POLITYKA BEZPIECZEŃSTWA INFORMACJI I DOKUMENTACJI ELEKTRONICZNEJ

w Federacji Polskich Banków Żywności w ramach Programu Fundusze Europejskie na Pomoc Żywnościową 2021-2027

CZYM JEST BEZPIECZEŃSTWO INFORMACJI?

1. W ramach realizacji Programu Fundusze Europejskie na Pomoc Żywnościową 2021-2027 [FEPŻ] organizacje partnerskie są zobowiązane do zachowania klauzuli poufności[1], a co za tym idzie stosowanie środków bezpieczeństwa dotyczących dokumentacji z realizacji Programu **(czyli wszelkich danych i informacji),** które uzyskują przy realizacji programu. Przypominamy, że to zobowiązanie dotyczy informacji i danych zarówno w systemach informatycznych, a więc w postaci elektronicznej, jak i dokumentów w postaci papierowej. To zobowiązanie jest przewidziane w:
   1.1. Ustawie o pomocy społecznej art. 134m,
   1.2. Wytycznych Instytucji Zarządzającej na realizację danego podprogramu,
   1.3. umowach współpracy z KOWR, a dalej OPO z OPR oraz OPR z OPL.
2. W związku z tym Federacja Polskich Banków Żywności jako Organizacja Partnerska Ogólnopolska [OPO] podejmuje i rekomenduje konkretne działania w systemach informatycznych, zwiększając przez to możliwości cyfrowej realizacji Programu FEPŻ.
3. Bezpieczeństwo informacji, często nazywane w skrócie InfoSec, to zestaw narzędzi i procedur zabezpieczeń, które szeroko chronią poufne informacje organizacji przed nadużyciami, nieautoryzowanym dostępem, zakłóceniami lub zniszczeniem. **To ważne by pamiętać, że niniejszy dokument, jak wskazano w pkt 2, dotyczy InfoSec w obszarze** dokumentacji z realizacji Programu **(czyli wszelkich danych i informacji) procedowanych w postaci elektronicznej w systemach informatycznych.**

PO CO NAM BEZPIECZEŃSTWO INFORMACJI?

4. System Zarządzania Bezpieczeństwem Informacji, czyli strategia działania w zakresie zapewnienia właściwej ochrony informacji poufnych, ma za zadanie ciągłe doskonalenie i optymalizowanie podjętych działań i procedur w celu minimalizacji ryzyk związanych z naruszeniem poufności [zwanym też naruszeniem bezpieczeństwa].
5. FEPŻ jest programem niosącym ze sobą duże ryzyko zniekształcenia procesów administracyjnych. Dlatego Federacja dbając o interes społeczny wszystkich organizacji partnerskich przygotowała stosowne rozwiązania dotyczące bezpieczeństwa informacji i dokumentacji elektronicznej. Zastosowanie tych rozwiązań i zasad ma zapewnić osiągnięcie ww. celu minimalizacji ryzyk, dzięki m.in. zapewnieniu właściwej ścieżki audytu zewnętrznego i wewnętrznego, oraz zapewnić łatwiejsze ustalenie nieprawidłowości i miejsca ich powstania, **ponadto co najważniejsze dla wszystkich organizacji - zwiększyć wiarygodność całego systemu realizacji FEPŻ przez organizacje partnerskie**.

JAKI JEST CEL NINIEJSZEJ POLITYKI?

6. Polityka Bezpieczeństwa Informacji i Dokumentacji Elektronicznej ma dwa cele: zaprezentowanie metod i sposobów zachowania bezpieczeństwa informacji elektronicznej i dokumentacji oraz związanych z nimi procesów przechowywania i udostępniania dokumentacji dotyczącej realizacji Programu FEPŻ przez Federację oraz organizacje partnerskie.

[1] Za art. 134m ust. 4 Ustawy o pomocy społecznej

PODSTAWOWE ZASADY DOTYCZĄCE BEZPIECZEŃSTWA INFORMACJI I DOKUMENTACJI ELEKTRONICZNEJ

7. **[Odpowiedzialność]** Odpowiedzialność za bezpieczeństwo informacji obejmuje nie tylko siedziby OPO, OPR i OPL. To także wszelkie sytuacje, w których informacje związane z realizacją programu przez OPO, OPR i OPL, (niebędące informacją przeznaczoną do publicznego udostępniania) są przetwarzane również poza ich siedzibami. Obejmuje to w szczególności zdalny dostęp do systemów informatycznych KOWR i OPO.
8. **[Zasada odpowiedzialności] Odpowiedzialność ponoszą OPO, OPR oraz OPL, w zakresie w jakim dotyczy to działań lub zaniechań ich współpracowników,** niezależnie od stosunku prawnego (umowy na podstawie której pracują dla danej organizacji) ich łączącego czy odpłatności lub jej braku (za wynagrodzeniem czy społecznie), włączając w to osoby pełniące funkcje w organach statutowych.
9. **[Dostęp]** Dostęp do systemów informatycznych [dalej też zw. aplikacjami], które dostarcza Federacja możliwy jest dla osób wskazanych przez OPO i OPR posiadających adres elektroniczny w domenie bankizywnosci.pl, zaś dla osób wskazanych przez OPL za pośrednictwem zweryfikowanych i autoryzowanych adresów e-mail. **Osoby te funkcjonują dla OPO jako użytkownicy aplikacji w jednej z dwóch ról tj. albo jako przedstawiciele OPR/OPL albo zwykli użytkownicy.** Dostęp udzielany jest w zakresie koniecznym do realizacji zadań w FEPŻ. **Osoby te muszą:**
   9.1. być osobami wskazanymi wyraźnie przez daną organizację partnerską [zgodnie z tzw. Pełnomocnictwem dla Przedstawicieli lub odpowiednio Upoważnieniem dla Użytkowników - zob. odpowiednio wzory z zał. 2 i 4 dla OPR, i 3 lub 5 dla OPL],
   9.2. odbyć szkolenie w zakresie obsługi aplikacji Federacji, do której ma być im udzielony dostęp,
   9.3. muszą potwierdzić ich wyznaczenie do obsługi danej aplikacji Federacji, oraz zapoznanie się z odpowiednimi instrukcjami w tym niniejszą Polityką.
10. **[Aplikacje]** Najczęściej używanymi aplikacjami są:
    10.1. **OPO i OPR:** ENOVA365, Microsoft Office 365, w tym MAŁY POMOCNIK, Aplikacja BEZ@;
    10.2. **OPL:** BEZ@ oraz Microsoft Office 365 - MAŁY POMOCNIK;
    10.3. W przypadku OPR i OPL to wszelkie inne aplikacje użytkowe ułatwiające codzienną pracę, które należy objąć odpowiednimi środkami InfoSec, ale których Federacja nie dostarcza na potrzeby realizacji FEPŻ.
11. **[Przestrzeganie zasad]** Naczelną zasadą pracy organizacji partnerskich z bezpieczeństwem informacji i danych FEPŻ oraz samych użytkowników aplikacji w tym dostarczanych przez Federację, jest przestrzeganie obowiązujących w danej organizacji:
    11.1. organizacji zasad i procedur ochrony danych osobowych i innych dotyczących środków bezpieczeństwa,
    11.2. procedur/Instrukcji dla Użytkownika Systemu (dostarczanych przez Federację),
    11.3. niniejszej polityki.
12. Użytkownicy zobowiązani są do korzystania z aplikacji zgodnie z Instrukcjami przekazami przez OPO, co podkreślamy w tym miejscu niezależnie od innych zobowiązań. Pamiętajmy też, że każda z organizacji OPO/OPR/OPL odpowiada za działania lub zaniechania wyznaczonych przez siebie Użytkowników, w tym za brak niezwłocznego powiadomienia, jeśli należało wyłączyć dostęp danemu Użytkownikowi.

13. **[Oświadczenie o zachowaniu poufności]** OPO, zgodnie z pkt 8, dla zabezpieczenia interesów swoich oraz OPR i OPL wymaga od tych organizacji partnerskich zapoznania Użytkowników [swoich przedstawicieli] z InfoSec oraz potwierdzania przez nich tego jak i zachowania poufności przez Użytkownika poprzez podpisanie oświadczania o zachowaniu poufności **zgodnie ze wzorem nr 1.**
14. OPO/OPR/OPL jest zobowiązane do posiadania podpisanego oświadczenia i jego przechowywania w dokumentacji personalnej osób zaangażowanych w realizację FEPŻ w okresie 10 lat od złożenia sprawozdania przez dane OPO na dany podprogram FEPŻ, co będzie weryfikowane podczas audytu wewnętrznego.
15. **[Pełnomocnictwa przedstawicieli i upoważnienia użytkowników]** OPO wymaga upoważnienia od danej organizacji partnerskiej dla każdej osoby, która ma z ramienia tej organizacji mieć dostęp do systemów dostarczanych przez Federację. Dla osób, które mają móc zatwierdzać dokumenty i składać skuteczne oświadczenia wymagamy pełnomocnictwa dla przedstawicieli zgodnego z wzorem nr 2 lub 3 (OPR odpowiednio OPL). Zaś dla użytkowników zwykłych, czyli bez uprawnień do reprezentacji odpowiednio załącznik nr 4 i 5 (OPR / OPL). Upoważnienia i pełnomocnictwa dotyczą tylko i wyłącznie użytkowania systemów informatycznych i składania oświadczeń woli, rozumianych jako przekazywanie do OPO, KOWR, OPL plików narzędzi informatycznych lub dokumentów w postaci elektronicznej lub papierowej wygenerowanych z narzędzi informatycznych dostarczanych przez Federację, i wiedzy tylko w tym zakresie.
16. Dostęp Użytkowników do aplikacji zostanie udzielony na okres nie dłuższy niż czas realizacji Podprogramu.
17. OPO lub OPR może podjąć decyzję o cofnięciu dostępu w dowolnym terminie. W przypadku cofnięcia dostępu przez OPR należy powiadomić o tym fakcie OPO. W przypadku zakończenia współpracy OPR/OPL z użytkownikiem OPO/OPR winno zostać poinformowane o tym fakcie niezwłocznie celem cofnięcia uprawnień i zablokowania możliwości logowania się do aplikacji.
18. [**Upoważnienie RODO]** OPO/OPR/OPL zapewniają posiadanie również we własnej dokumentacji RODO upoważnień do przetwarzania danych osobowych związanych z realizacją FEPŻ, w szczególności danych osób, którym udzielana jest pomoc żywnościowa. Wynika to z obowiązków z prawa i Wytycznych, że Administrator Danych Osobowych w OPO/OPR/OPL zgodnie z własną Polityką Ochrony Danych Osobowych zobowiązany jest upoważnić personel zaangażowany do realizacji FEPŻ 2021-2027 do przetwarzania danych osobowych. Obowiązek upoważnienia dotyczy zarówno danych i informacji w systemach informatycznych jak i tych przetwarzanych papierowo. Proponujemy w zał. nr 6 wzór takiego upoważnienia.
19. **[RODO w FEPŻ]** Szczegółowe zasady przetwarzania danych osobowym zawarte są w Wytycznych Instytucji Zarządzającej oraz w umowie na realizację FEPŻ między OPO a OPR oraz OPR a OPL.
20. **Podsumowując**, należy powtórzyć, że kwestie upoważnień, klauzuli poufności, dostępnych aplikacji są przedmiotem zapisów w umowach OPO-OPR-OPL, a niniejsza Polityka stanowi jako załącznik tych umów integralną część. Prawo, Wytyczne i umowy wymagają od organizacji całościowego podejścia do przetwarzania danych osobowych, ta Polityka skupia się zaś na bezpieczeństwie informacji w systemach informatycznych. Do Aplikacji Federacji dostęp mogą mieć tylko upoważnione i przeszkolone osoby, a OPO ma dostać od OPR/OPL:

    20.1. oświadczenia tych osób zgodne ze wzorem nr 1,

    20.2. pełnomocnictwa lub upoważnienia do Aplikacji i FEPŻ zgodne ze wzorem nr 2 lub 3, lub odpowiednio nr 4 lub 5, oraz

20.3. możliwość wglądu do upoważnień RODO do przetwarzania danych osobowych w FEPŻ zgodnych ze wzorem nr 6.

DOSTĘP DO APLIKACJI BEZ@, MS365 ORAZ ENOVA365 dla Użytkowników z OPR

21. W celu uzyskania dostępu do aplikacji Dyrektor Banku Żywności przekazuje upoważnienia (wzór 2 lub 4) za pośrednictwem adresu e-mail w domenie bankizywnosci.pl do OPO wraz z prośbą o utworzenie konta użytkownika [imię i nazwisko] i przekazanie danych niezbędnych do logowania.

22. Osoba odpowiedzialna w FPBŻ przekazuje na wskazany adres identyfikatory i hasła dostępowe pierwszego logowania. FPBŻ ma prawo odmówienia dostępu do systemów, o czym informuje Dyrektora Banku Żywności, w szczególności jeśli nie dostarczono odpowiednich oświadczeń lub upoważnień, o których pisaliśmy wcześniej.

DOSTĘP DO APLIKACJI BEZ@, MS365 – MAŁY POMOCNIK dla Użytkowników OPL

23. **Bank Żywności (OPR) wyznacza Użytkownika Głównego** w systemie informatycznym MAŁY POMOCNIK I BEZ@, a Federacja (OPO) udziela mu pełnomocnictwa do udzielania dostępu do MAŁEGO POMOCNIKA I BEZ@ przedstawicielom OPL.
24. W celu uzyskania dostępu do aplikacji Przedstawiciel OPL przekazuje do Dyrektora Banku Żywności upoważnienie zgodnie ze wzorem nr 3 i 5 wraz z prośbą o przekazanie danych niezbędnych do logowania. To OPR poprzez Użytkownika Głównego dokonuje weryfikacji zgłoszenia OPL oraz wskazanych adresów email.
25. Użytkownik Główny w OPR przekazuje na wskazany adres e-mail identyfikatory i hasła dostępowe pierwszego logowania.

26. OPR ma prawo odmówienia dostępu do systemów.

PODSTAWOWA ZASADA, CZYLI 1 OSOBA = 1 HASŁO = 1 LOGIN

27. Uzyskanie dostępu oznacza, że korzystać z niego może tylko OPO/OPR/OPL, czyli tylko działające w jego imieniu osoby fizyczne, które zostały upoważnione do dostępu zgodnie z wcześniej opisanymi regułami.
28. Powyższe oznacza, że OPO/OPR/OPL zapewniają i wymagają od Użytkowników, by nie dzielili dostępu z żadną inną osobą fizyczną. Użytkownik musi dbać o zachowanie swoich loginów i haseł w tajemnicy.
29. W praktyce oznacza to wymóg obsługiwania dostępu tylko i wyłącznie indywidualnym kontem/adresem email.
30. Przy korzystaniu z aplikacji dostarczanych przez Federację wymagana jest weryfikacja: adresu e-mail wraz z hasłem. Federacja sygnalizuje, że potencjalnie możliwe jest przez nią wprowadzenie dodatkowej (tzw. dwuetapowej) weryfikacji za pośrednictwem aplikacji autoryzujących jednorazowym kodem.
31. Wszystkie identyfikatory i hasła dostępowe będą przekazywane przez OPO i OPR w sposób zapewniający ich poufność.
32. Należy pamiętać, że za wszelkie podjęte w aplikacjach działania z wykorzystaniem przydzielonego identyfikatora i hasła odpowiada OPR i OPL, na którego wniosek dostęp został przyznany. To niesłychanie ważne, by pilnować zasady 1osoba=1hasło=1login. Naruszenie wyżej wskazanej zasady, będzie podważać jej rozliczalność i w efekcie wiarygodność całego pomysłu ułatwienia

nam wszystkim pracy poprzez cyfryzację przetwarzania danych i informacji w ramach FEPŻ przez Federację i organizacje partnerskie OPR i OPL.

DOSTĘP DO MS365, ENOVA 365, BEZ@ NA TELEFONACH PRYWATNYCH

33. W przypadku korzystania przez personel OPO/OPR z aplikacji na telefonach prywatnych należy uzyskać na to zgodę Dyrektora OPO/OPR. Zasady korzystania ze sprzętu prywatnego w celach służbowych powinny być opisane w zasadach Ochrony Danych danej organizacji. Dobrą praktyką jest również zawarcie z personelem porozumienia na wykorzystanie sprzętu prywatnego w celach służbowych.
34. W przypadku OPL korzystanie z MS365 - MAŁY POMOCNIK korzystanie z aplikacji na telefonach komórkowych jest zabronione.

ODPOWIEDZIALNOŚĆ UŻYTKOWNIKA KORZYSTAJĄCEGO Z APLIKACJI

35. OPR/OPL, jak już pisaliśmy, ponosi odpowiedzialność .za działania wskazanych przez siebie Użytkowników. Należy podkreślić, że nie ma znaczenia tu stosunek prawny (rodzaj umowy), czy odpłatność lub jej brak (czy pracuje dla Was za wynagrodzeniem czy wolontariacko), na podstawie którego Użytkownik działa w danej organizacji. Dla OPO zasadniczo pozostanie bez znaczenia też, czy OPR/OPL oraz w jaki sposób będzie egzekwowała taką odpowiedzialność.
36. Najważniejsze więc jest rzetelne przygotowanie przez OPR/OPL swojego Użytkownika, przekazanie mu instrukcji, niniejszej polityki, jak i innych zasad przetwarzania danych osobowych, oraz oświadczeń, upoważnień do zapoznania się i podpisu.
37. OPR/OPL muszą zapewnić, by Użytkownik w przypadku wykrycia naruszenia bezpieczeństwa niezwłocznie poinformował właściwego Administratora Danych Osobowych oraz Inspektora Ochrony Danych, jeżeli został wyznaczony w organizacji, a jeśli naruszenie bezpieczeństwa miało miejsce w aplikacjach dostarczonych przez Federację, to również Federację (więcej w pkt 39.3 in.).
38. Jeżeli użytkownik zauważył, że doszło do naruszenia bezpieczeństwa, w szczególności ujawnienia danych do logowania i nie zgłosił tego faktu zgodnie z powyższym obowiązkiem w wyniku czego doszło do naruszenia danych osobowych, to w zupełnie uzasadniony sposób mogą zostać wyciągnięte wobec niego konsekwencje wynikające z art. 52 Kodeksu pracy lub odpowiednio z art. 363 § 1 Kodeksu Cywilnego. Zapoznanie z pojęciami naruszeń bezpieczeństwa czy danych osobowych, zasad przetwarzania, środków bezpieczeństwa jest odpowiedzialnością danej organizacji.
39. Trzeba podkreślić, że szczególną odpowiedzialność za zmianę hasła dostępowego, które zostało przekazane do pierwszego logowania, utworzenie nowego hasła zgodnego z niniejszym standardem oraz jego przechowywanie, i ochrona przed dostępem do niego przez inne osoby. Zabronione jest zapisywanie haseł w menadżerze haseł np. menadżerze haseł Googla, na kartkach w notesach, naklejanie na monitorze komputera, trzymania pod klawiaturą lub w szufladzie oraz umieszczania ich w miejscach dostępnych dla innych osób.
40. **Podsumujmy na potrzeby aplikacji Federacji,** w przypadku zauważenia, że mogło dojść do naruszenia bezpieczeństwa teleinformatycznego w systemach dostarczonych przez Federację
    40.1. użytkownicy z OPL powiadamiają OPL, a OPL zawiadamia OPR oraz OPO,
    40.2. użytkownicy z OPR powiadamiają OPR, a OPR powiadamia OPO.

40.3. niezależnie do tego użytkownicy mają przesłać też informację bezpośrednio do OPO na wskazanych przez OPO adres e-mail:.federacja@bankizywnosci.pl i fepz@bankizywnosci.pl,

40.4. Dodatkowo powyższe organizacje powinny powiadomić w przypadku wykrycia naruszenia bezpieczeństwa teleinformatycznego Inspektora Ochrony Danych, jeżeli został wyznaczony w organizacji.

ZASADY DOTYCZĄCE ZMIANY HASŁA [wszystkich aplikacji dostarczonych przez Federację]

41. Aplikacje wymuszają wprowadzenie minimalnej długości hasła (hasło powinno się składać z min. 12-16 znaków, małe i duże litery, cyfry i symbole) okres maksymalnej ważności hasła oraz uniemożliwiają powtórne wykorzystanie tego samego hasła.
42. Oprogramowanie stosowane w OPO uniemożliwia użytkownikom wybór łatwych do odgadnięcia haseł. Hasło nie powinno być:
    42.1. związane z życiem zawodowym lub osobistym danej osoby (nie powinno być numerem rejestracyjnym samochodu, numerem telefonu, imieniem członka rodziny, częścią adresu);
    42.2. nazwiskiem, nazwą geograficzną, terminem technicznym lub określeniem potocznym;
    42.3. sekwencją kolejnych znaków na klawiaturze, np.: 123456, qwerty;
    42.4. dowolnym elementem spośród wymienionych powyżej z doklejoną na końcu cyfrą lub liczbą.
43. Hasła muszą spełniać, co najmniej jeden z niżej wymienionych warunków:
    43.1. połączenie kilku słów razem;
    43.2. zastąpienie w określonym słowie kilku małych liter dużymi;
    43.3. zastąpienie poszczególnych znaków w haśle wcześniejszymi lub dalszymi znakami w alfabecie lub na klawiaturze;
    43.4. zastąpienie w określonym słowie litery numerami odzwierciedlającymi ich pozycję w alfabecie;
    43.5. połączenie znaków przestankowych, cyfr i słów;
    43.6. umyślne zastosowanie słowa z błędem (niepopełnianym jednak często lub nietypowym);
    43.7. długość hasła dla użytkowników powinna wynosić minimum 12-16 znaków.
44. Dobre praktyki zmiany haseł
    44.1. Użytkownicy nie mogą stosować haseł takich samych lub podobnych do używanych przez nich poprzednio.
    44.2. Rekomendujemy zmianę hasła co minimum 90 dni.
    44.3. Użytkownicy nie mogą używać haseł opartych na ciągu znaków ulegających zmianie w zależności od daty lub innego przewidywalnego czynnika.
    44.4. Hasła nie mogą być wpisywane w obecności osób trzecich, które mogłyby zauważyć treść wpisywanego hasła.
    44.5. Jeśli istnieje podejrzenie, że hasło zostało ujawnione, należy je natychmiast zmienić i zgłosić ten fakt do OPO.

NARUSZENIA BEZPIECZEŃSTWA INFORMACJI I DOKUMENTACJI ELEKTRONICZNEJ

45. Użytkownicy korzystający z aplikacji są zobowiązani do zgłaszania zdarzeń, które wskazują lub świadczą o naruszeniu bezpieczeństwa informacji do OPO zaraz po uzyskaniu takiej informacji.
46. Naruszenia bezpieczeństwa informacji i dokumentacji dokumentacji elektronicznej to w szczególności:
    - 46.1. naruszenie lub próby naruszenia integralności systemu przeznaczonego do przetwarzania informacji;
    - 46.2. naruszenie lub próby naruszenia integralności informacji w systemie przetwarzania - wszelkie modyfikacje (dodanie, zmiana, usunięcie), zniszczenie lub próby ich dokonania przez osoby nieupoważnione lub upoważnione działające w złej wierze lub jako błąd osoby uprawnionej (np. zmiana zawartości danych, utrata całości lub części danych);
    - 46.3. naruszenie poufności poprzez celowe lub nieświadome przekazanie informacji osobie nieuprawnionej do ich otrzymania lub przekazanie informacji wewnątrz sieci OPO-OPR poza domenę bankizywnosci.pl np. na adres w domenie wp.pl, onet.pl, interia.pl, itd.. ;
    - 46.4. naruszenie ochrony informacji w aplikacji (np. nieautoryzowane logowanie do aplikacji lub inny objaw wskazujący na próbę lub działanie związane z nielegalnym dostępem do aplikacji z zewnątrz, skutkujące dostępem do informacji, do których dostęp nie powinien być możliwy);
    - 46.5. nieuprawniony dostęp lub próba dostępu do aplikacji (np. nieuprawniona praca na koncie użytkownika);
    - 46.6. umożliwienie dostępu do informacji osobie nieuprawnionej; niezablokowanie dostępu do aplikacji (podczas nieobecności osoby uprawnionej), brak nadzoru nad serwisantami i innymi osobami nieuprawnionymi;
    - 46.7. nieuprawniony dostęp lub próba dostępu do pomieszczeń, gdzie przetwarza się informacje;
    - 46.8. ujawnienie indywidualnych haseł dostępu użytkowników do aplikacji;
    - 46.9. wykonanie nieuprawnionych kopii informacji lub wydruków;
    - 46.10. niewykonywanie kopii bezpieczeństwa; zmianę lub usunięcie informacji zapisanych na kopiach bezpieczeństwa lub kopiach archiwalnych;
    - 46.11. zamierzoną lub niezamierzoną utratę poufności danych poprzez utratę: sprzętu lub nośnika danych (w tym na skutek kradzieży) i niepodjęcie w stosownym czasie odpowiednich działań neutralizujących.
    - 46.12. brak nośnika zawierającego informacje - kradzież lub zaginięcie wydruku lub innego nośnika informacji;
    - 46.13. niewłaściwe niszczenie nośników informacji zawierających dane wrażliwe lub ustawowo chronione, umożliwiające ich odczyt - wyrzucanie niezniszczonych nośników (np.: wydruk, płyta CD/DVD);
    - 46.14. błędne (nadmierne) nadanie uprawnień do przetwarzania informacji lub nadanie uprawnień osobie niespełniającej wymagań;
    - 46.15. naruszenie dostępności spowodowane nieobecnością w pracy pracowników kluczowych;
    - 46.16. inne zdarzenia, które wskazują lub świadczą o naruszeniu bezpieczeństwa informacji.

POSTANOWIENIA KOŃCOWE

47. Zmiany co do zasad oraz treści załączników w trakcie podprogramu akceptowane są przez Prezesa Federacji w konsultacji z Zarządem. OPO przekazuje niezwłocznie informacje do OPR i OPL o ewentualnych zmianach drogą elektroniczną. W przypadku wniesienia do tego dokumentu zmian w trakcie podprogramu FEPŻ powinien on być ponownie zatwierdzony przez Zarząd Federacji Polskich Banków Żywności przed rozpoczęciem kolejnego podprogramu.

48. Załączniki do niniejszego dokumentu należy traktować jako wzory, które mogą zostać zmodyfikowane przez OPR/OPL zgodnie z potrzebami organizacji. Rekomendujemy, jednakże, aby dokonywane zmiany **zawsze** skonsultować z Biurem Federacji.