**Szkolenie z Bezpieczeństwa Informacji przetwarzanych**

**w Systemie Monitorowania Europejskiego Funduszu Społecznego (SM EFS)**

z dnia 17 sierpnia 2023 r.

**Rozdział I**

**Słownik pojęć**

Użyte w niniejszym dokumencie określenia oznaczają:

1. Administrator Merytoryczny – wyznaczony pracownik Instytucji realizujący zadania określone w Wytycznych,
2. Beneficjent – podmiot, o którym mowa w art. 2 pkt 1 ustawy,
3. CST2021 – system teleinformatyczny o którym mowa w art. 2 pkt 29 Ustawy;
4. Dane osobowe – informacje, o których mowa w art. 4 pkt 1 RODO,
5. Incydent – pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji lub zmniejszeniem poziomu usług systemowych, które stwarzają znaczne prawdopodobieństwo zakłócenia działania SM EFS i zagrażają bezpieczeństwu informacji, w tym danych osobowych przetwarzanych w SM EFS,
6. Konto – zespół cech identyfikujących Użytkownika, z których wynika możliwość dostępu do usług po podaniu identyfikatora użytkownika oraz hasła;
7. Ministerstwo – urząd obsługujący ministra właściwego do spraw rozwoju regionalnego,
8. 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 SM EFS,
9. Program - program w rozumieniu art. 2 pkt 20 ustawy,
10. Realizator – podmiot korzystający z SM EFS w ramach realizacji projektu,
11. 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),
12. Rola – zespół praw i obowiązków wynikających ze statusu Użytkownika w SM EFS;
13. SM EFS – System Monitorowania Europejskiego Funduszu Społecznego administrowany przez Ministerstwo i będący jedną z aplikacji CST2021;
14. 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),
15. Użytkownik - osoba mająca dostęp do SM EFS, wyznaczona przez Instytucję do wykonywania w jej imieniu czynności związanych z realizacją programu lub przez, Beneficjenta lub Realizatora do wykonywania w jego imieniu czynności związanych z realizacją projektu,
16. Właściwa instytucja – instytucja, z którą Beneficjent zawarł umowę lub instytucja rozliczająca projekt (jeśli jest inna niż ta, która zawarła umowę),
17. Wytyczne – Wytyczne ministra właściwego do spraw rozwoju regionalnego w zakresie warunków gromadzenia i przekazywania danych w postaci elektronicznej na lata 2021-2027.
18. Zdarzenie związane z bezpieczeństwem informacji – stan SM EFS, 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 - 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:

a.   poufność – zapewnienie, że informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom, podmiotom lub procesom,

b.   integralność – zapewnienie, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany,

c.   dostępność – zapewnienie bycia osiągalnym i możliwym do wykorzystania na żądanie, w założonym czasie, przez autoryzowany podmiot,

d.   rozliczalność – zapewnienie, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi,

e.   autentyczność – zapewnienie, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana (autentyczność dotyczy użytkowników, procesów, systemów i informacji),

f.    niezaprzeczalność – braku możliwości wyparcia się swego uczestnictwa w całości lub w części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie,

g.   niezawodność – zapewnienie spójności oraz zamierzonych zachowań i skutków.

**Rozdział III**

**Wymagania sprzętowe pozwalające na korzystanie z SM EFS**

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

**Rozdział IV**

**Dostęp do SM EFS**

1. SM EFS jest dostępny pod domeną https://sm.efs.gov.pl (w przypadku środowiska szkoleniowego https://szkol.sm.efs.gov.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 SM EFS. Poziom uprawnień uzależniony jest od pełnionej w systemie roli.

**Rozdział V**

**Zasady bezpieczeństwa w SM EFS**

1. Hasła należy utrzymywać w tajemnicy i nie ujawniać ich innym osobom.
2. Kryteria w zakresie długości, złożoności oraz częstotliwości zmiany haseł:
3. hasło składa się z minimum 12 znaków,
4. hasło zawiera ca najmniej: jedną wielką literę, jedną małą literę, jedną cyfrę oraz jeden znak specjalny,
5. hasło jest zmieniane nie rzadziej niż co 90 dni,
6. hasło nie może zawierać 5 kolejnych znaków z loginu (adresu e-mail),
7. nowe hasło nie może zawierać 5 znaków starego hasła,
8. system nie pozwoli na użycie ostatnich 8 haseł.
9. Czas trwania nieaktywnej sesji (czas bezczynności) po jakim następuje automatyczne wylogowanie użytkownika z systemu wynosi 30 minut.
10. 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 SMEFS).
11. 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.
12. W przypadku zapomnienia hasła należy wykorzystać funkcjonalność „Przypomnij hasło”.
13. Użytkownik powinien przestrzegać zasady czystego biurka. W szczególności przed opuszczeniem swego stanowiska pracy użytkownik powinien schować wszelkie dokumenty związane z używanym SM EFS 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 SM EFS 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 SM EFS powinien sprawdzić:
2. czy w pasku adresowym przeglądarki adres zaczyna się od https,
3. czy w obrębie okna przeglądarki znajduje się mała kłódka informująca o szyfrowanym połączeniu ze stroną,
4. czy po kliknięciu na kłódkę pojawia się informacja o tym, że certyfikat został wydany dla: \*.sm.efs.gov.pl i jest on ważny.
5. Rozpoczęcie pracy użytkownika w systemie następuje po uruchomieniu przeglądarki oraz wprowadzeniu adresu https://sm.efs.gov.pl ( w przypadku środowiska szkoleniowego https://szkol.sm.efs.gov.pl ).
6. Po poprawnym zalogowaniu użytkownik otrzymuje w przeglądarce ekran startowy SM EFS zawierający zakładki modułów, do których użytkownik ma nadany dostęp.
7. W celu chwilowego zawieszenia pracy w SM EFS, należy zablokować ekran (zablokować pulpit lub włączyć wygaszacz ekranu zabezpieczony hasłem). Jeśli komputer użytkownika nie pozwala na zabezpieczenie ekranu hasłem, należy wylogować się z SM EFS.
8. Po zakończeniu pracy należy wylogować się z SM EFS 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 SM EFS**

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 Beneficjenta lub Realizatora 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 Instytucję jest zobowiązany do niezwłocznego powiadomienia Administratora Merytorycznego w tej Instytucji.

3.   Użytkownik będący Administratorem Merytorycznym postępuje zgodnie z Procedurą obsługi zgłoszeń w Service Desk Centralnego Systemu Teleinformatycznego.

**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. Jeżeli korzystasz z bankowości online lub robisz zakupy w sklepach internetowych, wykonuj te czynności wyłącznie na własnym komputerze, nigdy na sprzęcie publicznym. Nie przechowuj żadnych haseł ani numerów kart bankowych w plikach na komputerze.
10. Pamiętaj, że złośliwy kod może zostać zainstalowany na twoim komputerze automatycznie podczas przeglądania Internetu, czy pobierania z niego plików.
11. Uważnie czytaj umowy licencyjne (EULA) zanim zaakceptujesz ich warunki. Niektóre zagrożenia bezpieczeństwa w postaci niechcianych programów mogą zostać zainstalowane po tym jak zaakceptujesz umowę.
12. 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.

**Oświadczam, że zapoznałem/ zapoznałam się ze Szkoleniem z zakresu bezpieczeństwa SM EFS**