ZARZĄDZENIE NR 15/2025
DYREKTORA SUWALSKIEGO OŚRODKA KULTURY

z dnia 18 września 2025 r.

w sprawie zmiany Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, stanowiącym załącznik nr 2 do Zarządzenia nr 5/2021 Dyrektora Suwalskiego Ośrodka Kultury z dnia 8 lutego 2021 r. w sprawie wprowadzenia Polityki bezpieczeństwa informacji oraz Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

Na podstawie § 3 ust.5 pkt 3 Regulaminu Organizacyjnego Suwalskiego Ośrodka Kultury, ustawy z dnia 25 października1991r. o organizowaniu i prowadzeniu działalności kulturalnej (Dz.U. z 2024 r. poz. 87 tj.) oraz na podstawie Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. 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, dalej:RODO) (Dz.Urz.UE.L Nr 119, str. 1), zarządzam co następuje:

§ 1.

Zmieniam Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, stanowiącą załącznik nr 2 do Zarządzenia nr 5/2021 Dyrektora Suwalskiego Ośrodka Kultury z dnia 8.02.2021r. w sprawie wprowadzenia Polityki bezpieczeństwa informacji oraz Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, nadając brzmienie określone w załączniku nr 1 do niniejszego Zarządzenia.

§ 2.

Wykonanie Zarządzenia powierzam zastępcy dyrektora Suwalskiego Ośrodka Kultury oraz kierownikom komórek organizacyjnych Suwalskiego Ośrodka Kultury.

§ 3.

Zarządzenie wchodzi w życie z dniem podpisania.

Dyrektor Suwalskiego
Ośrodka Kultury

Ignacy Ołów

Załącznik do zarządzenia nr 15/2025
Dyrektora Suwalskiego Ośrodka Kultury
z dnia 18 września 2025 r.

Instrukcja zarządzania systemem informatycznym służącym

do przetwarzania danych osobowych.

(poprzednio Załącznik nr 2 do Zarządzenia nr 5/2021 z dnia 8 lutego 2021 r.)

Rozdział I.
Postanowienia ogólne

1. Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, zwana dalej „Instrukcją", określa procedury dotyczące zasad bezpieczeństwa przetwarzania danych osobowych oraz zasady postępowania administratora danych osobowych, osób przez niego wyznaczonych i użytkowników przetwarzających dane osobowe w Suwalskim Ośrodku Kultury zwanym dalej „Ośrodkiem".

2. Instrukcja została opracowana zgodnie z Rozporządzeniem Parlamentu Europejskiego iRady (UE) 2016/679 zdnia 27 kwietnia 2016 r. wsprawie ochrony osób fizycznych wzwiązku zprzetwarzaniem danych osobowych iw sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie oochronie danych) oraz rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024) oraz rozporządzenia Ministra Sprawiedliwości z dnia 28 kwietnia 2004 r. w sprawie sposobu technicznego przygotowania systemów i sieci do przekazywania informacji – do gromadzenia wykazów połączeń telefonicznych i innych przekazów informacji oraz sposobów zabezpieczenia danych informatycznych (Dz. U. Nr 100, poz. 1023).

3. Dyrektor Ośrodka wykonuje obowiązki administratora danych osobowych i administratora systemów informatycznych, a funkcję Inspektora Ochrony Danych sprawuje wyznaczony pracownik w odniesieniu do prowadzonych w Ośrodku zbiorów danych.

4. W systemach informatycznych służących do przetwarzania danych osobowych w Ośrodku stosuje się środki bezpieczeństwa na poziomie wysokim.

Rozdział II.
Nadawanie uprawnień do przetwarzania danych osobowych oraz ich rejestrowanie w systemie informatycznym.

1. Przed dopuszczeniem do pracy przy przetwarzaniu danych osobowych, każdy użytkownik powinien zostać zapoznany przez Inspektora Ochrony Danych z przepisami dotyczącymi ochrony danych osobowych oraz obowiązującymi w Ośrodku wewnętrznymi regulacjami w tym zakresie.

2. Do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych osobowych, mogą zostać dopuszczone wyłącznie osoby posiadające upoważnienie do przetwarzania danych osobowych wydane przez administratora danych osobowych.

3. Przyznanie uprawnień do przetwarzania danych osobowych w systemie informatycznym polega na przekazaniu dostępu do hasła oraz ustalenia zakresu dostępnych danych.
Inspektor ochrony Danych jest zobowiązany do prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych.

Rozdział III.
Stosowane metody i środki uwierzytelniania użytkownika oraz procedury związane z ich zarządzaniem i użytkowaniem.

1. Użytkownik uzyskuje dostęp do danych osobowych wyłącznie po podaniu hasła zaraz po włączeniu komputera.

2. Hasło składa się co najmniej z 8 znaków.

3. Hasło powinno zawierać małe i wielkie litery oraz cyfry i znaki specjalne (tzw. silne hasło).

4. Hasło nie może być zapisane w miejscu dostępnym dla osób nieuprawnionych i należy je zachować w tajemnicy.

5. Hasło należy zmieniać co najmniej raz na miesiąc, zmiany są systemowe lub programowe, przeprowadzane na bieżąco oraz w miarę potrzeby.

6. Użytkownik nie może udostępniać osobom nieuprawnionym hasła dostępu oraz osobom nieuprawnionym dostępu do swojego stanowiska pracy.

7. W przypadku, gdy istnieje podejrzenie, że hasło mogła poznać osoba nieuprawniona, użytkownik zobowiązany jest niezwłocznie zmienić hasło.

8. Hasła do firmowej poczty elektronicznej nie mogą być zapisane na stałe w programie pocztowym komputera.

Rozdział IV.
Rozpoczęcie, zawieszenie i zakończenie pracy przez użytkowników systemu

1. Użytkownik rozpoczynając pracę na komputerze loguje się do systemu informatycznego lub programu pocztowego.

2. Monitory stanowisk komputerowych, na których przetwarzane są dane osobowe, znajdujące się w pomieszczeniach, gdzie przebywają osoby, które nie posiadają upoważnień do przetwarzania danych osobowych, należy ustawić w taki sposób, aby uniemożliwić tym osobom wgląd w dane. Kończąc pracę użytkownik obowiązany jest wyłączyć sprzęt komputerowy. Monitor z danymi wrażliwymi nie może stać przy oknie, do którego możliwy jest dostęp dla osób postronnych.

Rozdział V.
Korzystanie z bankowości internetowej.

1. Do dokonywania operacji związanych z obsługą bankowości internetowej, dostępu do konta Ośrodka i wykonywania jakichkolwiek operacji, upoważnieni są wyłącznie główny księgowy i osoby upoważnione przez Dyrekcję.

2. Zabrania się przechowywania haseł dostępu do konta na biurku, w dokumentacji, razem z osobistym kluczem do konta (token), zapisywania w notatkach, w pamięci komputera na dyskach. Hasła i login należy zapamiętać.

3. Osobisty klucz do konta (token) każda z osób, główny księgowy i inne osoby upoważnione, przechowują w sposób należycie zabezpieczony, zapewniający nieużycie przez osoby trzecie. Po wylogowaniu się z banku, w czasie godzin pracy, token zamykany jest na klucz w kontenerach przy biurkach, a na zakończenie dnia pracy, w szafie pancernej.

4. Główny księgowy wprowadza wszelkie dane, które następnie zatwierdza Dyrektor.

5. Zabrania się korzystania z bankowości internetowej na komputerze, na którym stwierdzono źle działającą ochronę, oprogramowanie lub inne problemy.

6. W czasie wykonywania operacji bankowych, zabrania się odchodzenia od komputera, przyjmowania rozmów telefonicznych i załatwiania innych spraw.

Rozdział VI.
Tworzenie kopii zapasowych zbiorów danych.

1. Dane osobowe przetwarzane w systemie informatycznym podlegają zabezpieczeniu poprzez tworzenie cyklicznie (nie rzadziej niż raz na pół roku) kopii zapasowych.

2. Kopie zapasowe przechowywane są na dysku zewnętrznym w szafie pancernej.

3. Za bezpieczeństwo danych zapisanych w komputerach przenośnych oraz w innych urządzeniach przenośnych w całości odpowiada użytkownik komputera lub urządzenia przenośnego.

4. Zbędne wydruki zawierające dane osobowe natychmiast po wykorzystaniu muszą zostać zniszczone w niszczarce dokumentów.

5. Kopie zapasowe przechowuje się przez okres dwunastu miesięcy po okresie sporządzenia kopii.

Rozdział VII.
Sposób zabezpieczenia systemu informatycznego przed działaniem oprogramowania, którego celem jest uzyskanie dostępu do systemu informatycznego danych osobowych.

1. Za ochronę antywirusową systemu informatycznego odpowiada administrator danych osobowych.

2. System antywirusowy zainstalowany jest w każdym komputerze, systemy operacyjne mogą zawierać dodatkowe/wewnętrzne programy antywirusowe.

3. Program antywirusowy jest uaktywniony przez cały czas pracy każdego komputera
w systemie informatycznym lub programie pocztowym.

4. Wszystkie pliki otrzymane z zewnątrz, jak również wysyłane na zewnątrz, podlegają automatycznemu sprawdzeniu przez system antywirusowy pod kątem występowania wirusów, z zastosowaniem najnowszej dostępnej wersji programu antywirusowego.

5. W przypadku pojawienia się wirusa, użytkownik obowiązany jest zaprzestać wykonywania jakichkolwiek czynności w systemie i niezwłocznie powiadomić administratora bezpieczeństwa informacji.

6. Aktualizacje systemu/programu antywirusowego przeprowadzane są systemowo, programowo, cyklicznie oraz w razie potrzeby.

Rozdział VIII.
Udostępnianie danych osobowych i sposób odnotowywania informacji o udostępnianiu danych.

1. Dane osobowe przetwarzane w Ośrodku mogą być udostępnione osobom lub podmiotom uprawnionym do ich otrzymania na mocy Rozporządzenia Parlamentu Europejskiego iRady (UE) 2016/679 zdnia 27 kwietnia 2016 r. wsprawie ochrony osób fizycznych wzwiązku zprzetwarzaniem danych osobowych iw sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie oochronie danych) oraz innych przepisów powszechnie obowiązujących.

2. Dane osobowe udostępnia się na pisemny, umotywowany wniosek chyba, że przepisy odrębne stanowią inaczej.

3. Dane udostępnione Ośrodkowi przez inny podmiot można wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.

4. Dokładna kopia danych osobowych przesłanych do Zakładu Ubezpieczeń Społecznych przechowywana jest w bazie danych programu WOLTERS KLUWER postaci dokumentów i zestawów dokumentów oznaczonych odpowiednim statusem dokumentu lub zestawu, datą utworzenia dokumentu, datą wysłania zestawu.

5. Dokładna kopia danych osobowych przesłanych do banku przechowywana jest w bazie danych systemu bankowości elektronicznej do wejścia, której konieczne jest wprowadzenie loginu i hasła.

Rozdział IX.
Wykonywanie przeglądów i konserwacji systemu oraz nośników danych służących do przetwarzania danych.

1. Wszelkie prace związane z naprawami sprzętu komputerowego wykonywane są przez firmę zatrudnioną na podstawie umowy z klauzulą powierzenia przetwarzania danych osobowych i zachowaniem tajemnicy.

2. Zmiana konfiguracji sprzętu komputerowego, na którym znajdują się dane osobowe lub zmiana jego lokalizacji, może być dokonana tylko za wiedzą i zgodą administratora danych osobowych.

Rozdział X.
Korzystanie z poczty elektronicznej

1. Nadzór i opiekę techniczną nad systemem poczty elektronicznej sprawuje podmiot na podstawie umowy zawartej z SOK.

2. Użytkownik w okresie wykonywania obowiązków wynikających z umowy o pracę zobowiązany jest do sprawdzania skrzynki poczty elektronicznej udostępnionej przez pracodawcę w celu realizacji czynności zawodowych wynikających z umowy o pracę i zleconych dodatkowo przez pracodawcę,

3. Na wniosek istnieje możliwość utworzenia innego adresu, niż standardowa struktura. We wniosku wskazuje się osobę odpowiedzialną za użytkowanie skrzynki poczty elektronicznej i proponowany adres.

4. Poczta elektroniczna służy wyłącznie do celów służbowych. Wszelkie prywatne wiadomości zostaną usunięte przez Administratora Systemu.

5. Zabrania się rozsyłania m.in.:

1) ogłoszeń komercyjnych,

2) tzw. łańcuszków szczęścia (listów, które wykorzystując elementy socjotechniki generują niepożądany ruch na serwerze/rach poczty elektronicznej),

3) treści wulgarnych,

4) materiałów erotycznych,

5) treści niezgodnych z obowiązującymi przepisami prawa,

6) treści prawem chronionych bez odpowiedniego zabezpieczenia, np. szyfrowanie,

7) subskrypcji stron www (np. korzystania z newslettera),

8) treści maila lub w załączniku informacji zawierających dane osobowe lub inne dane prawnie chronione do adresatów spoza domen przyjętych w SOK, bez odpowiedniego zabezpieczenia,

9) przy wysyłaniu informacji zawierających dane osobowe należy:

a) w treści wiadomości nie zawierać żadnych danych osobowych/danych chronionych prawem,

b) załącznik zawierający dane osobowe/dane chronione prawem – zaszyfrować (tzn. spakować i zabezpieczyć hasłem),

c) hasło do rozpakowania załącznika przekazać adresatowi w inny sposób (nie poczta elektroniczną, np. sms).

6. Korespondencja, którą przechowuje i dostarcza system pocztowy jest własnością Pracodawcy.

7. Pracodawca w celach dowodowych oraz bezpieczeństwa systemów ma prawo do, kontroli skrzynek pocztowych użytkowników. O wynikach kontroli powinien by, poinformowany użytkownik.

8. Korespondencja elektroniczna, jak i pliki mogą zostać udostępnione innemu pracownikowi. Czynności tej dokonać można na pisemny wniosek przełożonego pracownika, którego dane mają zostać udostępnione. We wniosku wskazuje się powód udostępnienia oraz osobę, której udostępnia się opisywane zasoby.

9. Pracodawca zastrzega sobie prawo do:

1) natychmiastowej blokady skrzynki pocztowej w uzasadnionych przypadkach (takich jak naruszenie bezpieczeństwa, wykorzystanie skrzynki w sposób niezgodny z przeznaczeniem, przebywaniem pracownika na urlopie bezpłatnym, innej usprawiedliwionej i nieusprawiedliwionej nieobecności w pracy, w okresie wypowiedzenia umowy o pracę w okresie zwolnienia pracownika ze świadczenia pracy),

2) awaryjnego wyłączenia systemu bez uprzedniego powiadomienia,

3) zmiany zasad funkcjonowania poczty elektronicznej. Zmiany będą podawane do wiadomości za pomocą poczty elektronicznej.

4) odmowy założenia skrzynki pocztowej w uzasadnionych przypadkach.

10. Nie należy otwierać linków oraz załączników poczty elektronicznej ze źródeł niewiadomego pochodzenia.

11. Po pojawieniu się nieoczekiwanych listów z załącznikami powinno się informować informatyka.

12. W przypadku dostępu do poczty elektronicznej z sieci Internet należy przeczytać uważnie pojawiające się w przeglądarce komunikaty o alertach bezpieczeństwa i nigdy nie ignorować ostrzeżeń.

13. Nie zaleca się logowania do systemów poczty elektronicznej z komputerów dostępnych publicznie (np. kafejki internetowe, punkty Hot Spot).

14. Zabrania się konfiguracji prywatnych kont pocztowych w programach umożliwiających wysyłanie i odbieranie poczty e-mail.

15. Skrzynki pocztowe posiadają ograniczoną wielkość. Użytkownik zobowiązany jest do okresowej archiwizacji wiadomości.

16. Niszczenie brudnopisów, błędnych lub zbędnych kopii materiałów zawierających dane osobowe musi odbywać się w sposób uniemożliwiający odczytanie zawartej w nich treści, np.z wykorzystaniem niszczarki.

17. Niedopuszczalne jest wynoszenie materiałów zawierających dane osobowe poza obszar ich przetwarzania bez związku z wykonywaniem czynności służbowych. Za bezpieczeństwo i zwrot materiałów zawierających dane osobowe odpowiada w takim przypadku osoba dokonująca ich wyniesienia oraz jej bezpośredni przełożony.

Rozdział XI.
Korzystanie z internetu

1. Pracodawca wprowadza kategoryzację dostępu do sieci Internet.

2. Użytkownicy mogą korzystać z dostępu do Internetu tylko w celach służbowych.

3. Praca w sieci Internet nie może zagrażać bezpieczeństwu systemów informatycznych.

4. Pracodawca może wprowadzić kategoryzację stron internetowych oraz zablokować określonym osobom lub grupom dostęp do wybranych kategorii.

5. Odblokowanie witryny internetowej może nastąpić na pisemny wniosek kierownika komórki organizacyjnej, zatwierdzony przez IOD.

6. Zabrania się:

1) wykorzystywania sieci Internet w sposób, który mógłby narazić Pracodawcę na utratę dobrego imienia,

2) pobierania oprogramowania (w tym w wersjach darmowych), niezwiązanego z wykonywanymi obowiązkami służbowymi,

3) podłączania sieci Internet do fizycznie odseparowanych sieci,

4) udostępniania łącza internetowego dostarczonego przez pracodawcę innym osobom bez zgody kierownika komórki organizacyjnej oraz informatyka,

5) przekazywania identyfikatorów i haseł innym użytkownikom (wykorzystywania identyfikatorów i haseł innych użytkowników) do podnoszenia uprawnień dostępu do Internetu.

Rozdział XII.
Zgłaszanie incydentów informatycznych

1. Obowiązkiem każdego użytkownika jest kontrola poprawności działania sprzętu i oprogramowania jakim dysponuje.

2. Wszystkie zaistniałe incydenty praz podatności z zakresu informatyki należy bezzwłocznie zgłaszać informatykowi zgodnie z Procedurą reagowania na naruszenia ochrony danych osobowych.

3. Incydenty lub podatności na incydenty niezwiązane bezpośrednio z systemami informatycznymi (np. zalania, awarie zasilania itp.), należy kierować bezpośrednio do działu administracyjnego.

4. Wprowadza się następujące drogi przekazu informacji dotyczącej incydentów lub podatności: system zgłoszeniowy, a w szczególnych przypadkach: telefon, powiadomienie osobiste, poczta elektroniczna. Wybór środka przekazu zgłoszeniowego powinien być adekwatny do zaistniałej sytuacji.

5. W przypadku zgłaszania incydentów i podatności dotyczących danych osobowych, należy powiadomić Inspektora Ochrony Danych.