie służby informatyczne zgodnie z procedurą wsparcia technicznego.

Rozdział XII

Przepisy końcowe

1. ARR ARLEG S.A zastrzega sobie prawo jednostronnej zmiany Regulaminu bez konieczności uzasadniania przyczyny takiej zmiany.

2. ARR ARLEG S.A zobowiązuje się powiadamiać Użytkowników na stronie www.arleg.eu o zmianach Regulaminu.
3. Użytkownik ponosi odpowiedzialność za podanie adresu poczty elektronicznej, do którego nie ma dostępu, w szczególności adresu nieprawidłowego lub należącego do innego podmiotu oraz wynikające z tego faktu skutki w postaci nieotrzymania powiadomień w systemie.
4. Użytkownik ponosi ryzyko nieotrzymania powiadomienia określonego z przyczyn niezależnych od ARR ARLEG S.A .
5. Regulamin nie wyłącza stosowania innych instrukcji dotyczących funkcjonowania i zabezpieczenia Systemu Operatora.
6. Niniejszy Regulamin wchodzi w życie w dniu 05.06.2024 r.

Załącznik:
Szkolenie z bezpieczeństwa informacji

Szkolenie z bezpieczeństwa informacji

Szkolenie z Bezpieczeństwa Informacji przetwarzanych w Systemie Operatora

Rozdział I

Słownik pojęć

Użyte w niniejszym dokumencie określenia oznaczają:

1. Administrator – wyznaczony pracownik Instytucji realizujący zadania określone w Wytycznych,
2. Dane osobowe – informacje, o których mowa w art. 4 pkt 1 RODO,
3. Incydent – pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji lub zmniejszeniem poziomu usług systemowych, które stwarzają znaczne prawdopodobieństwo zakłócenia działania System Operatora i zagrażają bezpieczeństwu informacji, w tym danych osobowych przetwarzanych w System Operatora,
4. Konto – zespół cech identyfikujących Użytkownika, z których wynika możliwość dostępu do usług po podaniu identyfikatora użytkownika oraz hasła;
5. ARR ARLEG S.A. – Agencja Rozwoju Regionalnego ARLEG S.A, właściciel Systemu Operatora;
6. Podatność – luka (słabość) aktywu lub grupy aktywów, która może być wykorzystana przez co najmniej jedno zagrożenie, rozumiane jako potencjalna przyczyna niepożądanego incydentu, który może wywołać szkodę w Systemie Operatora,
7. Przedsiębiorca – podmiot korzystający z Systemu Operatora w ramach realizacji projektu,
8. RODO – rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. Urz. UE L. 2016.119.1),
9. Rola – zespół praw i obowiązków wynikających ze statusu Użytkownika w Systemie Operatora;
10. Ustawa – ustawa z dnia 28 kwietnia 2022 r. o zasadach realizacji zadań finansowanych ze środków europejskich w perspektywie finansowej 2021–2027 (Dz. U. z 2022 r. poz. 1079),
11. Użytkownik - osoba mająca dostęp do Systemu Operatora, wyznaczona przez Instytucję do wykonywania w jej imieniu czynności związanych z realizacją programu lub przez Przedsiębiorcę do wykonywania w jego imieniu czynności związanych z realizacją projektu,
12. Operator – instytucja, z którą Przedsiębiorca zawarł umowę,

13. Wytyczne – Wytyczne ministra właściwego do spraw rozwoju regionalnego w zakresie warunków gromadzenia i przekazywania danych w postaci elektronicznej na lata 2021-2027.
14. Zdarzenie związane z bezpieczeństwem informacji – stan Systemu Operatora, usługi lub sieci, wskazujący na możliwe naruszenie zasad opisanych w niniejszym dokumencie, błąd zabezpieczenia lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem.

Rozdział II

Bezpieczeństwo informacji – wprowadzenie

1. Bezpieczeństwo systemów informacyjnych to ochrona przed nieuprawnionym dostępem do informacji lub jej modyfikacją.
2. Ochrona powinna obejmować:
    a. przechowywanie, przetwarzanie, transmisję,
    b. zabezpieczenie przed odmową usługi (Denial of Services, DoS oraz Distributed denial of service, DDoS - atak na system komputerowy lub usługę sieciową w celu uniemożliwienia działania),
    c. środki umożliwiające wykrycie, dokumentację oraz przeciwdziałanie zagrożeniom.
3. Na bezpieczeństwo informacji składa się 7 elementów:
    c) poufność – zapewnienie, że informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom, podmiotom lub procesom,
    d) integralność – zapewnienie, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
    e) dostępność – zapewnienie bycia osiągalnym i możliwym do wykorzystania na żądanie, w założonym czasie, przez autoryzowany podmiot,
    f) rozliczalność – zapewnienie, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi,
    g) autentyczność – zapewnienie, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana (autentyczność dotyczy użytkowników, procesów, systemów i informacji),
    h) niezaprzeczalność – braku możliwości wyparcia się swego uczestnictwa w całości lub w części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie,
    i) niezawodność – zapewnienie spójności oraz zamierzonych zachowań i skutków.

Rozdział III

Wymagania sprzętowe pozwalające na korzystanie z Systemu Operatora

1. W celu prawidłowego korzystania z Systemu Operatora niezbędne są:
    a. połączenie z siecią Internet,
    b. indywidualne konto poczty elektronicznej e-mail,
    c. zainstalowana przeglądarka internetowa: Edge, Mozilla Firefox, Google Chrome lub Opera w najnowszej stabilnej wersji,
    d. włączenie obsługi technologii Java Script, tzw. "cookie" oraz wyłączenie blokowania wyskakujących okien w przeglądarce internetowej,
    e. zainstalowanie rozszerzenia Szafir SDK (tylko w przypadku przeglądarki Google Chrome i Firefox do obsługi kwalifikowanego podpisu elektronicznego).

Rozdział IV

Dostęp do SM FST

1. System Operatora jest dostępny pod domeną www.74a.uslugi-rozwojowe.pl przez 24 godziny na dobę, 7 dni w tygodniu z wyjątkiem przerw niezbędnych do wykonania czynności związanych z prawidłowym jego funkcjonowaniem.
2. Użytkownikiem jest każda osoba, która posiada zarejestrowane konto w Systemie Operatora. Poziom uprawnień uzależniony jest od pełnionej w systemie roli.

Rozdział V

Zasady bezpieczeństwa w Systemie Operatora

1. Hasła należy utrzymywać w tajemnicy i nie ujawniać ich innym osobom.
2. Kryteria w zakresie długości, złożoności oraz częstotliwości zmiany haseł:
    a. hasło składa się z minimum 8 znaków,
    b. hasło zawiera ca najmniej: jedną wielką literę, jedną małą literę, jedną cyfrę oraz znak specjalny,
    c. hasło jest zmieniane nie rzadziej niż co 90 dni,
    d. hasło nie powinno zawierać 5 kolejnych znaków z loginu (adresu e-mail),
    e. nowe hasło nie powinno zawierać 5 znaków starego hasła,

3. Przy opuszczaniu miejsca pracy dostęp do komputera osobistego powinien być blokowany przez zastosowanie mechanizmu zawieszania pracy systemu operacyjnego lub wylogowania się użytkownika (zakończenia pracy w System Operatora).
4. Nie należy ujawniać danych służących do logowania innym osobom. W przypadku pozyskania hasła przez osobę nieuprawnioną lub podejrzenia takiego pozyskania, należy bezzwłocznie dokonać zmiany hasła na nowe.
5. W przypadku zapomnienia hasła należy wykorzystać funkcjonalność „Przypomnij hasło".
6. Użytkownik powinien przestrzegać zasady czystego biurka. W szczególności przed opuszczeniem swego stanowiska pracy użytkownik powinien schować wszelkie dokumenty związane z używanym System Operatora oraz informatyczne nośniki danych (dyskietki, płyty CD, DVD, pendrive, itp.).

Rozdział VI

Konfiguracja sprzętu komputerowego użytkownika

1. Komputer użytkownika powinien posiadać oprogramowanie antywirusowe, którego sygnatury wirusów powinny być aktualizowane nie rzadziej niż raz na tydzień. Oprogramowanie antywirusowe powinno być stale aktywne.
2. Użytkownik powinien stale monitorować komunikaty pochodzące z oprogramowania antywirusowego zainstalowanego na stacji roboczej i reagować na nie.
3. Komputer użytkownika powinien być chroniony zaporą sieciową (firewall).
4. Podczas pracy z Systemem Operatora na komputerze użytkownika nie powinien być uruchomiony żaden serwer, w szczególności nie powinien być uruchomiony serwer WWW oraz FTP (TFTP).
5. Oprogramowanie komputera powinno być regularnie aktualizowane, w szczególności dotyczy to systemu operacyjnego oraz przeglądarki internetowej.

Rozdział VII

Rozpoczynanie, zawieszanie i kończenie pracy użytkowników w systemie

1. Użytkownik podczas logowania się do Systemu Operatora powinien sprawdzić:
   a) czy w pasku adresowym przeglądarki adres zaczyna się od https,

b) czy w obrębie okna przeglądarki znajduje się mała kłódka informująca o szyfrowanym połączeniu ze stroną,
c) czy po kliknięciu na kłódkę pojawia się informacja o tym, że certyfikat został wydany i jest on ważny.

2. Rozpoczęcie pracy użytkownika w systemie następuje po uruchomieniu przeglądarki oraz wprowadzeniu adresu www.74a.uslugi-rozwojowe.pl.
3. Po poprawnym zalogowaniu użytkownik otrzymuje w przeglądarce ekran startowy System Operatora zawierający zakładki modułów, do których użytkownik ma nadany dostęp.
4. W celu chwilowego zawieszenia pracy w System Operatora, należy zablokować ekran (zablokować pulpit lub włączyć wygaszacz ekranu zabezpieczony hasłem). Jeśli komputer użytkownika nie pozwala na zabezpieczenie ekranu hasłem, należy wylogować się z Systemu Operatora.
5. Po zakończeniu pracy należy wylogować się z Systemu Operatora poprzez wybranie funkcji „Wyloguj się" zlokalizowanej w rozwijanym menu w prawym górnym rogu ekranu. Nie należy kończyć pracy poprzez zamknięcie okna przeglądarki znakiem „X".

Rozdział VIII

Zgłaszanie zagrożeń bezpieczeństwa w Systemie Operatora

1. W przypadku:
   a) zauważenia podatności,
   b) zdarzenia związanego z bezpieczeństwem informacji,
   c) incydentu,
   d) zauważenia, że stan sprzętu komputerowego, zawartość zbioru danych osobowych w systemie, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenie bezpieczeństwa danych osobowych przetwarzanych w Systemie,

użytkownik reprezentujący Przedsiębiorcę jest zobowiązany do niezwłocznego powiadomienia właściwej Instytucji.

2. W przypadku:

a) zauważenia podatności,
b) zdarzenia związanego z bezpieczeństwem informacji,
c) incydentu,
d) podejrzenia wystąpienia podatności lub incydentu,
e) zauważenia, że stan sprzętu komputerowego, zawartość zbioru danych osobowych w systemie, ujawnione metody pracy, sposób działania programu lub

jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenie bezpieczeństwa danych osobowych przetwarzanych w Systemie,

użytkownik reprezentujący Operatora jest zobowiązany do niezwłocznego powiadomienia Administratora w tej Instytucji.

3. Użytkownik będący Administratorem postępuje zgodnie z wewnętrzną Procedurą obsługi zgłoszeń.

Rozdział IX

Internet - zasady bezpiecznego surfowania po stronach WWW

1. Korzystaj z pakietu typu internet security, który łączy oprogramowanie antywirusowe, zaporę ogniową, technologię pozwalającą na wykrywanie i blokowanie zagrożeń sieciowych oraz mechanizm blokowania ataków poprzez luki w przeglądarce internetowej. Takie oprogramowanie pozwala na zwiększenie poziomu ochrony przed złośliwym kodem i innymi zagrożeniami w odróżnieniu od tradycyjnych programów antywirusowych.
2. Regularnie aktualizuj wszystkie aplikacje zainstalowane na stacji roboczej, w szczególności zwracaj uwagę na programy najbardziej podatne na zagrożenia - np. pakiety biurowe, przeglądarki internetowe, czy kodeki.
3. Uaktualniaj definicje wirusów. Dzięki temu możesz chronić swój komputer przed najnowszymi znanymi wirusami krążącymi w sieci Internet. Najlepszym rozwiązaniem jest posiadanie programu ochronnego (antywirusowego), który automatycznie pobiera najnowsze definicje.
4. Stosuj trudne do odgadnięcia hasła, które są kombinacjami liter - zarówno małych, jak i dużych, cyfr oraz znaków specjalnych. Hasła nie powinny składać się ze słów czy wyrazów, które mogłyby być łatwe do odgadnięcia, na przykład z imienia i daty urodzenia. Regularnie zmieniaj lub modyfikuj hasła.
5. Nie przeglądaj, nie otwieraj ani nie pracuj z żadnym załącznikiem przesłanym drogą e-mail, którego nie oczekiwałeś lub przeznaczenia, którego nie jesteś pewien.
6. Unikaj klikania na linki i załączniki w wiadomościach e-mail lub komunikatorach internetowych. Tego typu odnośniki mogą stanowić zagrożenie.
7. Systematycznie sprawdzaj, czy Twój system operacyjny może być podatny na zagrożenia. Możesz skorzystać z darmowych skanerów systemów dostępnych w sieci Internet.
8. Zastosuj rozwiązania przeciwko zagrożeniom typu phishing (phishing – metoda oszustwa, w której przestępca podszywa się pod inną osobę lub instytucję, w celu wyłudzenia określonych informacji lub nakłonienia ofiary do określonych działań),

np. instalując dodatkowy pasek narzędzi w przeglądarce internetowej, który może ostrzec przed potencjalnie niebezpieczną witryną. Nigdy nie ujawniaj poufnych danych osobistych lub finansowych, dopóki nie będziesz miał pewności, że prośba o podanie tych informacji pochodzi z legalnego, bezpiecznego źródła.

9. Pamiętaj, że złośliwy kod może zostać zainstalowany na twoim komputerze automatycznie podczas przeglądania Internetu, czy pobierania z niego plików.
10. Uważnie czytaj umowy licencyjne (EULA) zanim zaakceptujesz ich warunki. Niektóre zagrożenia bezpieczeństwa w postaci niechcianych programów mogą zostać zainstalowane po tym jak zaakceptujesz umowę.
11. Uważaj na programy, które wyświetlają reklamy w interfejsie użytkownika. Wiele programów typy spyware/adware śledzi, w jaki sposób użytkownik reaguje na takie reklamy. Potraktuj obecność takich reklam jako ostrzeżenie - potencjalne zagrożenie typu spyware.

Rozdział X

Poczta elektroniczna - zasady korzystania i ograniczenia

1. Poczta elektroniczna stanowi podstawową broń w arsenale cyberprzestępców – jest narzędziem do wysyłania spamu, wirusów oraz przeprowadzania ataków phishingowych.
2. Właściwe korzystanie z poczty elektronicznej wiąże się z umiejętnością zabezpieczenia komputera przed działaniami przestępców oraz eliminacji zagrożeń pochodzących z zewnątrz, do których należą:

a) spam, czyli niezamawiane wiadomości zawierające m.in. reklamy różnych usług i produktów,
b) złośliwe oprogramowanie, czyli wirusy, trojany, rootkity, scareware, ransomware przesyłane w postaci załączników do e-maili lub pobierane po kliknięciu w odnośnik zawarty w wiadomości pochodzącej od przestępcy,
c) phishing, czyli atak, którego celem jest wyłudzenie poufnych danych użytkownika poczty e-mail.

3. Przeglądając wiadomości w skrzynce e-mail, wyrób w sobie nawyk odpowiadania na kilka prostych pytań opracowanych przez ekspertów ds. bezpieczeństwa. Celem tych pytań jest pomoc w identyfikacji niebezpiecznych e-maili.

a) Czy znasz nadawcę wiadomości?
b) Czy otrzymywałeś już inne wiadomości od tego nadawcy?
c) Czy spodziewałeś się otrzymać tę wiadomość?
d) Czy tytuł wiadomości i nazwa załącznika mają sens?

e) Czy wiadomość nie zawiera złośliwego oprogramowania – jaki jest wynik skanowania antywirusowego?

4. Pozytywne odpowiedzi na powyższe pytania zwiększą prawdopodobieństwo, że dana wiadomość nie będzie stanowiła zagrożenia dla Twojego systemu.
5. Negatywna odpowiedź na przynajmniej jedno z pytań powinna wzbudzić Twoją czujność i zachęcić do podjęcia działań, które zabezpieczą Cię przed atakiem, takich jak rezygnacja z odpowiedzi na wiadomość, nieklikanie w odnośniki umieszczone w e-mailu lub skasowanie wiadomości bez jej otwierania.
6. Jeżeli otrzymałeś podejrzaną wiadomość usuń ją, a następnie usuń ją z kosza swojej poczty elektronicznej.