Instrukcja zarządzania systemem informatycznym

Wersja dokumentu 1.00 z dnia 9 marca 2020 roku

GMINNY OŚRODEK KULTURY
SPORTU I REKREACJI
ul. REKREACYJNA 1, 72-005 PRZECŁAW
NIP: 8513239302 Regon 383734596

ZATWIERDZAM
GMINNY OŚRODEK KULTURY
SPORTU I REKREACJI
Mariusz Skóra
DYREKTOR

.....

podpis Dyrektora

Przecław, marzec 2020

GMINNY OŚRODEK KULTURY
SPORTU I REKREACJI
ul. REKREACYJNA 1, 72-005 PRZECŁAW
NIP: 8513239302 Regon 383734596

Spis treści

2.3 Osobą uprawnioną do wskazania konieczności posiadania uprawnień do systemów informatycznych, w tym do systemów, w których przetwarzane są dane osobowe jest Dyrektor GOKSiR bądź osoba przez niego upoważniona.

2.4 ASI w związku z nadawaniem uprawnień dostępowych do systemu informatycznego zobowiązuje się do:

- ✓ określenia w formie pisemnej zasad tworzenia loginów do systemów informatycznych o ile twórca systemu lub administrator centralny systemu nie określił zasad ich tworzenia;
- ✓ w przypadku, gdy dana osoba na podstawie wydanego upoważnienia do przetwarzania danych osobowych, otrzymuje uprawnienia dostępowe do systemów informatycznych po raz pierwszy, informuje ją o zasadach bezpieczeństwa związanych z ich użytkowaniem;
- ✓ nadaje osobie upoważnionej, indywidualny login i hasło do pierwszego zalogowania się w systemie i instruuje osobę o konieczności jego zmiany po zalogowaniu się do systemu, wskazując sposób wykonania tej czynności;
- ✓ powstrzymania się przed nadaniem uprawnień dostępowych w przypadku, jeżeli dana osoba nie posiada upoważnienia do przetwarzania danych osobowych w wymaganym zakresie zatwierdzonego przez ADO;
- ✓ nadania użytkownikowi unikalnego loginu w systemie informatycznym i nie może być to login, który w przeszłości był już stosowany w systemie informatycznym. Sprawdzenie unikalności loginu odbywa się na podstawie *Rejestru osób upoważnionych do systemów,* którego wzór stanowi **załącznik nr 1** do niniejszej instrukcji;
- ✓ prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych w systemach informatycznych w postaci *Rejestru osób upoważnionych do systemów*;
- ✓ skonfigurowania systemu w sposób zapewniający wymuszenie zmiany hasła przez użytkownika okresowo co 30 dni;
- ✓ hasła administracyjne mogą być w szczególnych sytuacjach stosowane dłużej niż zaznaczono to powyżej, jednak nie dłużej niż 6 miesięcy i każdorazowo po rozwiązaniu umowy z administratorem systemu informatycznego;
- ✓ skonfigurowania systemu, by hasło dostępu do systemu informatycznego spełniało poniższe warunki:
  - długość co najmniej 8 znaków,
  - zawierało małe i duże litery,
  - zawierało cyfry lub znaki specjalne,
  - w trakcie wpisywania, nie było widoczne na ekranie monitora,

3.3 Rozpoczęcie pracy na stacji roboczej następuje poprzez:

- ✓ uruchomienie komputera;
- ✓ wprowadzenie loginu i hasła lub samego hasła, w zależności od sposobu skonfigurowania jednostki;
- ✓ hasła są wprowadzane w sposób minimalizujący ryzyko podejrzenia ich przez osoby postronne;
- ✓ w przypadku problemów z rozpoczęciem pracy, spowodowanych odrzuceniem przez system wprowadzonego loginu i hasła, użytkownik natychmiast powiadamia o tym fakcie Dyrektora GOKSiR i administratora systemu informatycznego;
- ✓ w przypadku niestandardowego zachowania aplikacji przetwarzającej dane osobowe, pracownik natychmiast powiadamia o zaistniałym fakcie Dyrektora jednostki i administratora systemu informatycznego oraz powstrzymuje się przed dalszym korzystaniem z aplikacji.

3.4 Zabrania się wykonywania jakichkolwiek operacji w systemie informatycznym służącym do przetwarzania danych osobowych z wykorzystaniem loginu i hasła dostępu innego użytkownika.

3.5 W przypadku czasowego opuszczenia stanowiska pracy, użytkownik musi:

- ✓ dokonać zapisu wprowadzonych danych, wylogować się z systemu informatycznego służącego do przetwarzania danych osobowych;
- ✓ zablokować stację roboczą odpowiednią kombinacją klawiszy, przy czym odblokowanie może nastąpić dopiero po podaniu hasła [klawisze: windows+L lub klawisze: ctr+alt+delet].

3.6 W przypadku zakończenia pracy użytkownik musi:

- ✓ wylogować się z systemu informatycznego służącym do przetwarzania danych osobowych. Wylogowanie powinno być poprzedzone zapisem wprowadzonych danych, opcjonalnie sporządzeniem w miarę potrzeb kopii zapasowej danych oraz zabezpieczeniem przed nieuprawnionym dostępem nośników danych płyty CD, pendrive i innych, zawierających dane osobowe;
- ✓ zamknąć wszystkie aplikacje uruchomione na stacji roboczej;
- ✓ wyłączyć stację roboczą za pomocą odpowiednich poleceń, zawartych w zainstalowanym na niej systemie operacyjnym. Zabronione jest wyłączanie jednostki za pomocą przycisków „POWER" lub „RESET", (możliwe tylko i wyłącznie na wyraźne polecenie administratora systemu informatycznego);
- ✓ po wyłączeniu stacji roboczej, należy wyłączyć wszystkie pozostałe urządzenia z nią współpracujące, takie jak: monitor, drukarka, skaner, UPS, itp.;

tylko i wyłącznie z okresu jednego dnia i przechowywać nie dłużej, niż do końca następnego dnia roboczego.

4.2 Administrator systemu informatycznego prowadzi rejestr kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania.

4.3 Dla każdego elementu wymienionego w pkt. 4.2 będącego przedmiotem wykonywania kopii zapasowych, administrator systemu informatycznego w porozumieniu z użytkownikiem (grupą użytkowników, komórką organizacyjną użytkującą elementy), określa częstotliwość wykonywania kopii zapasowych oraz częstotliwość sprawdzeń przywracania danych w oparciu o wykonane kopie. Przedmiotowe ustalenia muszą zostać udokumentowane w postaci przyjętego harmonogramu wykonywania kopii zapasowych. Wzór *Harmonogramu wykonywania kopii zapasowych* stanowi **załącznik nr 5.**

4.4 Administrator systemu informatycznego w odniesieniu do każdego systemu, określi rodzaj wykonywanej kopii wybierając jej wariant z możliwych, o których mowa poniżej tj.

- ✓ standardowa – polega na skopiowaniu każdego wybranego pliku i wyczyszczeniu archiwa. Dzięki czemu przy tworzeniu kolejnej kopi zapiszą się pliki, w których zmieniło się archiwum. Tworzenie tego typu kopi trwa najdłużej. Zazwyczaj jest wykonywane przy tworzeniu pierwszej kopi;
- ✓ przyrostowa – wybór tego typu kopi zapasowej powoduje archiwizacje plików które zostały utworzone lub zmodyfikowane od momentu wykonania ostatniej kopi przyrostowej lub kopi normalnej. Proces odtwarzania danych polega na przywróceniu normalnej kopi zapasowej oraz kopi przyrostowych w kolejności tworzenia. Tworzenie kopi przyrostowej zajmuje mniej miejsca oraz mniej czasu niż w porównaniu z kopią normalną. Jednak odtwarzanie zajmuje więcej czasu;
- ✓ różnicowa – kopiuje tyle te pliki, które zmieniły się od czasu wykonania ostatniej kopii normalnej lub przyrostowej. Kopia różnicowa nie zmienia atrybuty archiwizacji plików. Aby przywrócić dane wystarczy kopia normalna i ostatnia kopia różnicowa. Kopia ta zajmuje więcej miejsca niż kopia przyrostowa, ale nie trzeba każdej wersji przechowywać na dysku, bo wystarczy najnowsza;
- ✓ codzienna – wykonuje kopie tylko tych plików które zostały utworzone lub zmienione w dni wykonania archiwizacji. Podczas wykonywania tej kopi nie jest czyszczony atrybut archiwizacji;
- ✓ kopia (backup) – polega na skopiowaniu zaznaczonych plików bez czyszczenia atrybutów archiwizacji. Opcja ta przydaje się dla osób, które wykonują kopie raz na jakiś czas i nie potrzebują regularnej archiwizacji lub chcą mieć dodatkową kopię pomiędzy cyklem archiwizacji.

5.4 Elektroniczne nośniki informacji, a także wydruki i inne dokumenty zawierające dane osobowe przechowywane są w zamykanych szafach w pomieszczeniach stanowiących obszar przetwarzania danych osobowych, celem zabezpieczenia ich przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem i zniszczeniem.

5.5 Nośniki zawierające kopie zapasowe, których celem jest zapewnienie możliwości przywrócenia działania i odtworzenia danych po awarii lub innym zdarzeniu o charakterze katastroficznym, winny być przechowywane w innych lokalizacjach niż lokalizacja jednostki, przy jednoczesnym spełnieniu wszystkich zasad bezpiecznego przechowywania, dających gwarancję ich zabezpieczenia przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem i zniszczeniem oraz gwarancję pełnej dostępności na wypadek konieczności ich wykorzystania w celu przywrócenia lub odtworzenia działań jednostki.

5.6 Okres przechowywania nośników informacji zawierających kopie zapasowe dla poszczególnych systemów informatycznych służących przetwarzaniu danych osobowych określa **załącznik nr 5** do Instrukcji – *Harmonogram wykonywania kopii zapasowych.* Po upływie tego okresu nośniki danych są niszczone lub dane na nich zawarte trwale usuwane.

5.7 Dopuszcza się powierzenie niszczenia nośników (szczególnie papierowych) danych osobowych, wyspecjalizowanym podmiotom zewnętrznym, pod warunkiem:

- ✓ zawarcia umowy powierzenia danych osobowych do dalszego przetwarzania z tym podmiotem;
- ✓ zagwarantowania poufności danych przez usługodawcę;
- ✓ umożliwienia prowadzenia nadzoru nad procesem niszczenia nośników przez IOD lub upoważnionego przez niego pracownika jednostki;
- ✓ udokumentowania faktu przekazania nośników do zniszczenia protokołem.

5.8 W przypadku wycofania sprzętu komputerowego z użycia, dane osobowe na nim zapisane są kasowane przez administratora systemu informatycznego przy użyciu dedykowanego oprogramowania do bezpiecznego usuwania danych. W przypadku braku możliwości programowego usunięcia danych, dysk podlega fizycznemu zniszczeniu. Za zniszczenie danych odpowiada administrator systemu informatycznego. Zniszczenie nośnika potwierdzane jest protokołem przechowywanym przez administratora systemu informatycznego.

5.9 W przypadku przekazania sprzętu komputerowego do podmiotu zewnętrznego, celem jego naprawy, należy usunąć z niego wszystkie zapisy zawierające dane osobowe, jeżeli jest to niemożliwe

- ✓ zaporę sieciową;
- ✓ wykorzystywanie wyłącznie oprogramowania systemowego posiadającego wsparcie techniczne;
- ✓ automatyczną aktualizację oprogramowania systemowego oraz antywirusowego;
- ✓ konfigurację oprogramowania, o którym mowa powyżej w sposób minimalizujący ryzyko naruszenia bezpieczeństwa (ciągła praca w tle i wykrywanie zagrożeń w czasie rzeczywistym);
- ✓ monitoring ruchu sieciowego;
- ✓ zainstalowanie ww. oprogramowania na każdej stacji roboczej i jednostce komputerowej.
- ✓ stałe blokowanie dostępu do stron internetowych sklasyfikowanych jako potencjalnie niebezpieczne (np.: portale randkowe, plotkarskie, erotyczne).

6.4 Za nadzór nad powyższymi zabezpieczeniami jest odpowiedzialny administrator systemu informatycznego, a w szczególności za:

- ✓ weryfikację aktualności sygnatur systemu antywirusowego i podejmowanie ewentualnych działań korekcyjnych;
- ✓ weryfikację logów systemu antywirusowego i podejmowanie działań korekcyjnych;
- ✓ przegląd logów zapory sieciowej oraz podejmowanie działań mających na celu zablokowanie ataków sieciowych;
- ✓ weryfikację poprawności aktualizacji oprogramowania systemowego.

7. Wykonywanie przeglądów i konserwacji systemów informatycznych oraz urządzeń służących do ich funkcjonowania

7.1 Konserwacja sprzętu i urządzeń pracujących w systemach informatycznych jednostki ma na celu, zapewnienie nieprzerwanej i bezpiecznej pracy tych systemów, zapobieganie utraty, uszkodzeniu lub naruszenia bezpieczeństwa.

7.2 Przeglądy i konserwacje urządzeń wchodzących w skład użytkowanych systemów informatycznych, są dokonywane przez administratora systemu informatycznego, wyznaczone przez niego osoby lub przez podmioty zewnętrzne w oparciu o zawarte umowy serwisowe.

7.3 W odniesieniu do użytkowanej w jednostce infrastruktury informatycznej realizowane są okresowe czynności konserwacyjne w sposób zapewniający, iż każdy jej element (jednostki robocze, drukarki, skanery, monitory itd.), zostanie objęty czynnościami, o których mowa minimum raz w roku. Harmonogram prac z tym związanych sporządza administrator systemu informatycznego wg **załącznika nr 6** do niniejszej instrukcji – *Harmonogram przeglądów i konserwacji urządzeń*. Przy tworzeniu harmonogramu należy uwzględnić zalecenia producenta urządzenia.

- ✓ określenie miejsca zainstalowania (ze wskazaniem nr inwentarzowego jednostki komputerowej lub jej nazwy, komórki organizacyjnej, nr pomieszczenia),

8.2 IOD niezależnie od innych osób posiada prawo do kontroli spisu licencjonowanego oprogramowania ze względu na charakter realizowanych działań.

8.3 Kontrole IOD licencjonowanego oprogramowania mogą być przeprowadzane w trybie doraźnym po uprzednim poinformowaniu Dyrektora jednostki.

8.4 Do przesłanek uruchamiających proces kontroli doraźnej w szczególności można zaliczyć:

- ✓ informację o popełnieniu lub podejrzeniu popełnienia czynu niedozwolonego przez pracownika, na żądanie Dyrektora GOKSiR lub innej osoby posiadającej wiedzę o takim zdarzeniu;
- ✓ otrzymanie zgłoszenia lub innej informacji o pojawieniu się lub podejrzeniu pojawienia się w systemie informatycznym nieautoryzowanego oprogramowania, aplikacji,

8.5 Nie rzadziej niż raz na dwa lata IOD w porozumieniu z ASI przeprowadza planową kontrolę spisu użytkowanego w jednostce oprogramowania.

8.6 Okresowo, nie rzadziej niż raz w roku, wszystkie komputery przenośne użytkowane poza lokalizacjami jednostki są sprawdzane przez administratora systemu informatycznego pod kątem obecności nieautoryzowanego oprogramowania.

8.7 W terminie do 20 stycznia każdego roku obrachunkowego celem zatwierdzenia, administrator systemu informatycznego przedstawia Dyrektorowi jednostki aktualne zestawienie przenośnych jednostek komputerowych, o których mowa w pkt. 8.6 wraz z harmonogramem ich przeglądu.

8.8 Do przeprowadzenia kontroli zgodności zainstalowanego oprogramowania z posiadanymi licencjami, a także zgodności z konfiguracją standardową, mogą zostać zastosowane narzędzia programistyczne umożliwiające m.in.:

- ✓ automatyczne sprawdzanie stacji roboczych i serwerów,
- ✓ centralne zarządzanie spisem licencjonowanego oprogramowania,
- ✓ automatyczne ostrzeganie przed przekroczeniem liczby licencji.

8.9 Administrator systemu informatycznego odpowiada za niezwłoczne usunięcie nielicencjonowanego oprogramowania, a informacja o przypadkach używania nieautoryzowanego oprogramowania jest przedstawiana Dyrektorowi jednostki.

9. Zarządzanie poprawkami technicznymi

9.1 Zarządzanie poprawkami ma na celu eliminowanie lub ograniczanie zidentyfikowanych podatności

- ✓ unikanie wskazywania, która część danych jest poprawna lub niepoprawna w przypadku wystąpienia błędu podczas logowania;
- ✓ ograniczenie liczby nieudanych prób logowania się do systemu do 3, a następnie blokowanie konta po 3 następujących po sobie nieudanych próbach logowania;
- ✓ wykonywanie zapisu każdego nieudanego logowania w logach zdarzeń;
- ✓ ograniczenie możliwości zalogowania się do systemu tylko w określonych przedziałach czasowych („oknach logowania") w godzinach określonych przez Dyrektora GOKSiR i pokrywających się z godzinami pracy placówki;
- ✓ blokowanie wyświetlania hasła w trakcie jego wprowadzania;
- ✓ szyfrowanie przesyłanych haseł.

10.3 Wszyscy użytkownicy systemów muszą posiadać unikalne identyfikatory użytkownika (loginy, identyfikatory ID użytkownika) do swojego wyłącznego użytku.

10.4 Dostęp do systemu dla użytkownika, który trzykrotnie pod rząd podał błędne hasło jest blokowany. Odblokowania dokonuje ręcznie administrator systemu informatycznego na pisemny wniosek Dyrektora GOKSiR.

11. Zarządzanie zmianami w systemach informatycznych

11.1 Kryteria odbioru systemu informatycznego obejmują dostarczenie przez dostawcę:

- ✓ w przypadku oprogramowania - dokumentacji technicznej, instrukcji dla administratora i użytkownika;
- ✓ w przypadku infrastruktury – dokumentacji powykonawczej obejmującej w szczególności schemat połączeń fizycznych i logicznych elementów infrastruktury;

11.2 Ponadto, kryteria odbioru obejmują:

- ✓ sprawdzenie wymagań wydajnościowych i pojemnościowych systemu informatycznego,
- ✓ dokumenty potwierdzające, że instalacja nowych systemów nie będzie miała negatywnego wpływu na dotychczas funkcjonujące systemy, szczególnie w chwilach największego ich obciążenia;
- ✓ dokumenty potwierdzające, że wpływ nowych systemów na bezpieczeństwo informacji, a w szczególności przetwarzanych danych osobowych został uwzględniony;
- ✓ szkolenia z zakresu posługiwania się i działania nowych systemów;

- zmiana infrastruktury awaryjna - stosowana w sytuacjach awaryjnych, gdzie czas implementacji zmiany jest krytyczny, z pominięciem lub uproszczeniem niektórych etapów (np. testów) przy założonym ryzyku,
- zmiana infrastruktury rutynowa - zaakceptowane wcześniej działanie związane z relatywnie prostymi czynnościami np. wymiana drukarki lub monitora.

✓ zmian aplikacyjnych będących poprawkami (w tym usuwanie błędów) albo modyfikacjami, zmiany aplikacyjne są klasyfikowane, jako:

- zmiany aplikacyjne regularne – oznaczają zmiany, które nie wymagają natychmiastowego wdrożenia,
- zmiany aplikacyjne awaryjne – wprowadzane w stanie pilnej konieczności z powodu zagrożenia działania, aplikacji,

11.9 Za proces zarządzania zmianami w poszczególnych obszarach jest odpowiedzialny Dyrektor GOKSiR i administrator systemu informatycznego.

11.10 Każda zmiana regularna jest poprzedzona udokumentowanym:

✓ opisem zmiany;

✓ opisem przyczyny zmiany wraz z podaniem aktów prawnych uzasadniających zmianę;

✓ opisem rodzaju wymaganych działań;

✓ szacowaniem ryzyka potencjalnego wpływu zmian;

✓ wykonaniem kopii zapasowej z możliwością odtworzenia stanu poprzedniego na wypadek nieprzewidzianych zdarzeń;

✓ przetestowaniem zmian.

11.11 Za realizację działań wskazanych w pkt. 11.10 odpowiada Dyrektor wraz z administratorem systemu informatycznego

11.12 Jeżeli zmiana ma charakter awaryjny, dokumentacja, o której mowa w pkt. 11.10 może być opracowana najpóźniej w przeciągu 7 dni od dokonania zmiany.

11.13 Zmiana mająca charakter awaryjny, którą trzeba wprowadzić bezzwłocznie w celu ograniczenia ryzyka poważnego zakłócenia działalności jednostki, wymaga zgody Dyrektora GOKSiR.

12. Bezpieczeństwo dokumentacji systemu

12.1 Dokumentacja powykonawcza infrastruktury oraz dokumentacja techniczna systemów podlegają