Zarządzenie Nr 117 /2021
Wójta Gminy Jedwabno
z dnia 14 grudnia 2021 roku

w sprawie wprowadzenia „Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Gminy w Jedwabnie".

Na podstawie § 20 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2017 r, poz. 2247 z późn.zm.)

zarządza się, co następuje:

§ 1. Wprowadza się „System Zarządzania Bezpieczeństwem Informacji w Urzędzie Gminy w Jedwabnie" stanowiącą załącznik Nr 1 do niniejszego zarządzenia.

§ 2. Zobowiązuje się pracowników Urzędu Gminy Jedwabno do przestrzegania zasad i procedur określonych w dokumentacji, o której mowa w § 1.

§ 3. Zarządzenie wchodzi w życie z dniem podpisania.

Wójt

(Sławomir Ambroziak)

Załącznik Nr 1
do zarządzenia Nr 117/2021
Wójta Gminy Jedwabno
z dnia 14. XII. 2021 r.

Urząd Gminy w Jedwabnie.

System Zarządzania Bezpieczeństwem Informacji.

Zatwierdził:

Data zatwierdzenia:

14.12.2021

System Zarządzania Bezpieczeństwem Informacji powstał w celu realizacji Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r. poz. 2247).

Ochronie podlegają dane, sprzęt komputerowy, systemy operacyjne i informatyczne oraz pomieszczenia, w których odbywa się proces przetwarzania danych. Zamieszczone zapisy mają na celu ochronę danych przed ich udostępnieniem, ujawnieniem, brakiem dostępności, przetwarzaniem danych z naruszeniem przepisów o ochronie danych osobowych, nieuprawnioną zmianą danych, ich utratą, uszkodzeniem lub zniszczeniem.
Dokument stanowi specyfikację zastosowanych technicznych środków zabezpieczających oraz elementów zarządzania systemami informatycznymi przetwarzającymi dane, których uszczegółowienie zawarto w procedurach.

Administrator tworzy w formie tradycyjnej (papierowej) dokument „Dziennik systemów" w którym odnotowywane będą zdarzenia istotne dla działania systemów informatycznych. W przypadku systemów które posiadają specyficzne instrukcje i zalecenia ASI sporządza szczegółowe instrukcje obejmujące działania informatyczne realizowane na tych systemach o ile taka konieczność zachodzi.

1.1. TECHNICZNE ŚRODKI OCHRONY

1.1.1. Środki sprzętowe, informatyczne i telekomunikacyjne:

–serwery danych i programów,
–aktywne urządzenia sieciowe,
–zasilacze awaryjne UPS podtrzymujące zasilanie serwerów, urządzeń sieciowych i routerów,
–zewnętrzne nośniki informacji.

1.1.2. Środki ochrony w ramach oprogramowania systemów:

–na bieżąco aktualizowane oprogramowanie antywirusowe,
–na bieżąco aktualizowane oprogramowanie systemowe oraz aplikacje,
–zabezpieczenia stosowane w serwerach baz danych,
–wykonywanie kopii zabezpieczających,
–identyfikator użytkownika (login), jednoznacznie identyfikujący użytkownika w systemie,
–dostęp do zasobów i modułów systemu ograniczony zakresem nadanych użytkownikowi uprawnień,
–blokowanie ekranu podczas nieobecności użytkownika w sposób uniemożliwiający odblokowanie osobom trzecim (np. wygaszacz ekranu z hasłem).

1.2. FIZYCZNE ŚRODKI OCHRONY

Krytyczne lub wrażliwe środki przetwarzania danych osobowych należy umieszczać w obszarach bezpiecznych, chronionych fizyczną granicą przez odpowiednie bariery bezpieczeństwa oraz zabezpieczenia wejścia.

1.3. ORGANIZACYJNE ŚRODKI OCHRONY

W celu ochrony danych osobowych wykorzystywane są organizacyjne środki zabezpieczające w postaci polityk, instrukcji i procedur stanowiących dokumentację bezpieczeństwa, z którą muszą zapoznać się wszyscy pracownicy i potwierdzić to własnoręcznym podpisem. Innym rodzajem organizacyjnych mechanizmów zabezpieczających są wstępne i okresowe szkolenia, które mają na celu podnoszenie świadomości użytkowników w zakresie zabezpieczania danych osobowych.

2. UDZIELANIE UPRAWNIEŃ I UPOWAŻNIEŃ DO PRZETWARZANIA DANYCH

Dostęp do zasobów informatycznych mają wyłącznie uprawnione osoby zgodnie z zakresem przydzielonego dostępu, wynikającego bezpośrednio z wykonywanych obowiązków.

2.1. PRZYGOTOWANIE STANOWISKA PRACY

Dla każdego użytkownika przygotowywane jest odpowiednie stanowisko komputerowe zgodnie z *Procedurą przygotowania/dostosowania stanowiska komputerowego do eksploatacji*. Ze względu na innego administratora danych osobowych procedura przygotowania stanowiska została również opisana *w Załączniku 19. Procedura przygotowania stanowiska komputerowego przeznaczonego dla Rady Gminy oraz usuwania danych audio*.

2.2. NADAWANIE UPOWAŻNIEŃ DO PRZETWARZANIA DANYCH W SYSTEMACH

Do obsługi systemów informatycznych oraz urządzeń wchodzących w ich skład mogą być dopuszczone wyłącznie osoby posiadające aktualne upoważnienie do przetwarzania danych osobowych.

REJESTROWANIE UPRAWNIEŃ

Dla każdego użytkownika, któremu zostało nadane upoważnienie do przetwarzania danych osobowych ustala się identyfikator. Identyfikator użytkownika nie powinien być zmieniany, a po wyrejestrowaniu użytkownika z systemu nie może być przydzielany innej osobie. Użytkownik otrzymuje indywidualny zakres uprawnień w systemie. W przypadku systemów, w których jest to możliwe ASI ustala hasło inicjujące i przekazuje je użytkownikowi, który jest

zobowiązany do jego zmiany. W pozostałych przypadkach ASI umożliwia wprowadzenie indywidualnego hasła przez użytkownika.

Nadawanie i odbieranie uprawnień zostało szczegółowo opisane w *Procedurze postępowania w zakresie nadawania/odbierania uprawnień do systemów* zawartej w tym dokumencie.

Nadawanie i odwoływanie uprawnień dla osób przetwarzających informacje w systemach zewnętrznych określają zasady i procedury ustalone przez administratora tego systemu.

3. ŚRODKI I METODY UWIERZYTELNIANIA UŻYTKOWNIKÓW

Bezpośredni dostęp do danych osobowych przetwarzanych przy użyciu danej aplikacji, użytkownik może mieć wyłącznie po podaniu danych uwierzytelniających (unikatowego identyfikatora i hasła) właściwych dla danego systemu. Użytkownicy nie mogą korzystać z innych identyfikatorów niż te, które zostały im przydzielone.

Funkcjonujące oprogramowanie zapewnia bezpieczne środowisko pracy, korzystając z wbudowanych funkcji uwierzytelniania, logowania i autoryzacji użytkowników oraz dostępu do sieci i zasobów sieciowych.

Dla celów zabezpieczeń ASI kontroluje dostęp do danych na poziomie obiektu, ustawiając różne poziomy uprawnień lub brak dostępu. Kontrola dostępu określa, w jaki sposób różni użytkownicy mogą korzystać z danych. Wskazane jest wykorzystanie do tego celu specjalistycznego oprogramowania, które w sposób bezsporny przechowywać będzie czas i zakres nadanych uprawnień. W przypadku braku możliwości wykorzystania takiego oprogramowania, należy zachować dane wnioskodawcy oraz szczegóły nadanych uprawnień w formie tradycyjnej. Przykład w formie tradycyjnej zarządzania dostępem regulują: *Procedura postępowania w zakresie nadawania/odbierania uprawnień do systemów informatycznych*, *Procedura blokowania, odblokowywania oraz usuwania kont użytkowników* oraz *Procedura zmiany haseł dla kont użytkowników*.

4. ROZPOCZYNANIE, ZAWIESZANIE I KOŃCZENIE PRACY W SYSTEMIE

Przed wejściem do pomieszczenia przetwarzania użytkownik powinien skontrolować stan pomieszczenia.

Pomieszczenia, w których są przetwarzane dane osobowe muszą znajdować się poza zasięgiem nieograniczonego dostępu.

Po zakończeniu pracy, pomieszczenia w obszarze przetwarzania powinny być zamykane w sposób uniemożliwiający dostęp do nich osób trzecich. Z kluczami do pomieszczeń należy postępować zgodnie z Polityką kluczy. Przed opuszczeniem pomieszczenia dokumenty i nośniki zawierające dane osobowe należy umieścić w zamkniętej szafie. Ostatnia osoba wychodząca danego dnia z pomieszczenia powinna również sprawdzić czy:

–urządzenia elektryczne zostały wyłączone,

–szafy zostały pozamykane na klucz,

–zamknięto okna.

Szczegółowe wytyczne w tym zakresie zawiera *Procedura rozpoczynania, zawieszania i kończenia pracy w systemach informatycznych*, stanowiąca *Załącznik nr 6* niniejszego dokumentu.

5. TWORZENIE KOPII ZAPASOWYCH I NOŚNIKÓW INFORMACJI

Kopie bezpieczeństwa systemów przetwarzających dane podlegające ochronie wykonują się automatycznie. W razie braku takiej możliwości kopię bezpieczeństwa wykonuje ASI.

Kopie bezpieczeństwa należy okresowo sprawdzać pod kątem ich dalszej przydatności do odtworzenia danych w wypadku awarii systemu. Odpowiedzialność za wykonanie tej czynności ponosi ASI.

Zasady postępowania podczas tworzenia kopii zapasowych i awaryjnych zwanych dalej kopiami bezpieczeństwa oraz metody i częstotliwość ich tworzenia określa *Procedura tworzenia kopii zapasowych* stanowiąca Załącznik nr 7 dokumentu.

6. ZARZĄDZANIE NOŚNIKAMI INFORMACJI

Nośniki informacji z danymi podlegającymi ochronie przechowuje się w warunkach uniemożliwiających dostęp do nich osób nieuprawnionych. Pomieszczenia, w których przechowywane są nośniki zawierające dane po zakończeniu pracy zamyka się na klucz. W przypadku uszkodzenia elektronicznego nośnika informacji należy dokonać jego fizycznego zniszczenia. Szczegółowe zasady postępowania z nośnikami informacji określa dokument *Procedura zarządzania nośnikami informacji* stanowiący Załącznik nr 8 dokumentu, *Załączniku nr 16. Procedura usuwania danych z nośników* a także *Załączniku nr 17. Zasady postepowania z pamięciami przenośnymi.*

7. ZŁOŚLIWE OPROGRAMOWANIE

Złośliwe oprogramowanie stanowi ogromne zagrożenie dla informacji gromadzonych w systemach informatycznych. Prawidłowa profilaktyka i świadomość zagrożenia są najważniejszymi sposobami uniknięcia naruszenia bezpieczeństwa informacji. ASI powinien na bieżąco orientować się o występowaniu aktualnych zagrożeń (np. korzystające ze strony https: //www.exploit-db.com). *Załącznik nr 9. Procedura zabezpieczania przed działalnością nieuprawnionego oprogramowania*, *Załącznik nr 20. Procedura usuwania oprogramowania typu Botnet* stanowią załączniki do dokumentu.

8. ZARZĄDZANIE BEZPIECZEŃSTWEM SIECI TELEINFORMATYCZNEJ

W celu ochrony przed zagrożeniami i utrzymania bezpieczeństwa systemu informatycznego, z uwzględnieniem przesyłanych informacji, wdrożono mechanizmy zarządzania i nadzorowania sieci. Za skuteczność zaimplementowanych zabezpieczeń odpowiedzialny jest ASI. Szczegółowe mechanizmy zabezpieczające zostały zdefiniowane w dokumencie *Procedura bezpieczeństwa sieci teleinformatycznych* zawarte w Załączniku nr 10 dokumentu.

9. DOSTĘP DO INTERNETU I POCZTY ELEKTRONICZNEJ

Szczególne znaczenie dla bezpieczeństwa danych ma prawidłowo wykorzystywany dostęp do Internetu i poczty elektronicznej. Należy przestrzegać zasady, iż z Internetu i poczty elektronicznej korzystać można jedynie do celów służbowych.

Procedura korzystania z usługi Internetu i poczty elektronicznej została szczegółowo opisana w Załączniku nr 11 zawartym w dokumencie. W przypadku stosowania certyfikatów (np. SSL) stosuje się *Załącznik nr 21. Instrukcja postępowania z kluczami kryptograficznymi i certyfikatami.*

10. EKSPLOATACJA KOMPUTERÓW PRZENOŚNYCH

W celu zapewnienia bezawaryjnej i bezpiecznej eksploatacji komputerów przenośnych, użytkownicy powinni stosować się do wytycznych zawartych w dokumencie *Procedura bezpiecznej eksploatacji komputerów przenośnych*, która stanowi Załącznik nr 12 dokumentu. Procedura zawiera ogólne zasady dotyczące pracy z komputerem przenośnym, opis zabezpieczeń przy pracy tych urządzeń oraz zalecenia dotyczące bezpiecznej ich eksploatacji. Za bezpieczeństwo komputera przenośnego odpowiedzialny jest jego użytkownik.

11. NARUSZENIE BEZPIECZEŃSTWA INFORMACJI W SYSTEMIE

Naruszenie bezpieczeństwa informacji to wszelkie mogące mieć miejsce zdarzenia lub działania, które stanowią lub mogą stanowić przyczynę naruszenia lub utraty zasobów, utraty poufności, integralności oraz rozliczalności, ograniczenia dostępności informacji lub zmniejszenia niezawodności systemu. Naruszeniem bezpieczeństwa są także odstępstwa od obowiązujących zasad przetwarzania danych osobowych nawet, jeżeli nie prowadzą do wyżej wymienionych skutków. W szczególności są to wszelkie sytuacje, w których nastąpiła utrata (np. kradzież lub zniszczenie), umożliwienie dostępu do danych dla osób nieposiadających upoważnienia do ich przetwarzania lub nieuzasadniona modyfikacja danych lub ich części, nawet jeśli jest możliwe całkowite odtworzenie utraconych danych. W przypadkach naruszenia bezpieczeństwa danych osobowych należy postępować zgodnie z *Procedurą postępowania w przypadku naruszenia bezpieczeństwa danych* a także *Procedurą zgłaszania incydentów informatycznych.*

12. ZABEZPIECZENIA KRYPTOGRAFICZNE

Użytkownicy wykorzystujący do celów służbowych przenośne jednostki robocze oraz nośniki wymienne powinni zwrócić szczególną uwagę na wrażliwość przetwarzanych danych. Jeśli na tego typu urządzeniach przechowywane są dane osobowe, użytkownik powinien zwrócić się do administratora stacji roboczych o umożliwienie dostępu do aplikacji, która pozwala na zaszyfrowanie katalogu z wrażliwymi danymi (szczegółowe informacje zawarto w *Procedurze bezpiecznej eksploatacji komputerów przenośnych* stanowiącej Załącznik nr 12, *Procedurze zarządzania nośnikami informacji* stanowiącej Załącznik nr 8 oraz *Załącznik nr 21. Instrukcja postępowania z kluczami kryptograficznymi i certyfikatami.*

13. PRZEGLĄDY, KONSERWACJE I NAPRAWY

Urządzenia oraz oprogramowanie podlegają okresowym przeglądom i konserwacjom zgodnie z zaleceniami ich producentów oraz bieżącymi potrzebami. Przeglądu dokonuje się także za każdym razem, gdy zostanie stwierdzone naruszenie bezpieczeństwa informacji.

Za dokonywanie przeglądów i konserwacji urządzeń oraz oprogramowania są odpowiedzialni wyznaczeni pracownicy lub ASI. Usługi serwisowe (techniczne i programowe) świadczą wyłącznie autoryzowane i uprawnione jednostki serwisowe.

Dokonywanie przeglądów i konserwacji urządzeń oraz oprogramowania odbywa się zgodnie z dokumentem *Procedura wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych* stanowiącym Załącznik nr 13. W przypadku konieczności dokonania naprawy poza siedzibą należy postępować zgodnie z dokumentem *Procedura przekazania poza obszar przetwarzania (do serwisu lub naprawy) urządzeń i nośników zawierających dane chronione* stanowiącym Załącznik nr 14.

14. ANONIMIZACJA, PSEUDONIMIZACJĘ ORAZ SZYFROWANIE.

Niniejsza procedura określa techniki zabezpieczenia danych osobowych, tj.: animizację, pseudonimizację, szyfrowanie. Stosowanie wyżej wymienionych technik ma na celu minimalizację ryzyka wynikającego z udostępniania danych osobowych procesorom lub współadministratorom. Procedura ma na celu zapewnienie podniesienia poziomu ochrony danych osobowych zgodnie z zasadą privacy by design a także odgrywa istotną rolę we wdrożeniu strategii minimalizacji danych a także przyczynia się do obniżenia potencjalnie negatywnych skutków dla podmiotów danych w przypadku wystąpienia naruszenia bezpieczeństwa. Administrator jest odpowiedzialny za ochronę danych osobowych, ustala cele i środki ich przetwarzania oraz decyduje o wyborze środków bezpieczeństwa, np.: poprzez zastosowanie anonimizacji, pseudonimizacji lub szyfrowania, ponosi odpowiedzialność za dobór standardów anonimizacji, pseudonimizacji i szyfrowania oraz

wdraża środki oraz utrzymuje narzędzia gwarantujące anonimizację, pseudonimizację oraz szyfrowanie danych osobowych.

15. OCHRONA DANYCH W FAZIE PROJEKTOWANIA.

Zadania przypisane poszczególnym osobom omówione są w *Załączniku 22. Instrukcja uwzględniania ochrony danych w fazie projektowania oraz domyślna ochrona danych.*

ZAŁĄCZNIKI – WYKAZ PROCEDUR

Lp.	Nazwa Procedury	Zakres Procedury	Adresaci
Załącznik nr 1	Procedura przygotowania/dostosowania stanowiska komputerowego.	Dokument opisuje zasady przygotowania/dostosowania stanowiska komputerowego do eksploatacji.	ASI, użytkownicy stanowisk komputerowych.
Załącznik nr 2	Procedura nadawania uprawnień.	Dokument opisuje zasady postępowania w zakresie nadawania/odbierania uprawnień do systemów informatycznych.	ASI, Użytkownicy stanowisk komputerowych.
Załącznik nr 3	Procedura blokowania, odblokowywania oraz usuwania kont użytkowników.	Dokument opisuje zasady blokowania, odblokowywania oraz usuwania kont użytkowników.	ASI.
Załącznik nr 4	Procedura zmiany hasła.	Dokument opisuje zasady zmiany haseł dla kont użytkowników.	Użytkownicy stanowisk komputerowych, ASI.
Załącznik nr 5	Procedura uwierzytelniania.	Dokument opisuje zasady uwierzytelniania użytkowników, tworzenia unikatowych haseł i ich ochrony.	ASI, Użytkownicy stanowisk komputerowych.
Załącznik nr 6	Procedura rozpoczynania, zawieszania i kończenia pracy w systemach informatycznych.	Dokument opisuje zasady rozpoczynania, zawieszania i kończenia pracy w systemie informatycznym.	Użytkownicy.
Załącznik nr 7	Procedura tworzenia kopii.	Dokument opisuje zasady tworzenia kopii zapasowych.	ASI.
Załącznik nr 8	Procedura zarządzania nośnikami.	Dokument opisuje zasady zarządzania nośnikami informacji.	Użytkownicy stanowisk komputerowych, ASI.
Załącznik nr 9	Procedura zabezpieczania przed nieuprawnionym oprogramowaniem.	Dokument opisuje zasady zabezpieczenia przed działalnością nieuprawnionego oprogramowania.	ASI, wszyscy użytkownicy systemów.
Załącznik nr 10	Procedura bezpieczeństwa sieci teleinformatycznej.	Dokument opisuje zasady bezpieczeństwa sieci teleinformatycznych.	ASI, Użytkownicy,
Załącznik nr 11	Procedura korzystania z usługi Internetu i poczty elektronicznej.	Dokument opisuje zasady korzystania z usług Internetu i poczty elektronicznej.	użytkownicy, ASI.
Załącznik nr 12	Procedura bezpiecznej eksploatacji komputerów przenośnych.	Dokument opisuje zasady bezpiecznej eksploatacji komputerów przenośnych.	Wszyscy użytkownicy komputerów przenośnych, ASI.
Załącznik nr 13	Procedura wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.	Dokument opisuje zasady wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.	ASI, Pracownicy;
Załącznik nr 14	Procedura przekazywania urządzeń i nośników poza obszar przetwarzania (do serwisu lub naprawy).	Dokument opisuje zasady przekazywania urządzeń i nośników zawierające dane chronione poza obszar przetwarzania.	ASI, pracownicy, użytkownicy;
Załącznik nr 15	Anonimizacja, pseudonimizacja oraz szyfrowanie.	Dokument opisuje zasady, sposoby oraz cel stosowania.	ASI, pracownicy
Załącznik nr 16	Procedura usuwania danych z nośników	Dokument opisuje zasady, sposoby oraz cel stosowania.	
Załącznik nr 17	Zasady postępowania z pamięciami przenośnymi.	Dokument opisuje zasady, metody uzyskania nośnika oraz odpowiedzialności.	ASI, pracownicy
Załącznik nr 18	Procedura zgłaszania incydentów informatycznych	Dokument opisuje zasady oraz odpowiedzialności	ASI, osoba upoważniona
Załącznik nr 19	Instrukcja uwzględniania ochrony danych w fazie projektowania oraz domyślna ochrona danych.	Dokument opisuje zasady oraz odpowiedzialności	ASI, pracownik
Załącznik nr 20	Procedura usuwania oprogramowania typu BOTNET	Dokument opisuje przykładowe metody oraz odpowiedzialności	ASI
Załącznik nr 21	Instrukcja postępowania z kluczami kryptograficznymi oraz certyfikatami.	Dokument opisuje zasady oraz odpowiedzialności	ASI, pracownicy
Załącznik nr 22	Instrukcja uwzględniania ochrony danych w fazie projektowania oraz domyślna ochrona danych.	Dokument opisuje zasady oraz odpowiedzialności	ASI, Kadra kierownicza.

Załącznik nr 1. Procedura przygotowania stanowiska pracy

CEL PROCEDURY

Celem procedury jest określenie zasad przygotowania/dostosowania stanowiska komputerowego do eksploatacji, a także wskazanie szczegółowych parametrów standardowego wyposażenia użytkownika w zakresie zasobów informatycznych. Czynności związane z nadawaniem/cofaniem uprawnień do poszczególnych systemów użytkowych reguluje odrębny dokument – *Procedura postępowania w zakresie nadawania/odbierania uprawnień do systemów informatycznych.*

ODPOWIEDZIALNOŚĆ

Za przestrzeganie zasad wymienionych w niniejszej procedurze odpowiadają:

a. Administrator Systemów Informatycznych – odpowiada za prawidłowe przygotowanie/dostosowanie stanowiska komputerowego do eksploatacji;

b. Wszyscy pracownicy korzystający ze stanowisk komputerowych, z uwzględnieniem praktykantów, stażystów oraz pracowników zleceniowych i każdej innej formy współpracy.

ZAKRES I WARUNKI STOSOWANIA

Procedura ma charakter ogólny i dotyczy przygotowania oraz modyfikowania wszystkich funkcjonujących stanowisk komputerowych. Wymagania podane w dokumencie spełniają zalecenia zawarte w normie PN-ISO/IEC 27001 w zakresie wskazanym w punkcie 6.1, 6.2, 7.2, 8.1, 11.2,12.1, 12.2, 12.4.

POSTANOWIENIA OGÓLNE

–Każdy użytkownik stanowiska komputerowego powinien posiadać własne konto bez uprawnień administracyjnych, na którym może pracować z zachowaniem rozliczalności działań podejmowanych w systemie.

–Użytkownikowi nie wolno ingerować w konfigurację sprzętową stacji roboczej.

–Użytkownikowi nie wolno samodzielnie instalować na stacji roboczej oprogramowania (w tym dodatków do przeglądarek), ani używać aplikacji w wersji portable (programów nie wymagających instalacji, przenoszonych na różnych nośnikach pamięci).

TREŚĆ PROCEDURY

PRZYGOTOWANIE STANOWISKA KOMPUTEROWEGO

Nowe stanowisko komputerowe jest przygotowywane przez administratora stacji roboczych na podstawie informacji z o zatrudnieniu.

–Administrator stacji roboczych przygotowuje stanowisko komputerowe do pracy i przekazuje informację o zakończeniu zadania.

–W razie potrzeby administrator stacji roboczych przeprowadza szkolenie stanowiskowe (wskazuje materiały przydatne do prawidłowej eksploatacji stacji roboczej).

DOSTOSOWANIE STANOWISKA KOMPUTEROWEGO

–W przypadku potrzeby wprowadzenia modyfikacji zakres modyfikacji określa ASI.

–Pozostałe czynności przebiegają analogicznie, jak w przypadku przygotowania nowego stanowiska pracy.

–W niektórych przypadkach konieczne jest wykonanie dodatkowych czynności w celu dostosowania stacji roboczej do eksploatacji. Wnioskowana modyfikacja może bowiem wiązać się z koniecznością nadania nowych uprawnień, zmianą zakresu upoważnienia, dodatkowym zakupem sprzętu, oprogramowania lub innych zasobów informatycznych.

□ Administrator Systemów Informatycznych konfiguruje stanowisko komputerowe zgodnie z następującymi zasadami:

- Wszystkie operacje dostępu do zasobów pracownika muszą być wykonywane za jego wiedzą i zgodą, dotyczy to również podłączenia zdalnego.
- Stosuje się zasadę, że wszystkie logi komputera administrator przechowuje przez okres minimum 2 lat.

Logi systemowe muszą zachowywać co najmniej następujące informacje: uruchomienie i wyłączenie komputera, zalogowanie i wylogowanie użytkownika, podłączanie zewnętrznych nośników informacji, wszystkie aspekty zdalnego podłączenia do komputera, kopiowanie lub próby kopiowania zbiorów, usuwanie lub próby usuwania zbiorów. Konieczne jest włączenie: inspekcji użycia uprawnień, inspekcji zarządzania kontami, inspekcji dostępu do obiektów, inspekcji zmian zasad, konto gościa musi być wyłączone, wyłączona jest możliwość zmiany nazwy konta gościa i administratora, włączona opcja „wyczyść plik stronicowania pamięci wirtualnej".

- W przypadku zastosowania przenośnej jednostki komputerowej obowiązuje obowiązek szyfrowania partycji dyskowych np. z wykorzystaniem BitLockera. Kopię hasła szyfrowania ASI przekazuje Administratorowi Danych. Fakt przekazania hasła ASI dokumentuje w dzienniku systemu.
- Administrator Danych przechowuje także aktualną kopię hasła administratora komputera, którą otrzymuje od ASI po każdej zmianie. Administrator Danych może podjąć decyzję o przechowywaniu hasła przez inną osobę. Fakt przekazania hasła ASI dokumentuje w dzienniku systemu. Zasady tworzenia haseł, przechowywania i niszczenia określa procedura „Zasady tworzenia haseł administratorów".

STANDARDOWE WYPOSAŻENIE STANOWISKA KOMPUTEROWEGO

Nowy użytkownik stacji roboczej zostaje wyposażony w standardowy sprzęt i oprogramowanie.

SPRZĘT

–Jednostka centralna z monitorem lub urządzenie typu All in one;

–Klawiatura;

–Mysz.

OPROGRAMOWANIE (minimalne)

–System operacyjny – zaktualizowany system operacyjny z rodziny MS Windows w wersji PRO;

–Open Office lub MS Office –stabilna i wspierana wersja oprogramowania;

–Przeglądarka internetowa – np. Microsoft Edge i/lub alternatywna przeglądarka;

–Przeglądarka plików pdf – np. Adobe Reader;

–Kompresor plików – np. 7 Zip;

–Oprogramowanie antywirusowe;

–Podłączenie drukarek – zainstalowanie drukarek (podstawowej i alternatywnej) umożliwiające użytkownikowi wydrukowanie dokumentów;

–Inne aplikacje niezbędne do wykonywania obowiązków.

Administrator stacji roboczych umożliwia nowemu użytkownikowi korzystanie ze skonfigurowanej stacji roboczej. W celu uzyskania dostępu do pozostałych zasobów informatycznych (indywidualny dostęp do systemu operacyjnego, poczty elektronicznej, Internetu, wybranych aplikacji użytkowych) należy zastosować *Procedurę postępowania w zakresie nadawania/odbierania uprawnień do systemów informatycznych.*

DOKUMENTOWANIE ZLECEŃ WYKONANIA ZADANIA

Zleceniodawca przekazuje administratorowi otrzymaną informację o zatrudnieniu lub informację o dostosowanie stanowiska komputerowego do eksploatacji.

ASI ewidencjonuje w wybranej formie elektronicznej (np. podkatalog w ramach służbowego konta pocztowego) przekazane informacje, które stanowią podstawę zlecenia przygotowania/dostosowania stanowiska komputerowego do eksploatacji.

CZAS REALIZACJI ZADANIA

Stanowisko komputerowe powinno zostać przygotowane/dostosowane do eksploatacji w możliwie najkrótszym czasie. Działanie powinno być udokumentowane.

Załącznik 1. Protokół konfiguracji stacji roboczej oraz przeszkolenia pracownika.

W dniu ..... w Urzędzie Gminy w Jedwabnie Administrator Systemów Informatycznych przekazał do eksploatacji stację roboczą (nr inwentarzowy .....). Jednostka komputerowa została skonfigurowana do pracy .

.....

(data, imię i nazwisko)

W dniu ..... W Urzędzie Gminy w Jedwabnie Administrator Systemów Informatycznych przeszkolił .....
(imię i nazwisko)
do pracy na stacji roboczej.
Szkolenie zawierało następujące elementy:
- bezpieczne posługiwanie się komputerem,
- zasady tworzenia haseł,
- zasady korzystania z zewnętrznych nośników informacji,
- obsługa aplikacji: .....
.....

Szkolenie trwało: .....

.....

Załącznik nr 2. Procedura nadawania odbierania uprawnień.

CEL PROCEDURY

Celem procedury jest określenie sposobu postępowania w zakresie nadawania i odbierania uprawnień do eksploatowanych systemów informatycznych.

ODPOWIEDZIALNOŚĆ

Za przestrzeganie zasad wymienionych w niniejszej procedurze odpowiadają:

a. ADO/Kierownicy Komórek Organizacyjnych - weryfikuje i zatwierdza wnioski o nadanie/odebranie uprawnień;

b. Administrator Systemów Informatycznych – odpowiada za nadanie/odebranie uprawnień w systemie;

c. Wszyscy pracownicy, których zadania są związane z nadawanymi/odbieranymi uprawnieniami, z uwzględnieniem praktykantów, stażystów oraz pracowników zleceniowych i każdej innej formy współpracy wymagającej dostępu do danych osobowych.

Zadania przypisane w niniejszej procedurze może wykonywać wyznaczony pracownik, upoważniony przez bezpośredniego przełożonego.

ZAKRES I WARUNKI STOSOWANIA

Procedurę stosuje się w odniesieniu do wszelkich czynności związanych z nadawaniem i odbieraniem uprawnień do systemów informatycznych. Wszystkie osoby przetwarzające dane osobowe w formie elektronicznej powinny posiadać aktualne uprawnienia w zakresie niezbędnym do wykonywania obowiązków służbowych – wymóg ten dotyczy także osób odbywających staż, praktyki studenckie oraz pracowników zatrudnionych na umowę zlecenie, w tym przypadku zakres uprawnień definiowany jest odpowiednio z wykorzystaniem umowy o staż, umowy o praktykę studencką lub umowy zlecenia. Wymagania podane w dokumencie spełniają zalecenia zawarte w normie PN-ISO/IEC 27001 w zakresie wskazanym w punkcie 9.1, 9.2, 9.3, 9.4

POSTANOWIENIA OGÓLNE

TREŚĆ PROCEDURY

NADAWANIE UPRAWNIEŃ

- Wyznaczona osoba uzupełnia wniosek o nadanie uprawnień z zakresem upoważnienia do przetwarzania danych osobowych, w przypadku braku nieprawidłowości zatwierdza wniosek o nadanie uprawnień, a następnie przekazuje go ASI. W sytuacji stwierdzenia niezgodności wyznaczona osoba wyjaśnia i ustala przyczyny rozbieżności.

–ASI zakłada konto i nadaje pracownikowi uprawnienia do systemu użytkowego.

–ASI przekazuje informację o nadaniu uprawnień do użytkownika oraz osoby zatwierdzającej wniosek.

–W przypadku systemów, w których jest to możliwe ASI ustala hasło inicjujące i przekazuje je użytkownikowi, który jest zobowiązany do jego zmiany. W pozostałych przypadkach ASI umożliwia wprowadzenie indywidualnego hasła przez użytkownika.

–ASI potwierdza na wniosku wykonanie zmian zgodnych z żądaniem.

–Wnioski o nadanie uprawnień są przechowywane odpowiednio przez wyznaczonego pracownika (punkt 7 niniejszej procedury). Mogą być przechowywane w formie elektronicznej, wtedy zasady prowadzenia dokumentacji papierowej nie obowiązują a dokumentacja elektroniczna zawiera co najmniej tyle informacji co tradycyjna.

–W razie potrzeby ASI przeprowadza szkolenie stanowiskowe – wskazuje dokumentację i inne materiały przydatne do prawidłowej obsługi systemu oraz pomaga w rozwiązywaniu problemów technicznych.

W przypadku zastosowania specjalistycznego oprogramowania weryfikującego uprawnienia w systemach, sposób wnioskowania, nadawania i odbierania tych uprawnień powinien zostać dostosowany tego programu, z zachowaniem zasady weryfikacji oraz historii nadawania, odbierania czy modyfikacji uprawnień.

ODBIERANIE UPRAWNIEŃ

–Wyznaczony pracownik/właściciel przekazuje do ASI wniosek o odebranie uprawnień dla danego pracownika (zgodnie ze wzorem – stanowiącym Załącznik nr 2 do niniejszej procedury) lub drogą elektroniczną.

–ASI odbiera wszystkie uprawnienia nadane użytkownikowi, w tym blokuje możliwość dostępu do systemu operacyjnego lub domeny, Internetu i poczty elektronicznej i baz danych.

–ASI przekazuje informację o odebraniu uprawnień do wyznaczonej osoby.

–ASI potwierdza na wniosku wykonanie zmian zgodnych z żądaniem.

–Wnioski o odebranie uprawnień są przechowywane przez wyznaczonego pracownika. Mogą być przechowywane w formie elektronicznej, wtedy zasady prowadzenia dokumentacji papierowej nie obowiązują a dokumentacja elektroniczna zawiera co najmniej tyle informacji co tradycyjna.

MODYFIKOWANIE UPRAWNIEŃ

–Występując o modyfikację, we wniosku należy wskazać wszystkie uprawnienia, jakie powinien posiadać pracownik, bez względu na to, czy zostały już przydzielone wcześniejszym wnioskiem. Uprawnienia, które pracownik wcześniej posiadał, a nie są ujęte w nowym wniosku, zostają odebrane. Nie dotyczy to uprawnień do systemu operacyjnego lub domeny, Internetu

i poczty elektronicznej, które są anulowane tylko w przypadku wpłynięcia wniosku o odebranie uprawnień (Załącznik nr 2 do niniejszej procedury).

–W przypadku przesłania nowego wniosku o nadanie uprawnień nie ma potrzeby przesyłania wniosku o odebranie uprawnień. Pojawienie się nowego wniosku o nadanie uprawnień jest równoznaczne z końcem ważności poprzedniego wniosku.

–wyznaczona osoba niezwłocznie weryfikuje i zatwierdza wniosek o nadanie uprawnień, a następnie przekazuje go do ASI, w celu modyfikacji uprawnień.

–ASI wprowadza modyfikacje w zakresie uprawnień do systemów informatycznych zgodnie z wnioskiem zatwierdzonym przez wyznaczoną osobę.

–ASI potwierdza na wniosku wykonanie zmian zgodnych z żądaniem.

–ASI przekazuje informację o nadaniu uprawnień do użytkownika.

–Wnioski o nadanie uprawnień dla wszystkich użytkowników są przechowywane przez wyznaczonego pracownika. Mogą być przechowywane w formie elektronicznej, wtedy zasady prowadzenia dokumentacji papierowej nie obowiązują a dokumentacja elektroniczna zawiera co najmniej tyle informacji co tradycyjna.

PRZECHOWYWANIE WNIOSKÓW O NADANIE/ODEBRANIE UPRAWNIEŃ

Wyznaczony pracownik prowadzi segregator, w którym w kolejności alfabetycznej, przechowywane są wszystkie złożone dotąd wnioski o nadanie/odebranie uprawnień. W prawym górnym rogu dokumentów, które straciły ważność (zastąpiono je nowym wnioskiem lub złożony był wniosek o odwołanie uprawnień) powinien widnieć napis *NIEAKTUALNY od [data nowego wniosku o nadanie/odebranie uprawnień]*. Dla każdego pracownika jako pierwsze powinny być ułożone dokumenty aktualnie obowiązujące. W przypadku korzystania z formy elektronicznej wniosku, forma papierowa nie jest obligatoryjna.

Wyznaczony pracownik prowadzi też segregator dla osób, których umowa o pracę wygasła lub została rozwiązana. W przypadku przywrócenia takiej osoby do pracy, należy przenieść dokumenty do segregatora osób aktualnie zatrudnionych. Wyznaczony pracownik prowadzi ewidencję aktualnie nadanych uprawnień. Wnioski mogą być przechowywane w formie elektronicznej, wtedy zasady prowadzenia dokumentacji papierowej nie obowiązują a dokumentacja elektroniczna zawiera co najmniej tyle informacji co tradycyjna.

PRZEGLĄD UPRAWNIEŃ UŻYTKOWNIKÓW

Zleca przegląd ewidencji nadanych uprawnień, w celu określenia ich aktualności i kompletności. Jeśli w trakcie przeglądu zostaną ujawnione jakiekolwiek nieścisłości, przyczyny zaistniałych zdarzeń są wyjaśniane. Dodatkowo przeprowadza się przegląd uprawnień, nadanych pracownikom.

CZAS REALIZACJI ZADANIA

Uprawnienia powinny zostać nadane/odebrane niezwłocznie po wpłynięciu wniosku. Wszelkie problemy uniemożliwiające wykonanie zadania we wskazanym czasie powinny być zgłaszane ADO.

ZAŁĄCZNIKI

Załącznik 1 -Wzór „Wniosek o nadanie uprawnień"

Załącznik 2 -Wzór „Wniosek o odebranie uprawnień"

Załącznik nr 1

WNIOSEK O NADANIE UPRAWNIEŃ DO SYSTEMÓW INFORMATYCZNYCH

Wnioskodawca

Nazwisko i imię osoby: .....

Stanowisko: .....

Dane użytkownika

Nazwisko i imię: .....

Stanowisko: .....

Numer pomieszczenia przetwarzania danych: .....

Nr telefonu: .....

Adres e-mail: .....

Informacje o systemie, danych i wnioskowanych uprawnieniach

Nazwa systemu	Zakres uprawnień (wg kolumny Rodzaj uprawnienia

.....

Data, podpis

Informacje o komputerze, z którego będą wykonywane połączenia do systemu informatycznego

Numer IP komputera lub Nazwa komputera	
Identyfikator użytkownika	
E-mail:	

Informacja o przydzielonych identyfikatorach do systemów informatycznych (wypełnia ASI)

Nazwa systemu	Identyfikator (login)

Potwierdzenie nadania wnioskowanych uprawnień (wypełnia ASI)

Nazwa systemu	Data i podpis ASI

.....

Data, podpis ASI

.....

Data, podpis osoby otrzymującej uprawnienia

Załącznik nr 2

WNIOSEK O ODEBRANIE UPRAWNIEŃ DO SYSTEMÓW INFORMATYCZNYCH

Wnioskodawca

Nazwisko i imię	
Uwagi	

Dane użytkownika

Imię i Nazwisko	
Stanowisko	
Telefon:	E-Mail:

Informacje o systemie i wycofanych uprawnieniach

Nazwa systemu	
Wycofane uprawnienia	

.....

Data, podpis

Potwierdzenie odebrania uprawnień
(wypełnia ASI)

Nazwa systemu	Data i podpis ASI

Załącznik nr 3. Procedura blokowania, odblokowania i usuwania kont użytkowników.

CEL PROCEDURY

Celem procedury jest określenie zasad blokowania, odblokowywania oraz usuwania kont użytkowników w przypadku ustania stosunku pracy lub absencji pracownika dłuższej niż trzy miesiące.

ZAKRES I WARUNKI STOSOWANIA.

Procedura przeznaczona jest dla wszystkich kont użytkowników domenowych, kont użytkowników do systemu operacyjnego i kont użytkowników do aplikacji użytkowych. Wymagania podane w dokumencie spełniają zalecenia zawarte w normie PN-ISO/IEC 27001 w zakresie wskazanym w punkcie 9.

TREŚĆ PROCEDURY

ZAKOŃCZENIE ZATRUDNIENIA

- Po otrzymaniu informacji o ustaniu stosunku pracy, konto użytkownika zostaje zablokowane przez ASI.
- Zablokowanie następuje w dniu ustania stosunku pracy.
- Informacja dotycząca zablokowania konta jest przekazywana przez ASI do bezpośredniego przełożonego pracownika.
- Po zablokowaniu konta użytkownika administrator systemu informatycznego wykonuje kopię danych użytkownika, która w niektórych przypadkach podlega archiwizacji. Okres archiwizacji zawartości konta zależy od aktualnej polityki firmy. W przypadku stosowania mechanizmu archiwizacji, pracownik jest informowany o czasie przechowywania danych.
- Po wykonaniu kopii, o której mowa w poprzednim podpunkcie, administrator systemu informatycznego usuwa profil użytkownika oraz dokumenty zapisane lokalnie przez tego użytkownika w okresie zatrudnienia.
- Informacja dotycząca usunięcia konta jest przekazywana przez administratora systemu informatycznego do bezpośredniego przełożonego pracownika.

ABSENCJA DŁUŻSZA NIŻ 3 MIESIĄCE

- Po otrzymaniu informacji o absencji pracownika trwającej dłużej niż trzy miesiące, konto użytkownika dla tej osoby jest blokowane przez administratora systemu informatycznego.
- W momencie powrotu do pracy pracownika, bezpośredni przełożony pracownika składa wniosek o odblokowanie odpowiedniego konta.
- Złożony wniosek trafia do ASI, który wprowadza niezbędne modyfikacje w systemie, co potwierdza podpisem na wniosku.
- Informacja dotycząca odblokowania konta jest przekazywana drogą mailową przez administratora systemu informatycznego do składającego wniosek.

- ASI prowadzi segregator z wnioskami o odblokowanie konta użytkownika. Wzór wniosku o odblokowanie konta użytkownika stanowi załącznik nr 1 do niniejszej procedury lub przechowuje wnioski w formie elektronicznej.
- Administrator systemu informatycznego prowadzi dokumentację w zakresie blokowania, odblokowywania oraz usuwania kont użytkowników, której wzór stanowi załącznik nr 2 do niniejszej procedury. Wnioski mogą być przechowywane w formie elektronicznej, wtedy zasady prowadzenia dokumentacji papierowej nie obowiązują a dokumentacja elektroniczna zawiera co najmniej tyle informacji, co tradycyjna.

ZAŁĄCZNIKI

Załącznik 1 -Wzór „Wniosek o odblokowanie konta użytkownika"

Załącznik nr 1

WNIOSEK O ODBLOKOWANIE KONTA UŻYTKOWNIKA

Wnioskodawca

Stanowisko	
Nazwisko i imię osoby	

Dane użytkownika

Nazwisko i imię	
Stanowisko	
Telefon	

Uzasadnienie:

.....

.....

.....

.....

Data, podpis osoby kierującej komórką

Informacje o komputerze użytkownika

Numer komputera, z którego będzie następowało połączenie	
Identyfikator użytkownika	
E-mail:	

Potwierdzenie odblokowania konta użytkownika

.....

Data, podpis ASI

Załącznik nr 4. Procedura zmiany hasła.

CEL PROCEDURY

Celem procedury jest określenie czynności, które należy wykonać w przypadku konieczności odblokowania lub zmiany hasła do konta użytkownika domenowego, konta użytkownika do systemu operacyjnego lub konta użytkownika do aplikacji użytkowej.

ODPOWIEDZIALNOŚĆ

Za przestrzeganie zasad wymienionych w niniejszej procedurze odpowiadają:

a. użytkownicy korzystający z kont domenowych, kont do systemu operacyjnego lub kont do aplikacji użytkowych,

b. administrator systemu informatycznego.

ZAKRES I WARUNKI STOSOWANIA

Dokument stosuje się w razie konieczności odblokowania lub zmiany hasła do konta użytkownika domenowego, konta użytkownika do systemu operacyjnego lub konta użytkownika do aplikacji użytkowej. Jeśli konto użytkownika zostało zablokowane w wyniku absencji pracownika trwającej dłużej niż 3 miesiące, w celu odblokowania dostępu należy stosować *Procedurę blokowania, odblokowywania oraz usuwania kont użytkowników* – Załącznik nr 3. Wymagania podane w dokumencie spełniają zalecenia zawarte w normie PN-ISO/IEC 27001 w zakresie wskazanym w punkcie 9.

Hasło jest zmieniane w przypadku:

- upłynięcia terminu ważności poprzedniego hasła,
- zablokowania konta w przypadku wielokrotnego wprowadzenia błędnego hasła,
- niezwłocznie po nadaniu hasła inicjującego przez administratora systemu informatycznego,
- niezwłocznie w przypadku ujawnienia hasła lub podejrzenia, że hasło zostało skompromitowane.

TREŚĆ PROCEDURY

ODBLOKOWANIE KONTA UŻYTKOWNIKA BEZ ZMIANY HASŁA

- W przypadku braku możliwości zalogowania się na konto użytkownika i/lub otrzymania komunikatu o zablokowaniu konta, użytkownik powinien skontaktować się z ASI.
- Administrator odblokowuje konto przyporządkowane podanemu przez użytkownika identyfikatorowi konta użytkownika.
- Podczas rozmowy z ASI użytkownik powinien zalogować się z wykorzystaniem identyfikatora konta użytkownika i dotychczas używanego hasła.

Zablokowane przez trzykrotne błędne wprowadzenie hasła konto użytkownika zostanie automatycznie odblokowane po min. 15 minutach bez potrzeby zgłaszania tego faktu.

ODBLOKOWANIE KONTA UŻYTKOWNIKA ZE ZMIANĄ HASŁA

–W przypadku zablokowania konta użytkownika istnieje możliwość zmiany hasła na nowe.

–Administrator ustala hasło inicjujące dla wskazanego w zgłoszeniu identyfikatora i przekazuje je użytkownikowi.

–W trakcie pierwszego logowania po odblokowaniu konta, użytkownik zmienia hasło inicjujące na unikatowe, zgodne z wytycznymi zawartymi w *Procedurze uwierzytelniania użytkowników, tworzenia unikatowych haseł i ich ochrony.*

Załącznik nr 5. Procedura uwierzytelniania

CEL PROCEDURY

Celem procedury jest określenie zasad przydzielania oraz przekazywania użytkownikom identyfikatorów i haseł. Procedura zawiera zasady konstrukcji haseł, tryb i częstotliwość ich zmian oraz metody ich ochrony.

ODPOWIEDZIALNOŚĆ

Za przestrzeganie zasad wymienionych w niniejszej procedurze odpowiadają:

a. Wszyscy użytkownicy systemów,
b. Administrator Systemów Informatycznych,
c. Administrator Danych

ZAKRES I WARUNKI STOSOWANIA

Procedura przeznaczona jest dla wszystkich osób, które zobowiązane są do przestrzegania zasad zawartych w dokumentacji bezpieczeństwa informacji. Procedura ma zastosowanie do wszystkich systemów informatycznych, które przetwarzają dane osobowe. Wymagania podane w dokumencie spełniają zalecenia zawarte w normie PN-ISO/IEC 27001 w zakresie wskazanym w punkcie 9.

TREŚĆ PROCEDURY

ZASADY PRZYDZIELANIA IDENTYFIKATORÓW I HASEŁ

–Każdy użytkownik otrzymuje unikatowy identyfikator do swojego osobistego i wyłącznego użytku, który jednoznacznie wskazuje na osobę dokonującą uwierzytelnienia w systemie. W ten sposób każde działanie w systemie może zostać przypisane konkretnej osobie, która jest za nie odpowiedzialna. Identyfikator po ustaniu zatrudnienia nie jest usuwany z systemu i nie może być przyznany innej osobie.
–Identyfikator jest ciągiem znaków, tworzonym według ściśle określonej konwencji, jednolitej dla całej organizacji.
–Identyfikator w systemie nadaje ASI zarządzający uprawnieniami użytkowników.
–W przypadku systemów, w których jest to możliwe ASI ustala hasło inicjujące i przekazuje je użytkownikowi. W pozostałych przypadkach ASI umożliwia wprowadzenie indywidualnego hasła przez użytkownika.
–Hasło inicjujące podlega obowiązkowej zmianie przez użytkownika przy pierwszym logowaniu do systemu na hasło znane jedynie właścicielowi. Zmiana hasła powinna nastąpić niezwłocznie po podaniu hasła inicjującego przez ASI.
–Hasło (z wyjątkiem inicjującego pracę w systemie) ustala dla siebie wyłącznie użytkownik i zachowuje je w tajemnicy.
–Hasło użytkownika musi być zmieniane nie rzadziej niż co 90 dni, niezależnie od tego czy system komputerowy wymusza zmianę, czy też nie.
–Użytkownik odpowiada za systematyczną zmianę swoich haseł dostępu.

UWIERZYTELNIENIE UŻYTKOWNIKA W SYSTEMIE

- Bezpośredni dostęp do danych chronionych przetwarzanych w systemie informatycznym użytkownik może uzyskać wyłącznie po dokonaniu uwierzytelnienia w systemie.
- Uwierzytelnienie następuje po podaniu identyfikatora oraz właściwego hasła (logowanie do systemu).
- Po poprawnym uwierzytelnieniu, użytkownik może wykonywać wszystkie czynności, na jakie pozwalają przydzielone mu prawa dostępu.

INDYWIDUALNE HASŁO DOSTĘPU DO SYSTEMU OPERACYJNEGO LUB HASŁO DOMENOWE

Użytkownik systemu informatycznego, aby uzyskać dostęp do obsługiwanej przez siebie aplikacji, w pierwszej kolejności podaje identyfikator i hasło.

Oprogramowanie wymusza wybór przez użytkownika haseł odpowiedniej jakości. Długość nie może być mniejsza niż 8 znaków, a hasło musi spełniać przynajmniej trzy z następujących wymagań:

- zawierać małe litery alfabetu łacińskiego,
- zawierać duże litery alfabetu łacińskiego,
- zawierać cyfry systemu dziesiętnego (od 0 do 9),
- zawierać znaki specjalne (niealfabetyczne).

Oprogramowanie systemowe powinno być tak skonfigurowane, aby wymuszało zmianę hasła inicjującego przy pierwszym rejestrowaniu się w systemie oraz wymuszało zmianę hasła. ASI biorąc pod uwagę opinię niezależnych organizacji zajmujących się bezpieczeństwem może (np. NIST), może zmienić parametry tworzenia hasła i czasu ważności, zapisując datę zmiany i parametry w dzienniku systemu oraz informując o zmianie użytkowników.

HASŁA DO APLIKACJI UŻYTKOWYCH (PRZYKŁAD BUDOWY)

Po pozytywnym uwierzytelnieniu w systemie operacyjnym lub domenie użytkownik podaje identyfikator i hasło do obsługiwanej aplikacji.

- Zabrania się jako hasła używać identyfikatora.
- Budowa hasła nie powinna być oparta na prostych skojarzeniach, mieć związku z danymi osobistymi użytkownika tzn. imieniem, nazwiskiem, przezwiskiem, pseudonimem, datą urodzenia zarówno jego jak i jego najbliższych osób, numerem telefonu, numerem dowodu osobistego, numerem rejestracyjnym samochodu itp.
- Zabrania się używać ciągu jednakowych znaków, samych cyfr lub samych liter, prostych sekwencji klawiszy, np. qwerty, 123abc.
- Nie należy używać w hasłach polskich liter diakrytycznych, takich jak: ę, ó, ą, ś, ł, ż, ź, ć, ń.
- Nowe hasło nie powinno być podobne do poprzedniego hasła lub być jego wariantem.
- Hasło musi zawierać co najmniej 8 znaków (liter/cyfr/znaków specjalnych).
- Dobrze dobrane hasła stanowią kombinację liter (wielkich i małych), cyfr i znaków specjalnych.

OCHRONA HASEŁ

–Każdy pracownik obsługujący system informatyczny przetwarzający dane podlegające ochronie jest zobowiązany do zachowania w tajemnicy swojego hasła dostępu. Zabrania się udostępniania haseł innym osobom. Hasło utrzymuje się w tajemnicy również po upływie jego ważności.

–Zabrania się przechowywania hasła w postaci jawnie zapisanej w miejscu dostępnym dla innych osób, w szczególności niedozwolone jest przechowywanie hasła zapisanego np.: na obudowie komputera, monitora lub na odwrocie klawiatury.

–Zabronione jest podejmowanie wszelkich prób przywłaszczenia lub rozszyfrowania hasła innego użytkownika.

–W szczególnie uzasadnionych wypadkach, na wniosek użytkownika, jego hasło może zostać zmienione przez ASI. Hasło tak zmienione podlega zasadom zmiany określonym dla hasła inicjującego.

–Indywidualne hasło dostępu do systemu operacyjnego hasło do poczty elektronicznej może być zmienione (bez zgody i wiedzy użytkownika) przez ASI, na wniosek ADO.

PRZECHOWYWANIE HASEŁ

Ustala się, że przechowywane mają być hasła:

- administratorów baz danych,
- administratorów serwerów,
- administratorów stacji roboczych,
- administratorów aplikacji,
- administratorów programów antywirusowych,
- użytkowników konsol administracyjnych,
- Hasła administracyjne do urządzeń sieciowych.

ASI tworzy listę systemów, do których tworzy się hasła administracyjne którą komunikuje osobie bezpośrednio nadzorującej jego pracę lub ADO.

Hasła w oznaczonych kopertach opisanych datą utworzenia, systemem, podpisem osoby zmieniającej hasło przechowuje ADO lub osoba wyznaczona.

Przykład koperty zawiera załącznik nr 4.

–Wzór ewidencji zmiany haseł stanowi Załącznik nr 1 do niniejszej procedury.

W przypadku konieczności awaryjnego użycia haseł, osoba pobiera hasło i dokonuje wpisu w *Ewidencji udostępniania ratunkowych kopii haseł administratorów*, która stanowi Załącznik nr 2 do niniejszej procedury. Użyte hasło powinno zostać zmienione przez ASI w możliwie najkrótszym czasie. W uzasadnionych przypadkach hasło może zostać udostępnione na podstawie jednorazowego upoważnienia.

ZAŁĄCZNIKI

Załącznik nr 1 - Wzór „Ewidencja ratunkowych kopii haseł administratorów"
Załącznik nr 2 - Ewidencja udostępniania ratunkowych kopii haseł administratorów.
Załącznik nr 3 - Wzór upoważnienia do pobrania ratunkowej kopii hasła administratora.
Załącznik nr 4 - Wzór formularza zmiany hasła administratora.

Załącznik nr 1

Ewidencja ratunkowych kopii haseł administratorów

Lp.	Nazwa systemu/urządzenia	Data i godz. przekazania hasła	Imię i nazwisko przekazującego oraz podpis	Data zniszczenia hasła	Imię i nazwisko oraz podpis
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					

Załącznik nr 2 - Ewidencja udostępniania ratunkowych kopii haseł administratorów.

Lp.	Data i godz. udostępnienia hasła	Nazwa systemu/urządzenia	Nazwisko i imię pobierającego hasło	Podpis pobierającego hasło
1	2	3	4	5

Załącznik nr 3. Wzór upoważnienia do pobrania ratunkowej kopii hasła administratora.

Data _____

UPOWAŻNIENIE DO POBRANIA RATUNKOWEJ KOPII HASŁA ADMINISTRATORA

Upoważniam Pana/Panią

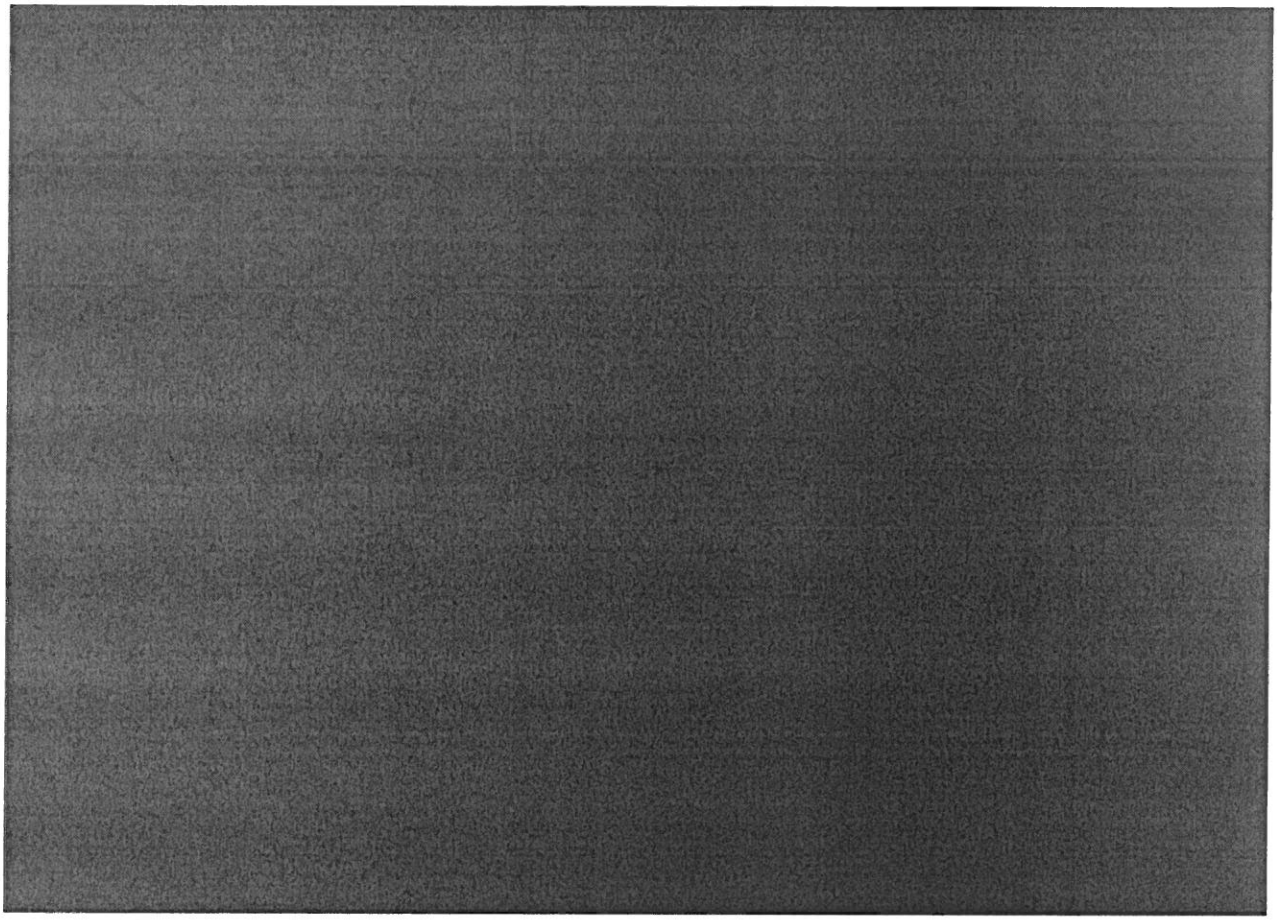
Imię i Nazwisko	
Stanowisko	
Powód	

do pobrania ratunkowej kopii hasła administratora do następujących systemów informatycznych/urządzeń komputerowych: .....

Załącznik nr 4 - Wzór formularza zmiany hasła administratora

Formularz zmiany hasła administratora

1.	Nazwa systemu/urządzenia (nazwa domenowa, adres IP)	
2.	Imię i nazwisko administratora zmieniającego hasło	
3.	Stanowisko	
4.	Nazwa użytkownika/konta (podawana podczas logowania)	
5.	Hasło	
6.	Data i godzina zmiany hasła	
7.	Powód zmiany hasła	
8.	Czytelny podpis administratora zmieniającego hasło	
9.	Uwagi	



Etykieta koperty zawierającej ratunkowe kopię hasła administratora

HASŁO RATUNKOWE		
1.	Nazwa systemu/urządzenia, lokalizacja	
2.	Imię i nazwisko administratora	
3.	Data zmiany hasła	
4.	Data ważności hasła	

Załącznik nr 6. Procedura rozpoczynania, zawieszania i kończenia pracy w systemach informatycznych.

CEL PROCEDURY

Celem procedury jest określenie zasad rozpoczynania, zawieszania i kończenia pracy w systemach informatycznych przetwarzających informacje podlegające ochronie.

ODPOWIEDZIALNOŚĆ

Za przestrzeganie zasad wymienionych w niniejszej procedurze odpowiadają:

wszyscy użytkownicy systemów.

ZAKRES I WARUNKI STOSOWANIA

Procedura przeznaczona jest dla wszystkich osób korzystających z systemów przetwarzających informacje podlegające ochronie. Procedura ma charakter ogólny i zastosowanie do wszystkich systemów informatycznych. Wymagania podane w dokumencie spełniają zalecenia zawarte w normie PN-ISO/IEC 27001 w zakresie wskazanym w punkcie 9, 11,

TREŚĆ PROCEDURY

ROZPOCZĘCIE PRACY

- Przed rozpoczęciem pracy pracownik powinien się upewnić, czy jego stanowisko pracy jest gotowe do jej rozpoczęcia:
  - w obszarze przetwarzania nie ma osób nieupoważnionych,
  - na widocznym miejscu nie ma zbędnych nośników i wydruków zawierających informacje prawnie chronione,
  - nie nastąpiło naruszenie bezpieczeństwa informacji,
  - ekran monitora stanowiska przetwarzania danych jest ustawiony tak, żeby uniemożliwić wgląd w dane osobom postronnym.
- Pracę z komputerem rozpoczyna się logując się za pomocą swojego identyfikatora i hasła:
  - w pierwszej kolejności użytkownik systemu loguje się do systemu operacyjnego lub domeny. Po pomyślnej weryfikacji dostępu do zasobów, użytkownik może rozpocząć pracę z aplikacjami, do których uzyskał stosowne uprawnienia.
  - użytkownik, w momencie logowania się do systemu operacyjnego lub domeny i innych aplikacji, musi zachować należytą ostrożność w trakcie podawania swojego hasła. Nikt poza właścicielem konta nie powinien znać indywidualnego hasła użytkownika.
  - w razie wystąpienia nieprawidłowości, w sytuacji podejrzenia naruszenia bezpieczeństwa systemu, np. w przypadku braku możliwości zalogowania się na swoje konto, stwierdzenia

fizycznej ingerencji w przetwarzane dane lub narzędzia programowe czy sprzętowe, należy powiadomić ASI.

PRACA Z KOMPUTEREM

- Obowiązkiem użytkownika jest śledzenie reakcji poszczególnych urządzeń i komunikatów pojawiających się na monitorze podczas uruchamiania i eksploatacji komputera.
- Użytkownik powinien korzystać z przydzielonej mu przestrzeni na dysku sieciowym w celu archiwizacji dokumentów i ich ochrony przed utratą na wypadek awarii dysku twardego stacji roboczej, na której pracuje.
- Należy przestrzegać warunków podłączenia sprzętu do wewnętrznych oraz zewnętrznych sieci łączności, gniazd elektrycznych i logicznych, określonych przez administratora systemu. Wszelkie zmiany w istniejących podłączeniach i konfiguracji, bez uprzedniego zezwolenia administratora systemu, są niedozwolone.
- Zabrania się pozostawiania bez nadzoru niezabezpieczonego komputera.
- W przypadku pracy na zasilaniu awaryjnym należy, po otrzymaniu komunikatu od automatycznego monitora stanu sieci zasilającej, niezwłocznie zakończyć pracę we wszystkich aplikacjach przetwarzających dane i wyłączyć stację komputerową. Przetwarzanie danych w czasie pracy urządzeń podtrzymujących napięcie nie jest dopuszczalne, ponieważ po przekroczeniu limitu czasu nie gwarantuje poprawności zapisu danych. Wyznaczony czas jest tylko po to, aby prawidłowo zakończyć procesy przetwarzania danych.

ZAWIESZENIE I ZAKOŃCZENIE PRACY

- W przypadku konieczności zawieszenia pracy i odejścia od stanowiska, użytkownik powinien się upewnić, że dane są właściwie chronione, w szczególności nie są widoczne na ekranie, a nośniki lub wydruki zawierające dane są właściwie zabezpieczone.
- Gdy stanowisko komputerowe jest używane przez więcej niż jednego użytkownika, osoba opuszczająca stanowisko jest zobowiązana do zakończenia pracy wszystkich uruchomionych aplikacji oraz do wylogowania się z systemu operacyjnego lub domeny: przycisk „Start" – Zamknij - Wyloguj.
- Gdy stanowisko komputerowe jest używane przez jednego użytkownika, w przypadku opuszczenia stanowiska należy komputer zablokować: klawisze CTRL-ALT-DELETE – przycisk: Zablokuj komputer.
- Dla komputerów mających odpowiednie możliwości techniczne dopuszcza się również blokowanie komputera poprzez automatyczny wygaszacz. W takim przypadku ASI ustawia automatyczny wygaszasz chroniony hasłem i uruchamiany po 15 minutach nieaktywności użytkownika.
- W momencie zakończenia pracy użytkownik zobowiązany jest zakończyć i zamknąć wszystkie uruchomione aplikacje i wyłączyć komputer: przycisk „Start" – Zamknij - Zamknij system.

Załącznik nr 7. Procedura tworzenia kopii.

CEL PROCEDURY

Celem procedury jest określenie zasad tworzenia, przechowywania, konserwacji i wykorzystywania kopii bezpieczeństwa.

ODPOWIEDZIALNOŚĆ

Za przestrzeganie zasad wymienionych w niniejszej procedurze odpowiada:

Administrator Systemów Informatycznych,

ZAKRES I WARUNKI STOSOWANIA

Procedura przeznaczona jest dla ASI. Procedura ma zastosowanie do wszystkich eksploatowanych systemów informatycznych przetwarzających dane osobowe. Wymagania podane w dokumencie spełniają zalecenia zawarte w normie PN-ISO/IEC 27001 w zakresie wskazanym w punkcie 12, 11, 9, 8.

TREŚĆ PROCEDURY

ZASADY POSTĘPOWANIA

–Za tworzenie kopii bezpieczeństwa systemów komputerowych odpowiedzialni są ASI.

–Kopie bezpieczeństwa tworzy się dla wszystkich systemów informatycznych, przetwarzających dane osobowe.

Wskazane jest posiadanie kilku rodzajów kopii np.: kopia pełna aplikacji i bazy danych, kopia przyrostowa bazy danych, kopia eksportu bazy danych, kopia ratunkowa systemu operacyjnego.

Akceptowalne jest również wykonywanie obrazu systemu, który udostępnia bazy danych.

Warunkiem niezbędnym jest weryfikacja poprawności utworzenia kopii (bazy danych czy obraz systemu) wykonana poprzez odtworzenie i uruchomienie. Fakt weryfikacji takiej bazy danych ASI odnotowuje w dzienniku systemu.

–Proces wykonywania określony jest w instrukcji tworzenia kopii będącej w posiadaniu ASI, zaś wszelkie odstępstwa dokumentowane są w dzienniku systemu.

–Każda kopia bezpieczeństwa wykonywana jest na odrębnym nośniku informacji, w liczbie egzemplarzy, która zapewni skuteczne odtworzenie systemu operacyjnego, aplikacji lub bazy danych. Alternatywę stanowi wykonywanie kopii bezpieczeństwa na inny serwer lub dysk.

–Przy kopiowaniu nie można wykorzystywać uszkodzonych nośników lub innych niż przewiduje specyfikacja urządzeń, na których wykonywane są kopie.

–Nośniki informacji zawierające kopie bezpieczeństwa są wyraźnie oznaczone, a oznaczenie to wskazuje, że nośniki te zawierają archiwum danych.

–Wycofane z eksploatacji nośniki, na których zapisywane były kopie bezpieczeństwa, przekazywane są w celu zniszczenia w sposób uniemożliwiający odczytanie danych.

–Częstotliwość tworzenia kopii bezpieczeństwa określają administratorzy systemów z uwzględnieniem istniejących wymogów wynikających z zasad eksploatacji systemów informatycznych. Harmonogram

tworzenia kopii zapasowych, dla poszczególnych zasobów informatycznych stanowi dokumentację wewnętrzną.

–Proces tworzenia kopii bezpieczeństwa opiera się na standardowych narzędziach dostępnych w systemach operacyjnych służących do wykonywania kopii bezpieczeństwa i odtwarzania danych z kopii lub dedykowanego oprogramowania.

MIEJSCA PRZECHOWYWANIA KOPII BEZPIECZEŃSTWA

Kopii bezpieczeństwa nie można przechowywać w tych samych pomieszczeniach, w których znajdują się oryginały zabezpieczanych informacji.

Wszystkie nośniki z kopiami należy składować (o ile są możliwości) w ogniotrwałym sejfie, umieszczonym w pomieszczeniu Urzędu Gminy niebędącym serwerownią, w której znajduje się serwer aplikacji. Pomieszczenie takie musi znajdować się wewnątrz strefy, do której dostęp osób postronnych jest ograniczony. Nośniki należy przechowywać z troską, aby kopie dostępne były tylko dla osób do tego upoważnionych. Osoby te powinny dochować staranności w korzystaniu z nośników tak aby nie dostały się one w posiadanie osób nieuprawnionych.

Wszystkie nośniki umieszczone w sejfie muszą być właściwie opisane, zgodnie z zasadami obowiązującymi dla poszczególnych rodzajów kopii. Informacje o przechowywanych kopiach muszą być odnotowywane w ewidencji przechowywanych nośników. Zalecane jest, aby powyższa ewidencja znajdowała się w posiadaniu ASI i była przechowywana w miarę możliwości ww. sejfie. Ewidencja powinna zawierać w szczególności następujące pozycje: rodzaj kopii, data wykonania kopii, podpis osoby przekazującej, minimalna data przechowywania kopii, data przekazania nośnika do ponownego użycia lub likwidacji, podpis osoby odbierającej.

Minimalny okres przechowywania nośników wynika z zasad wykonywania poszczególnych rodzajów kopii, przyjmuje się, że każdego rodzaju kopii nie powinno być mniej niż 3.

Nośniki z kopiami systemu operacyjnego, binariów, aplikacji i bazy danych mogą być wykorzystane do prowadzenia działań naprawczych aplikacji po uzyskaniu zgody Administratora danych. Po upływie okresu przechowywania kopii, nośniki mogą być cyklicznie wykorzystane do wykonania kolejnych kopii lub zostać zniszczone

NOŚNIKI INFORMACJI

–Wszyscy użytkownicy systemów informatycznych zobowiązani są do ochrony nośników przed ich fizycznym uszkodzeniem, zniszczeniem lub odczytaniem informacji na nich zawartych przez nieuprawnione osoby.

–Zabrania się wykorzystywania nośników informacji niewiadomego pochodzenia.

–Nośniki informatyczne otrzymywane z zewnątrz należy używać wyłącznie po uprzednim sprawdzeniu programem antywirusowym.

–Nośniki zawierające dane osobowe muszą być wyraźnie opisane w celu:

- zapobiegania przypadkowemu wydaniu ich do ponownego użycia,
- zapobiegania nieumyślnemu ujawnieniu informacji podlegających ochronie,

▪ poinformowania potencjalnych użytkowników o konieczności szczególnej ochrony tych nośników.

–Nośniki zawierające dane osobowe nie mogą być wynoszone z siedziby bez zgody ADO. Prowadzona jest ewidencja ww. nośników. Nośniki pamięci zawierające dane osobowe, wynoszone z siedziby muszą być zaszyfrowane.

ZASADY PRZECHOWYWANIA NOŚNIKÓW INFORMACJI

Przechowywanie nośników informacji zawierających dane osobowe odbywa się w warunkach zapewniających ich ochronę przed ujawnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, nieuprawnioną zmianą, uszkodzeniem lub zniszczeniem.

Załącznik nr 8. Procedura zarządzania nośnikami.

CEL PROCEDURY

Celem procedury jest określenie zasad przechowywania oraz usuwania nośników z danymi osobowymi.

ODPOWIEDZIALNOŚĆ

Za przestrzeganie zasad wymienionych w niniejszej procedurze odpowiadają:

a. Wszyscy użytkownicy systemów informatycznych,
b. Administratorzy Systemów Informatycznych,
c. ADO – kontrola stosowania zasad.

ZAKRES I WARUNKI STOSOWANIA

Procedura ma zastosowanie do wszystkich eksploatowanych systemów informatycznych przetwarzających dane osobowe. Wymagania podane w dokumencie spełniają zalecenia zawarte w normie PN-ISO/IEC 27001 w zakresie wskazanym w punkcie 8,

TREŚĆ PROCEDURY

NOŚNIKI INFORMACJI

Wszyscy użytkownicy systemów informatycznych zobowiązani są do ochrony nośników przed ich fizycznym uszkodzeniem, zniszczeniem lub odczytaniem informacji na nich zawartych przez nieuprawnione osoby.

–Zabrania się wykorzystywania nośników informacji niewiadomego pochodzenia.

–Nośniki informatyczne otrzymywane z zewnątrz należy używać wyłącznie po uprzednim sprawdzeniu programem antywirusowym.

–Nośniki zawierające dane osobowe muszą być wyraźnie opisane w celu:

▪ zapobiegania przypadkowemu wydaniu ich do ponownego użycia,
▪ zapobiegania nieumyślnemu ujawnieniu informacji podlegających ochronie,

▪ poinformowania potencjalnych użytkowników o konieczności szczególnej ochrony tych nośników.

–Nośniki zawierające dane osobowe nie mogą być wynoszone z terenu bez zgody ADO. Prowadzona jest ewidencja ww. nośników.

–Nośniki pamięci zawierające dane osobowe, wynoszone z terenu, muszą być zaszyfrowane.

ZASADY PRZECHOWYWANIA NOŚNIKÓW INFORMACJI

Przechowywanie nośników informacji zawierających dane osobowe odbywa się w warunkach zapewniających ich ochronę przed ujawnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, nieuprawnioną zmianą, uszkodzeniem lub zniszczeniem.

USUWANIE DANYCH OSOBOWYCH Z URZĄDZEŃ I NOŚNIKÓW INFORMACJI

–Dane osobowe przechowywane na nośnikach informacji muszą być z nich usuwane w momencie ustania przyczyn, dla których zostały na tych nośnikach zapisane lub po upływie czasu przewidzianego do ich przechowywania.

–Nośniki przeznaczone do zniszczenia przechowuje się w chronionym pomieszczeniu.

–Dane znajdujące się na tych nośnikach podlegają ochronie w takim samym stopniu jak dane tego samego rodzaju nie przeznaczone do usunięcia.

–Usunięcia danych chronionych zapisanych na zewnętrznych nośnikach informacji jednorazowego zapisu należy dokonywać wyłącznie poprzez fizyczne niszczenie tych nośników. Należy się posługiwać dokumentem *Procedura usuwania danych z nośników (Załącznik nr 16)*.

–W przypadku konieczności przekazania urządzeń i nośników informacji do naprawy poza siedzibę należy postępować zgodnie z dokumentem *Procedura przekazywania urządzeń i nośników zawierających dane chronione poza obszar przetwarzania - Załącznik nr 14.*

W przypadku niezbędności wykorzystania nośników wymiennych stosuje się *Załącznik nr 17. Zasady postępowania z pamięciami przenośnymi*

Załącznik nr 9. Procedura zabezpieczenia przed nieuprawnionym oprogramowaniem.

CEL PROCEDURY

Celem procedury jest określenie zasad zapewniających zapobieganie i wykrywanie obecności szkodliwego oprogramowania.

ODPOWIEDZIALNOŚĆ

Za przestrzeganie zasad wymienionych w niniejszej procedurze odpowiadają:

a. Administratorzy Systemów Informatycznych,
b. Wszyscy użytkownicy systemów,
c. ADO – kontrola stosowania zasad.

ZAKRES I WARUNKI STOSOWANIA

Procedura przeznaczona jest dla wszystkich osób, które zobowiązane są do stosowania dokumentacji bezpieczeństwa. Procedura ma charakter ogólny i ma zastosowanie do wszystkich systemów informatycznych przetwarzających dane osobowe. Wymagania podane w dokumencie spełniają zalecenia zawarte w normie PN-ISO/IEC 27001 w zakresie wskazanym w punkcie 12, 18.

TREŚĆ PROCEDURY

LICENCJONOWANE OPROGRAMOWANIE ANTYWIRUSOWE

–W całej organizacji funkcjonuje oprogramowanie antywirusowe. Jego wdrożenie i zarządzanie są koordynowane przez ASI.

–Na ingerencje nieuprawnionego oprogramowania narażone są wszystkie stacje robocze, serwery oraz komputery przenośne oraz maszyny wirtualne będące zasobami.

–Źródłami nieuprawnionego oprogramowania mogą być przesyłki poczty elektronicznej, strony internetowe, nielicencjonowane oprogramowanie, niesprawdzone nośniki informacji, itp.

–Licencjonowane oprogramowanie antywirusowe jest zainstalowane na następujących urządzeniach wchodzących w skład eksploatowanych systemów informatycznych:

- wszystkich stacjach roboczych,
- wszystkich serwerach.

Funkcjonujące oprogramowanie antywirusowe:

- umożliwia bezpieczne korzystanie z komputera, zapewniając wykrywanie i automatyczne usuwanie wirusów, koni trojańskich, robaków i innego złośliwego oprogramowania,
- zapewnia odpowiednią ochronę, w przypadku pojawienia się nowych programów złośliwych, dzięki automatycznemu aktualizowaniu systemu zabezpieczeń,
- jest tak skonfigurowane, aby umożliwiało kontrolę systemu plików w czasie rzeczywistym.

OBOWIĄZKI ASI SYSTEMU ANTYWIRUSOWEGO

–Oprogramowanie antywirusowe jest systematycznie i automatycznie aktualizowane. Nadzór nad aktualizacjami prowadzi ASI.

–ASI monitoruje prawidłowość i skuteczność działania funkcjonującego oprogramowania antywirusowego.

OBOWIĄZKI WSZYSTKICH UŻYTKOWNIKÓW SYSTEMU INFORMATYCZNEGO

–Wszyscy użytkownicy systemu informatycznego muszą mieć świadomość, że nie da się w pełni wyeliminować zagrożeń związanych z przedostaniem się do zasobów informatycznych nieuprawnionego oprogramowania, mimo zainstalowanego i na bieżąco aktualizowanego oprogramowania antywirusowego.

–Nie wolno wyłączać monitorowania w czasie rzeczywistym dotyczącego ochrony antywirusowej.

–Obowiązuje zakaz instalacji przez użytkowników, bez zgody ASI, jakiegokolwiek oprogramowania na komputerach, w tym przenośnych. Oprogramowanie na serwerach instaluje wyłącznie ASI. W uzasadnionych przypadkach ASI może upoważnić inną osobę do instalacji oprogramowania.

–Należy bezwzględnie przestrzegać praw autorskich do programów oraz umów licencyjnych.

–Automatyczna aktualizacja oprogramowania powinna być wykonywana bez zbędnej zwłoki.

–Przed uruchomieniem zewnętrznej pamięci wymiennej należy sprawdzić ją oprogramowaniem antywirusowym na obecność złośliwego oprogramowania.

–Przed uruchomieniem pliku pobranego z Internetu należy go sprawdzić oprogramowaniem antywirusowym na obecność złośliwego oprogramowania.

–Nie należy podłączać do stacji urządzeń pamięci wymiennej nieznanego pochodzenia.

–Przypadki wykrycia kodu złośliwego, którego nie można usunąć przy pomocy zainstalowanego oprogramowania antywirusowego, użytkownicy zgłaszają do ASI. Jednocześnie należy natychmiast przerwać pracę do czasu zezwolenia na jej kontynuację uzyskanego od ASI.

–Wszyscy użytkownicy są zobowiązani do identyfikowania sytuacji powstawania zagrożeń ze strony nieuprawnionego oprogramowania oraz przeciwdziałania tym zagrożeniom.

–Należy zwracać uwagę na nietypowe zachowania systemu informatycznego, takie jak: nieoczekiwane efekty dźwiękowe, nieznane nowe pliki lub katalogi, nagłe zmniejszenie się wolnego miejsca na dysku, niespodziewane komunikaty itp. Wszystkie takie sytuacje należy zgłaszać ASI.

AUTOMATYCZNE USUWANIE ZŁOŚLIWEGO OPROGRAMOWANIA

Zainstalowane oprogramowanie antywirusowe powinno dokonać automatycznego usunięcia kodu złośliwego z systemu. W przypadku stwierdzenia wystąpienia oprogramowania typu Botnet należy skorzystać z procedury zawartej w dokumencie *„Procedura usuwania oprogramowania typu BOTNET" zawartej w Załączniku 17.*

INNE METODY USUWANIA ZŁOŚLIWEGO OPROGRAMOWANIA

W przypadku zgłoszenia przez użytkownika do ASI wykrycia złośliwego oprogramowania, nie dającego się usunąć przy pomocy zainstalowanego oprogramowania, ASI podejmuje działania zmierzające do jego usunięcia przy użyciu innych dostępnych metod.

Po przeprowadzonych działaniach mających na celu usunięcie kodu złośliwego, ASI sporządza raport z podjętych czynności zmierzających do usunięcia nieuprawnionego oprogramowania i składa go ADO

(wzór stanowi Załącznik nr 1 do niniejszej procedury). W przypadku spełnienia warunków realizowany jest dokument *Załącznik nr.18. Procedura zgłaszania incydentów informatycznych.*

ZAŁĄCZNIKI

Załącznik 1 - Wzór „Raport z podjętych czynności zmierzających do usunięcia nieuprawnionego oprogramowania".

Załącznik nr 1

Raport z podjętych czynności zmierzających do usunięcia złośliwego oprogramowania

Część I Zgłoszenie wykrycia złośliwego oprogramowania w systemie informatycznym *(Wypełnia zgłaszający)*	
1. Dane osoby zgłaszającej wykrycie złośliwego oprogramowania - imię, nazwisko nr pomieszczenia	
2. Data i godzina zgłoszenia AS	
3. Krótki opis zgłaszanego problemu	
Część II Raport z podjętych czynności *(Wypełnia interweniujący)*	
1. Dane osoby podejmującej działania w celu usunięcia złośliwego oprogramowania - imię, nazwisko, adres telefon, adres e-mail	
2.Numer inwentarzowy komputera	
3. Wersja i rodzaj użytego oprogramowania antywirusowego	
3. Krótki opis rodzaju infekcji systemu. Nazwa, typ wirusa oraz miejsce na dysku, w którym wirus był znaleziony.	
4.Opis podjętych działań np. usunięcie wirusa, kwarantanna, przeniesienie zainfekowanego pliku w inne miejsce itp.	
5. Opis czynności niezbędnych do wykonania w innych elementach systemu np.: szczegółowa kontrola antywirusowa na innych	
6. Data i godzina wykonania działań oraz podpis wykonującego	Data: podpis:

Załącznik nr 10. Procedura bezpieczeństwa sieci teleinformatycznej.

CEL PROCEDURY

Celem procedury jest określenie zasad i metod działania zapewniających utrzymanie bezpieczeństwa w sieciach komputerowych oraz zadań administratorów systemów informatycznych odpowiedzialnych za administrowanie siecią.

ODPOWIEDZIALNOŚĆ

Za przestrzeganie zasad wymienionych w niniejszej procedurze odpowiadają:

a. Administrator Systemów Informatycznych,
b. Wszyscy użytkownicy systemów,
c. ADO – kontrola stosowania zasad.

ZAKRES I WARUNKI STOSOWANIA

Procedura przeznaczona jest dla administratorów i wszystkich użytkowników sieci komputerowej. Wymagania podane w dokumencie spełniają zalecenia zawarte w normie PN-ISO/IEC 27001 w zakresie wskazanym w punkcie 9, 11, 12, 13.

TREŚĆ PROCEDURY

SIECI TELEINFORMATYCZNE ORAZ ICH ADMINISTRATORZY

Za zarządzanie komunikacją w lokalnych sieciach komputerowych oraz zapewnienie ciągłego, bezawaryjnego i bezpiecznego ich funkcjonowania jest odpowiedzialny ASI.

ZADANIA ADMINISTRATORA

–ASI dba o właściwą konfigurację serwerów oraz innych składników sieci i nadzoruje ich pracę.

–ASI odpowiada za bezpieczeństwo informacji dotyczących rodzaju serwerów, urządzeń telekomunikacyjnych, teletransmisyjnych, sposobu połączeń i systemu łączności.

–Monitorowanie sieci teleinformatycznych odbywa się w szczególności poprzez:

- przeglądanie logów systemowych z serwerów w celu wychwycenia niestandardowych zdarzeń,
- archiwizowanie wybranych zdarzeń z serwerów,
- przeglądanie oraz archiwizowanie wybranych zdarzeń urządzeń sieciowych,
- aktualizację oprogramowania urządzeń sieciowych,
- instalację oprogramowania monitorującego, o ile jest to konieczne,
- zapewnienie braku jakiejkolwiek automatyzacji w ustawianiu monitorowania sieci (różne pory dnia, różne okresy działania programów),
- niezwłoczne reakcje na zgłoszenia użytkowników o niestandardowym zachowaniu eksploatowanego systemu informatycznego,
- w celu dokumentowania pracy ASI prowadzi dziennik systemu, w którym odnotowane są istotne zdarzenia,

- ASI przechowuje w formie tradycyjnej (wydruk) konfigurację urządzeń sieciowych,
- W miarę możliwości technicznych łączy adres MAC z adresem IP a niewykorzystane porty switchów blokuje.

ZASADY KOMUNIKACJI OBOWIĄZUJĄCE UŻYTKOWNIKÓW SIECI

Techniczne środki łączności mogą być używane wyłącznie do celów służbowych.

W szczególności niedozwolone jest:

- nawiązywanie połączeń lub prób nawiązywania połączeń z systemami informatycznymi bez posiadania odpowiedniego upoważnienia do dostępu do tych systemów,
- wykorzystywanie systemów informatycznych do działań zagrażających bezpieczeństwu systemów oraz sieci teleinformatycznych,
- instalowanie i użytkowanie modemów na stacjach podłączonych do sieci lokalnych bez zgody ADO,
- podłączanie do gniazd sieciowych urządzeń, które nie stanowią zasobów organizacji, poza działaniami serwisowymi.
- jednoczesne podłączenie komputera do sieci LAN i innej sieci zewnętrznej – poprzez Wi-Fi lub modem zewnętrzny.

Załącznik nr 11. Procedura korzystania z Internetu i poczty elektronicznej.

CEL PROCEDURY

Celem procedury jest określenie zasad dostępu i korzystania z zasobów Internetu oraz poczty elektronicznej.

ODPOWIEDZIALNOŚĆ

Za przestrzeganie zasad wymienionych w niniejszej procedurze odpowiadają:

a. Wszyscy użytkownicy systemów,
b. Administratorzy Systemu Informatycznego,
c. ADO kontrola stosowania zasad.

ZAKRES I WARUNKI STOSOWANIA

Procedura przeznaczona jest dla ASI oraz dla wszystkich użytkowników, którym udostępniono możliwość korzystania z Internetu i poczty elektronicznej. Wymagania podane w dokumencie spełniają zalecenia zawarte w normie PN-ISO/IEC 27001 w zakresie wskazanym w punkcie 13, 14, 15, 18.

TREŚĆ PROCEDURY

ZASADY KOMUNIKACJI W SIECIACH KOMPUTEROWYCH

–Dostęp do Internetu i poczty elektronicznej powinien być wykorzystywany tylko i wyłącznie do celów służbowych.

–Przekazywanie informacji chronionych za pomocą poczty elektronicznej jest możliwe wyłącznie pod warunkiem odpowiedniego ich zabezpieczenia (np. hasło zabezpieczające, szyfrowanie).

ZASADY KORZYSTANIA Z INTERNETU

–Zabrania się udostępniania osobistego konta innym osobom w celu przeglądania Internetu lub wysyłania poczty elektronicznej.

–Użytkownik pracujący w Internecie powinien być świadomy obciążenia, jakie wnosi do sieci teleinformatycznej.

–Użytkownik ponosi odpowiedzialność za działania, które mogą negatywnie wpływać na wizerunek organizacji, np. wysyłanie obraźliwych wiadomości.

–Użytkownik nie powinien:

- prenumerować na służbowy adres e-mail zbędnych usług,
- pobierać plików graficznych, dźwiękowych, filmowych, jeżeli nie jest to związane z działalnością służbową na zajmowanym stanowisku,
- pobierać z Internetu plików niewiadomego pochodzenia,
- pobierać, uruchamiać oraz rozpowszechniać oprogramowania bez potrzeby uzasadnionej działalnością służbową, nawet jeżeli do jego użytkowania nie jest wymagana opłata lub posiadanie licencji,
- używać sieci teleinformatycznej do celów handlowych i prywatnych,
- wykorzystywać dostępu do usług Internetu w celach niezwiązanych z wykonywaniem obowiązków.

ZASADY KORZYSTANIA Z POCZTY ELEKTRONICZNEJ (E-MAIL)

Użytkownik nie powinien:

- wysyłać masowo (bez uzasadnionej obowiązkami służbowymi potrzeby) wiadomości adresowanej do wielu odbiorców,
- wysyłać wiadomości, które publicznie ujawnione, mogą narazić organizację na straty,
- wysyłać wiadomości, które mogą spowodować utratę wyników pracy u odbiorców (zawirusowane pliki załączników, złośliwe programy itp.).

Użytkownik powinien:

- codziennie kontrolować pocztę, ponieważ stanowi ona ważne ogniwo w obiegu informacji,
- wysyłać wyłącznie podpisane wiadomości,
- wysyłać wyłącznie wiadomości z opisanym polem tematu,
- w przypadku wysyłania wiadomości do wielu użytkowników stosować pole UDW,
- w przypadku dużych plików stosować programy kompresujące i/lub dzielić je na większą liczbę wiadomości.

PRZYZNANIE/ODEBRANIE UPRAWNIEŃ

Przyznanie/odebranie pracownikowi uprawnienia do korzystania z usług Internetu i poczty elektronicznej następuje jednocześnie z przyznaniem/odebraniem dostępu do systemu operacyjnego lub domeny zgodnie z *Procedurą postępowania w zakresie nadawania i odbierania uprawnień do systemów informatycznych*.

Załącznik 12. Procedura bezpieczeństwa komputerów przenośnych.

CEL PROCEDURY

Celem procedury jest zdefiniowanie mechanizmów zabezpieczających oraz zasad prawidłowego użytkowania przenośnych stacji roboczych.

ODPOWIEDZIALNOŚĆ

Za przestrzeganie zasad wymienionych w niniejszej procedurze odpowiadają:

a. Administratorzy Systemów Informatycznych,
b. Wszyscy użytkownicy komputerów przenośnych, smartfonów i tabletów
c. ADO kontrola stosowania zasad.

ZAKRES I WARUNKI STOSOWANIA

Procedura przeznaczona jest dla wszystkich użytkowników komputerów przenośnych. Wymagania podane w dokumencie spełniają zalecenia zawarte w normie PN-ISO/IEC 27001 w zakresie wskazanym w punkcie 11, 18.

TREŚĆ PROCEDURY

PRACA Z KOMPUTEREM PRZENOŚNYM, SMARTFONEM I TABLETEM.

Za bezpieczeństwo komputera przenośnego odpowiedzialny jest jego użytkownik.

–Przenośną stację roboczą należy chronić przed:

- zgubieniem,
- zniszczeniem,
- uszkodzeniem,
- kradzieżą,
- złośliwym oprogramowaniem,
- niepowołanym działaniem osób do tego nieuprawnionych.

–Sprzęt i nośniki informacji nie mogą być pozostawione bez nadzoru w miejscach publicznych.

–Użytkownik jest zobowiązany do korzystania z komputera przenośnego w sposób minimalizujący ryzyko podejrzenia przetwarzanych danych przez osoby nieuprawnione.

–Należy bezwzględnie przestrzegać zaleceń producentów, dotyczących ochrony sprzętu, np. ochrony przed silnym polem elektromagnetycznym czy temperaturą.

–Komputera przenośnego nie wolno udostępniać osobom nieupoważnionym.

–Użytkownik jest zobowiązany do archiwizowania danych przetwarzanych na komputerze przenośnym w celu zabezpieczenia przed ich utratą.

–Niedozwolone jest jednoczesne podłączenie komputera przenośnego do lokalnej sieci komputerowej z inną siecią zewnętrzną (np. poprzez Wi-Fi lub modem zewnętrzny).

ZALECENIA DOTYCZĄCE ZABEZPIECZEŃ KOMPUTERÓW PRZENOŚNYCH

ZABEZPIECZENIA FIZYCZNE

–Jeżeli przenośna stacja robocza wykorzystywana będzie przez dłuższy czas w jednym pomieszczeniu, to zaleca się (jeśli możliwości techniczne na to pozwalają) korzystanie z linki zabezpieczającej.

–Komputery przenośne należy transportować tylko w przystosowanych do tego celu torbach.

–Dodatkowe urządzenia zewnętrzne instalować może tylko Administrator Systemu Informatycznego. Dostępne urządzenia zewnętrzne (pendrive, dyski) muszą być szyfrowane. W przypadku korzystania z dysków przenośnych należy stosowań procedurę *Załącznik nr 17 Zasady postępowania z pamięciami przenośnymi.*

–Naprawy, serwis, modernizacje należy realizować tylko poprzez upoważnionych pracowników (zgodnie z *Procedurą wykonywania przeglądów i konserwacji systemów oraz nośników służących do przetwarzania danych osobowych* – Załącznik nr 13).

ZABEZPIECZENIA ORGANIZACYJNE

–Każdy użytkownik komputera przenośnego powinien posiadać własne konto, na którym może pracować z zachowaniem rozliczalności działań podejmowanych w systemie.

–Dane osobowe przechowywane na przenośnej stacji roboczej należy zapisywać tylko i wyłącznie w zaszyfrowanym zasobie, w celu uniemożliwienia odczytu przez nieuprawnione do tego osoby. Każdy użytkownik przetwarzający dane osobowe lub inne informacje prawnie chronione z wykorzystaniem przenośnej stacji roboczej jest zobowiązany zgłosić ASI zapotrzebowanie na dostęp do aplikacji pozwalającej na zaszyfrowanie wybranych wolumenów, partycji lub całego dysku. Preferowane jest szyfrowanie całego dysku z wykorzystaniem zasobów systemowych.

–Jeśli przenośna stacja robocza nie jest włączona do sieci, to należy obowiązkowo dokonywać okresowej aktualizacji oprogramowania. Niedopuszczalny jest brak aktualizacji systemu operacyjnego i aplikacji

ZABEZPIECZENIA PROGRAMOWE REALIZOWANE NA POZIOMIE BIOS-u:

–Na wszystkich komputerach przenośnych ASI ustawia hasło dostępu do konfiguracji systemu BIOS.

–ASI blokuje w ustawieniach BIOS opcję „BOOT" z urządzeń innych niż lokalny dysk twardy i ustawia domyślnie bootowanie z HDD.

–Wszystkie dyski powinny być zaszyfrowane (np. BitLocker)

ZABEZPIECZENIA PROGRAMOWE REALIZOWANE PRZEZ SYSTEM:

–ASI ustawia automatyczny wygaszasz chroniony hasłem i uruchamiany w przypadku nieaktywności użytkownika trwającej dłużej niż 15 minut.

–ASI włącza i konfiguruje systemową zaporę Windows oraz oprogramowanie antywirusowe.

BEZPIECZNA EKSPLOATACJA KOMPUTERÓW PRZENOŚNYCH, SMARTFONÓW I TABLETÓW

- Nie należy wyłączać urządzeń przyciskiem do jej włączania – należy robić to z poziomu systemu operacyjnego.
- Nie należy uruchamiać urządzeń bezpośrednio po transportowaniu go w bardzo niskiej temperaturze. Należy opóźnić jego uruchomienie do czasu osiągnięcia przez niego temperatury pokojowej.
- Urządzenia przenośne należy chronić przed przegrzaniem.
- Należy stosować się do zaleceń producentów dotyczących eksploatacji, transportu i ochrony urządzeń.

Załącznik nr 13. Procedura wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

CEL PROCEDURY

Celem procedury jest określenie zasad przeprowadzania bieżących przeglądów i konserwacji elementów mających wpływ na poprawność przetwarzania danych osobowych.

ODPOWIEDZIALNOŚĆ

Za przestrzeganie zasad wymienionych w niniejszej procedurze odpowiadają:

Administratorzy Systemów Informatycznych,

ADO kontrola stosowania zasad.

ZAKRES I WARUNKI STOSOWANIA

Procedura ma charakter ogólny i dotyczy wszystkich eksploatowanych systemów informatycznych przetwarzających dane osobowe. Wymagania podane w dokumencie spełniają zalecenia zawarte w normie PN-ISO/IEC 27001 w zakresie wskazanym w punkcie 18, 11, 13.

TREŚĆ PROCEDURY

TRYB DOKONYWANIA PRZEGLĄDÓW I KONSERWACJI

–Urządzenia oraz oprogramowanie podlegają okresowym przeglądom i konserwacjom zgodnie z zaleceniami ich producentów oraz bieżącymi potrzebami, a także za każdym razem, gdy zostanie stwierdzone naruszenie bezpieczeństwa systemu informatycznego.

–Do wykonywania przeglądów wykorzystuje się standardowe narzędzia systemowe, aplikacyjne oraz inne, umożliwiające jednoznaczne określenie stanu zasobu i/lub tendencję zmiany wskaźników mających istotne znaczenie dla niezawodnej i wydajnej pracy systemów informatycznych.

–Przeglądów i konserwacji urządzeń oraz oprogramowania dokonują ASI.

–Przeglądów i konserwacji dokonują również jednostki serwisowe w ramach gwarancji producenta lub jednostki serwisowe, z którymi zawarto umowy na świadczenie usług serwisowych. W takim wypadku należy postępować zgodnie z dokumentem *Procedura przekazania urządzeń oraz nośników poza obszar przetwarzania (do serwisu lub naprawy)* – Załącznik nr 14 do dokumentu.

DZIENNIK PRZEGLĄDÓW I ZDARZEŃ SERWISOWYCH

–ASI prowadzi dziennik przeglądów i zdarzeń serwisowych dla administrowanych urządzeń, oprogramowania systemowego oraz aplikacyjnego. Dziennik może być tożsamy z Dziennikiem systemu.

–Dziennik ten dokumentuje wszystkie przeglądy oraz wykonywane czynności serwisowe od momentu zgłoszenia uszkodzenia do jednostki serwisowej, aż do jego usunięcia.

–W dzienniku należy umieszczać w szczególności informacje na temat:

- monitorowania stanu zasobu i stwierdzenia poprawnego lub wadliwego jego funkcjonowania,
- rejestracji zgłoszenia o usterce,

- przekazania zgłoszenia do odpowiedniej jednostki serwisowej,
- przeprowadzonych czynności serwisowych,
- przeprowadzonych modyfikacji elementów systemów informatycznych.

Załącznik nr 14. Procedura przekazywania urządzeń i nośników poza obszar przetwarzania (do serwisu lub naprawy).

CEL PROCEDURY

Celem procedury jest określenie zasad przekazywania urządzeń i nośników zawierających dane osobowe poza siedzibę.

ODPOWIEDZIALNOŚĆ

Za przestrzeganie zasad wymienionych w niniejszej procedurze odpowiadają:

a. Administratorzy Systemów Informatycznych,

b. ADO.

ZAKRES I WARUNKI STOSOWANIA

Procedura przeznaczona jest dla pracowników za współpracę z jednostkami serwisowymi w ramach konserwacji i napraw urządzeń oraz nośników zawierających dane osobowe. Wymagania podane w dokumencie spełniają zalecenia zawarte w normie PN-ISO/IEC 27001 w zakresie wskazanym w punkcie 13, 12, 11, 8.

TREŚĆ PROCEDURY

–Odpowiedzialnymi za przekazywanie urządzeń zawierających dane osobowe poza obszar przetwarzania, w przypadku napraw lub konserwacji, są wyznaczeni pracownicy. Nadzór nad niniejszymi czynnościami sprawuje ADO.

–Napraw i konserwacji urządzeń informatycznych mogą dokonywać jednostki serwisowe w ramach gwarancji producenta oraz jednostki serwisowe, z którymi zawarto umowy na świadczenie usług serwisowych.

–Usługi serwisowe, w stosunku do urządzeń zawierających dane osobowe, powinny być wykonywane w strefach chronionych i pod kontrolą upoważnionych pracowników.

–Jeżeli usługi serwisowe muszą być świadczone poza strefami chronionymi, w żadnym przypadku nie wolno podawać hasła do zaszyfrowanego dysku.

–Należy zwrócić szczególną uwagę na ochronę urządzeń i nośników podczas transportu. W celu ochrony zasobów przed uszkodzeniami fizycznymi należy stosować odpowiednie opakowania, zgodnie z wymogami producentów. Zaleca się korzystanie ze sprawdzonej firmy kurierskiej. W przypadku danych szczególnie wrażliwych stosuje się dostarczenie do rąk własnych.

–Części urządzeń podlegające wymianie, które mogą zawierać dane osobowe należy zniszczyć.

Załącznik nr 15. Anonimizacja, pseudonimizacja oraz szyfrowanie.

CEL PROCEDURY

Celem niniejszej procedury jest określenie zasad dokonywania anonimizacji, pseudonimizacji i szyfrowania danych osobowych oraz określenie warunków doboru wymienionych środków bezpieczeństwa w stosunku do przetwarzanych danych.

ODPOWIEDZIALNOŚĆ

Za przestrzeganie zasad wymienionych w niniejszej procedurze odpowiadają:

a) Pracownik;

b) ASI.

ZAKRES I WARUNKI STOSOWANIA

Procedura jest dokumentem ogólnodostępnym dla wszystkich pracowników, a jej znajomość jest obowiązkowa dla wszystkich oraz pracowników komórki IT zaangażowanych w proces bezpieczeństwa informacji. Wymagania podane w dokumencie spełniają zalecenia zawarte w normie PN-ISO/IEC 27001 w zakresie wskazanym w punkcie 18.

TREŚĆ PROCEDURY

Niniejsza procedura określa techniki zabezpieczenia danych tj.:

1) anonimizacja,
2) pseudonimizacja,
3) szyfrowanie.

Odpowiednie stosowanie wyżej wymienionych technik ma na celu minimalizację ryzyka wynikającego z udostępniania danych osobowych procesorom lub współadministratorom.
Procedura ma na celu zapewnienie podniesienia poziomu ochrony danych osobowych zgodnie z zasadą „privacy by design" oraz odgrywa istotną rolę we wdrożeniu strategii minimalizacji danych, przyczynia się do obniżenia potencjalnie negatywnych skutków dla podmiotów danych w przypadku wystąpienia naruszenia bezpieczeństwa.

Poniższa tabela przedstawia podstawy wybranych mechanizmów zabezpieczających.

	ANONIMIZACJA	PSEUDONIMIZACJA	SZYFROWANIE
Sposób działania:	Identyfikacja tożsamości jednostki nie jest możliwa	Pola umożliwiające identyfikację tożsamości jednostki są zastąpione kluczem	Utajnienie informacji
Odwracalność procesu	Nie	Tak, z trudnością	Tak, z łatwością
Zastosowanie:	- brak podstawy przetwarzania danych osobowych; - po zakończeniu okresu retencji danych; - zgodnie z możliwościami /potrzebami.	w raportach, analizach itd.	wszelkie dane osobowe

Etapy procesu wymagającego zastosowania mechanizmu zabezpieczania.

W momencie wystąpienia zdarzenia, które potencjalnie może wymagać zastosowania mechanizmów zabezpieczających, Pracownik winien potwierdzić konieczność zastosowania

określonych technik (na przykład: cofnięcie zgody przez klienta, prośba o usunięcie danych, koniec okresu retencji, potrzeba wysłania wiadomości elektronicznej z danymi osobowymi).

Wybór metody zabezpieczenia – przesyłanie danych emailem. Aby zapewnić poufność danych osobowych w sytuacji, gdy są one przekazywane innej osobie lub firmie za pomocą poczty elektronicznej, konieczne jest zastosowanie szyfrowania. Stosowanie szyfrowania nie wymaga każdorazowej konsultacji z komórką IT, pracownicy mają bezpośredni dostęp do programu szyfrującego, a w razie wątpliwości co do stosowania tej metody, punktem kontaktu jest Pracownik.

Wybór metody zabezpieczenia – inne. Gdy wystąpi zdarzenie wymagające zastosowania zaawansowanych metod zabezpieczenia danych (anonimizacja lub pseudonimizacja) i zostanie to potwierdzone przez Pracownika, zwraca się on do komórki ds. IT w celu analizy możliwych do zastosowania dla danej kategorii danych technik.

Wybór metody zabezpieczenia – główne systemy informatyczne. W przypadku, gdy konieczność zastosowania techniki zabezpieczenia dotyczy głównych systemów, w których są przetwarzane dane osobowe) sposób postępowania, w tym wybór metody postępowania, jest z góry określony i wynika z możliwości technicznych systemu.

Wdrożenie mechanizmu zabezpieczającego. Komórka ds. IT realizuje zastosowanie mechanizmu zabezpieczającego (bądź dostarcza narzędzia, do stosowania technik przez Pracownika) dane w systemach, zgodnie z ustalonym z Pracownikiem schematem.

Udokumentowanie zastosowania mechanizmu zabezpieczającego. Pracownik przygotowuje stosowną dokumentację dotyczącą zanonimizowanych danych.

Podjęcie decyzji w przypadku braku możliwości technicznych. W przypadku, gdy brak jest technicznych możliwości wdrożenia mechanizmów zabezpieczających, komórka właściwa ds. IT przekazuje taką informację do Pracownika oraz IOD, IOD podejmuje decyzję o akceptacji ryzyka, bądź w wyjątkowych przypadkach eskaluje takie ryzyko do Zarządu

Wybór mechanizmu zabezpieczającego na środowisku innym niż produkcyjne. W przypadku, gdy konieczność zastosowana mechanizmu zabezpieczającego dotyczy kopii danych w zakresie środowiska innego niż produkcyjne, wybór metody oraz sposób jej wykonania zależy od możliwości technicznych systemu. Decyzję w tej sprawie podejmuje komórka ds. IT przy uwzględnieniu możliwości technicznych systemów. Na środowiskach developerskich oraz szkoleniowych nie powinno się przetwarzać danych osobowych bez uprzedniego zastosowania anonimizacji / pseudonimizacji z uwagi na ochronę poufności danych. W przypadku braku możliwości technicznych zastosowania odpowiedniego środka zabezpieczającego, ASI informuje o tym Pracownika oraz IOD który podejmuje decyzję o akceptacji ryzyka przetwarzania danych.

Anonimizacja

Jest procesem modyfikacji danych osobowych uniemożliwiającym ich ponowne przyporządkowanie do danej jednostki oraz alternatywą dla trwałego usuwania danych osobowych po upłynięciu okresu retencji.

Proces ten jest nieodwracalny i należy zachować ostrożność przy jego wykorzystywaniu. Dane, które zostały zanonimizowane nie są dłużej danymi osobowymi w rozumieniu RODO, a więc przepisy nie mają wobec nich zastosowania. Po dokonaniu anonimizacji dane mogą być przetwarzane w dowolny sposób. Powoduje to, że wykorzystanie zanonimizowanych informacji na potrzeby statystyczne/analityczne staje się możliwe. Anonimizacja może być stosowana wobec wszystkich celów przetwarzania, które nie wymagają operacji na danych osobowych w formie jednoznacznie identyfikowalnej.

Stosowanie tej metody jest zasadne w następujących przypadkach:

1) po upłynięciu okresu retencji,

2) w odpowiedzi na wycofanie zgody na przetwarzanie danych osobowych,
3) w odpowiedzi na prośbę o usunięcie danych osobowych oraz
4) w przypadku braku podstawy dalszego przetwarzania (np. po zrealizowaniu celu przetwarzania, po zakończeniu procesu).

Decyzja o stosowaniu techniki oraz jej zakres powinien podlegać każdorazowo weryfikacji.

Podstawowe metody wykorzystywane do anonimizacji danych osobowych:

1) **Utajenie** – usunięcie części danych identyfikacyjnych z danego zbioru danych w celu redukcji stopnia identyfikowalności, np. usunięcie danego pola ze zbioru danych;
2) **Generalizacja** – przekształcenie pewnych konkretnych wartości na element przedziału / szerszego zakresu, np. przekształcenie danych dot. wieku jednostki (18 lat) na przedział wiekowy (18-24 lata);
3) **Randomizacja** – modyfikacja danych w celu zerwania ich połączenia z jednostką, może polegać na wprowadzeniu losowych zmian w zbiorze polegających np. na zamianie pewnych wartości pomiędzy rekordami dotyczącymi poszczególnych jednostek (np. podmiana daty urodzenia)

Żadna z opisanych powyżej technik nie daje całkowitej gwarancji, że otrzymane w wyniku anonimizacji dane nie będą możliwe do jednoznacznej identyfikacji.

Pseudonimizacja

To proces przetwarzania danych osobowych uniemożliwiający ich przypisanie konkretnej osobie bez użycia dodatkowych informacji, polega na usunięciu pewnego zakresu danych identyfikacyjnych ze zbioru i zastąpienie go przez jedną lub więcej sztucznych wartości / pseudonimów.

Pseudonimizacja jest procesem odwracalnym; dane osobowe ukryte za danymi spseudonimizowanymi mogą w każdej chwili zostać odzyskane, co wiąże się z konsekwencją możliwości identyfikacji tożsamości. Ogranicza jedynie możliwość tworzenia powiązań zbioru danych z prawdziwą tożsamością osoby, której dane dotyczą. Należy zaznaczyć, iż technika ta stanowi użyteczny środek bezpieczeństwa, ale nie metodę anonimizacji, lecz równocześnie jest ważnym elementem składowym procesu organizowania / projektowania danego procesu przetwarzania danych osobowych w sposób mający zapewnić ochronę prywatności podmiotów danych.

W efekcie pseudonimizacji nie otrzymamy anonimowego zbioru danych, jednakże dane wrażliwe zostają zabezpieczone i zmniejsza się ryzyko dla osób, których one dotyczą.

Stosowanie pseudonimizacji jest zasadne w następujących przypadkach, kiedy:

1) bezpośrednia identyfikacja podmiotu danych nie jest elementem koniecznym dla osiągnięcia celu przetwarzania danych (np. analiza i raportowanie), ale może być konieczna później;
2) dane osobowe są przetwarzane w dodatkowym celu, powiązanym z podstawowym celem przetwarzania (np. cel statystyczny) – w takich wypadkach dane osobowe powinny zostać spseudonimizowane zanim zostaną wykorzystane w drugorzędnym celu;
3) dane osobowe są przetwarzane w celach naukowych, historycznych lub statystycznych.

Metody pseudonimizacji danych osobowych

Pseudonimizacja obejmuje usunięcie lub ukrycie bezpośrednich identyfikatorów oraz w niektórych przypadkach, pewnych pośrednich identyfikatorów, które w kombinacji z pozostałymi danymi mogłyby ujawnić tożsamość jednostki. Wyeliminowane dane są później przechowywane w osobnej bazie, która może zostać połączona z utajnionymi danymi przy użyciu klucza, którym może być np. losowy numer identyfikacyjny lub inny pseudonim.

Techniczne środki umożliwiające zastosowanie pseudonimizacji:

1) szyfrowanie,
2) tokenizacja,
3) stosowanie skrótów.

Środki technicznie łącznie ze środkami organizacyjnymi (np. polityki, privacy by design) zapewniającymi separację spseudonimizowanych danych i klucza identyfikacyjnego, tworzą integralną

całość procesu pseudonimizacji. Powyższe techniki powinny być stosowane wyłącznie po konsultacji i przy wsparciu komórki właściwej ds. IT.

Proces pseudonimizacji:

Pracownik podejmuje decyzje odnoście rodzaju i zastosowania pseudonimizacji w uzgodnieniu z komórką ds. IT.

Komórka właściwa ds. IT ocenia możliwości techniczne oraz informuje na bieżąco o dostępnych dla danej czynności rozwiązaniach.

IOD rejestruje informacje w zakresie:

1) celu pseudonimizacji danego zbioru danych osobowych,
2) kategorii danych osobowych,
3) metoda pseudonimizacji,
4) data/czas pseudonimizowania,
5) wolumen danych osobowych.

Szyfrowanie

Proces przekształcania informacji uniemożliwiający dostęp do nich osobom innym niż ich dedykowany odbiorca poprzez wykorzystanie schematu kryptograficznego, który przekształca dane. Zaszyfrowane dane mogą zostać przywrócone do pierwotnej formy poprzez deszyfrowanie, możliwe wyłącznie wtedy, gdy odbiorca danych posiada wiedzę na temat wykorzystanego schematu szyfrowania oraz klucz deszyfrujący.

Szyfrowanie zapewnia zabezpieczenie na okoliczność:

1) poufności danych (zrozumiałe dla dedykowanego odbiorcy wyłącznie);
2) integralność danych (nieautoryzowana modyfikacja danych);
3) uwierzytelnienie danych (weryfikacja tożsamości osoby przetwarzającej dane);
4) autoryzacja danych (na podstawie uwierzytelnienia, algorytm przyznaje hasło lub udostępnia klucz wymagany do rozkodowania informacji);
5) niezaprzeczalność danych (przejrzystość w identyfikacji udostępniającego dane).

Stosowanie szyfrowania jest zasadne m.in. w następujących przypadkach:

Zawsze	Nie ma potrzeby	W zależności od potrzeb
- dane wrażliwe (np. dane dot. zdrowia); - numer identyfikacyjny (np. PESEL); - numer paszportu / dowodu osobistego; - dane finansowe (np. numer karty, kod CVC); - numer prawa jazdy.	- podstawowe informacje kontaktowe (np. imię, nazwisko, e-mail); - ID użytkownika.	Dane osobowe, których nie da się przypisać do pozostałych kategorii, powinny zostać oddzielnie przeanalizowane (metodą przypadek do przypadku). Należy wziąć pod uwagę następujące elementy: - analizę zysków i strat, - wolumen danych osobowych, które podlegających szyfrowaniu, - miejsce przetwarzania danych, - typ danych osobowych, -stosowane środki bezpieczeństwa, inne istotne elementy. Ocena powinna zostać dokonana przy wsparciu IOD oraz komórki ds. IT.

Kluczowe elementy procesu szyfrowania danych są następujące:

1) algorytm szyfrowania: matematyczna funkcja wykorzystywana do szyfrowania / deszyfrowania danych osobowych;
2) schemat szyfrowania: można wyróżnić dwa schematy szyfrowania - symetryczny oraz asymetryczny; schematy symetryczne używają tych samych kluczy szyfrujących zarówno do szyfrowania, jak i deszyfrowania, podczas gdy schematy asymetryczne wykorzystują odrębne klucze do szyfrowania i deszyfrowania danych;
3) klucz szyfrowania: informacja wykorzystywana przez algorytm szyfrujący w celu zaszyfrowania / odszyfrowania informacji. Analogicznie jak hasło podczas logowania do konta użytkownika, klucz szyfrowania musi być podany w celu odszyfrowania danych –

wprowadzenie nieprawidłowego kodu skutkuje zakodowaniem danych do nieczytelnej formy;

4) długość klucza: z góry ustalona długość klucza - im klucz jest dłuższy, tym jest on trudniejszy do złamania;
5) tryb działania szyfru blokowego.

Powyższa technika powinna być stosowana wyłącznie po konsultacji z i przy wsparciu komórki ds. IT. Proces szyfrowania dotyczy przesyłania danych osobowych przy użyciu poczty elektronicznej. Dane osobowe powinny być przesyłane w postaci zaszyfrowanego załącznika. Nie dopuszcza się przesyłania danych w treści maila lub w niezabezpieczonym pliku dołączonym do wiadomości. Pracownicy samodzielnie dokonują szyfrowania określonych danych, a w razie wątpliwości mogą skonsultować konieczność wykorzystania tej metody z komórką IT.

Załącznik nr 16. Procedura usuwania danych z nośników.

1. Definicje

Pojęcie/skrót	Definicja
UG	Urząd Gminy w Jedwabnie.
Administrator danych	Wójt Gminy Jedwabno
DBAN KillDisk	Specjalistyczne oprogramowanie przeznaczone do trwałego usuwania danych. **DBAN** jest aplikacją usuwającą wszystkie dane z dysku twardego. **KillDisk** także usuwa dane z dysku twardego (lub dysków twardych komputera) ale dodatkowo umożliwia całkowite usunięcie danych z wybranych katalogów na dysku twardym oraz umożliwia wygenerowanie raportu z procesu usunięcia danych.
Demagnetyzer	Urządzenie do nieodwracalnego usuwania danych z nośników magnetycznych przy pomocy silnego pola magnetycznego. Zastosowanie demagnetyzera do usunięcia danych z dysku twardego skutkuje uszkodzeniem układów elektronicznych dysku, co powoduję, że dysk nadaje się wyłącznie do utylizacji.
DMDE	Program do odzyskiwania danych
Komputer	Urządzenie elektroniczne przeznaczone do przetwarzania informacji, wyposażone m.in. w nośniki danych, np. komputer stacjonarny, serwer, laptop itp.
Likwidacja	Proces wycofania środka trwałego z użytkowania obejmujący jego usunięcie z ewidencji środków trwałych oraz utylizację. Likwidację przeprowadza komisja likwidacyjna.
Pamięć flash	Rodzaj pamięci pozwalającej na zapisywanie lub kasowanie wielu komórek pamięci podczas jednej operacji programowania. Jest to pamięć trwała, po odłączeniu zasilania nie traci zapisanych w niej danych. Pamięci FLASH są stosowane we wszelkich kartach pamięci oraz pamięciach USB
ASI, Administrator	Administrator Systemów Informatycznych

2. Cel dokumentu

Celem dokumentu jest określenie zasad usuwania informacji z nośników informatycznych przeznaczonych do utylizacji lub przekazania w celu dalszego użytkowania.

3. Odpowiedzialność

Za realizację procedury odpowiada ASI.

4. Zakres, warunki i wyłączenie stosowania

Procedurę stosuje się w Urzędzie Gminy w Jedwabnie przy usuwaniu danych z dysków twardych a także innych nośników, np. taśm, dyskietek, pamięci flash, w sytuacji, gdy sprzęt komputerowy lub nośniki przeznaczone są do utylizacji lub przekazania w celu dalszego użytkowania.

Procedura ma zastosowania do nośników zawierających informacje, które nie podlegają ochronie na mocy ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. nr 182 poz. 1228).
Procedura ma zastosowanie do nośników sprawnych i uszkodzonych.

4.1. Obszary bezpieczeństwa teleinformatycznego

Procedura określa działania w następujących obszarach związanych z bezpieczeństwem teleinformatycznym w zakresie wynikającym z Załącznika A do normy PN-ISO/IEC 27001:

A.9.2.6 - Bezpieczne zbywanie lub przekazywanie do ponownego użycia
A.10.7.1 - Zarządzanie nośnikami wymiennymi
A.10.7.2 - Niszczenie nośników
A.10.7.3 - Procedury postępowania z informacjami

5. Dokumenty związane

Polska Norma PN-ISO/IEC 27001.

6. Przebieg procedury

6.1. Zasady usuwania danych

- Oprogramowanie służące usuwaniu danych musi być użyte w taki sposób, aby nadpisana została cała powierzchnia nośnika. W przypadku **sprawnych** dysków twardych przeznaczonych do dalszego użytkowania, jeśli dysk zawiera informacje prawnie chronione (tj. dane osobowe, skarbowe itp.) lub nie ma pewności jakie dane zawiera, to konieczne jest co najmniej trzykrotne nadpisanie powierzchni nośnika z wykorzystaniem różnych wzorców zapisywanych danych.
- W przypadku braku możliwości przeprowadzenia pełnej procedury programowego usunięcia danych dysk należy przekazać do usunięcia danych z wykorzystaniem demagnetyzera lub zniszczyć fizycznie.
- Podczas wykorzystywania programów do usuwania informacji należy postępować zgodnie z instrukcjami wyświetlanymi na ekranie monitora.
- Proces usuwania danych powinien być realizowany z zachowaniem zasad bezpieczeństwa i higieny pracy na stanowisku pracy.
- Uszkodzone nośniki magnetyczne należy wymazywać, jeśli to możliwe, w demagnetyzerze a następnie przekazywać do likwidacji.
- Uszkodzone, zbędne lub zużyte nośniki CD/DVD należy przekazywać wyłącznie do likwidacji.

6.2. Proces usuwania danych

6.2.1. W procesie programowego usuwania danych z dysków twardych przeznaczonych do dalszego użytkowania należy stosować oprogramowanie DBAN lub KillDisk.

DBAN należy stosować w przypadku usuwania danych z wszystkich dysków twardych zamontowanych w komputerze i podłączonych przez port USB. W przypadku dysków twardych co do których jest pewność lub podejrzenie, że zawierają informacje prawnie chronione należy wybrać opcję „dodshort", która nadpisuje powierzchnię nośnika trzykrotnie: zerami, jedynkami i liczbami losowymi.

KillDisk należy stosować w przypadku usuwania danych z wybranych dysków twardych (można zaznaczyć kilka urządzeń) lub z pamięci flash. W celu uzyskania raportu z usunięcia danych należy kliknąć „Settings" na pasku narzędzi i zaznaczyć „Save erasing/wiping certificate to PDF" i „Display certificate after erasing/wiping". Aby usunąć dane należy w oknie „System local disks" wybrać dysk, który ma być wymazany, następnie kliknąć „Kill" na pasku narzędzi, następnie kliknąć „Start" i wpisać tekst „ERASE-ALL-DATA". Program w wersji darmowej nadpisuje powierzchnię nośnika jednokrotnie zerami.

a) Programowe usuwanie danych należy stosować, jeśli dysk twardy przeznaczony jest do dalszego użytkowania w Urzędzie Gminy lub do przekazania w celu dalszego użytkowania.
b) Usuwanie danych przy pomocy demagnetyzera należy stosować, jeśli dysk twardy jest uszkodzony lub przeznaczony do likwidacji.

6.2.2 Usuwanie danych z pamięci flash:

a) Jeśli nośnik jest sprawny, należy usunąć dane wykorzystując zalecany program do usuwania danych nadpisując trzykrotnie cały obszar pamięci;
b) Jeśli nośnik nie jest sprawny należy przeznaczyć go do utylizacji metodą fizycznego rozdrobnienia.

6.2.3 Usuwanie danych z innych nośników magnetycznych (taśmy, dyskietki):

a) Należy wykorzystać demagnetyzer do trwałego usunięcia danych, jeśli jest to z jakiegoś powodu niemożliwe należy fizycznie zniszczyć nośnik.

6.3. Weryfikacja usunięcia danych z dysków twardych.

W przypadku jakichkolwiek wątpliwości, co do poprawności przebiegu procesu usunięcia danych lub działania zastosowanego programu należy przeprowadzić weryfikację usunięcia danych, poprzez poddanie wymazanego nośnika analizie odczytu przy pomocy programu do odzyskiwania danych **DMIDE.**

Po wymazaniu dysku na całej powierzchni nośnika powinny znajdować się dane losowe lub cała powierzchnia nośnika powinna być wyzerowana. W przypadku pozostawienia na nośniku jakichkolwiek innych danych, w szczególności, jeśli część nośnika została wyzerowana a część zawiera jakieś dane, nawet losowe, proces usunięcia danych należy powtórzyć lub usunąć dane z dysku przy pomocy demagnetyzera.

6.4. Niszczenie nośników CD i DVD

Nośniki typu CD/DVD należy niszczyć przy pomocy niszczarek przeznaczonych do niszczenia tych nośników.

6.5. Sporządzenie protokołu z usunięcia danych

Usunięcie informacji musi być potwierdzone protokołem wykonanym wg wzoru w Załączniku nr 1 podpisanym przez:

1. Osoby, które w procesie likwidacji sprzętu użyją demagnetyzera w celu usunięcia informacji;
2. Osoby, które w ramach wykonywanych zadań używają oprogramowania specjalistycznego o którym mowa w procedurze w celu usunięcia informacji.
3. Osoby, które w procesie likwidacji sprzętu korzystały z działań fizycznego niszczenia nośnika.

Jeśli program zastosowany do usunięcia danych umożliwia utworzenie raportu z procesu usunięcia, to raport należy dołączyć do protokołu. Protokoły przechowywane są w wydziale, który dokonał usunięcia danych lub przez inne ciało na podstawie odrębnych regulacji.

7. Wyjątki w przebiegu procedury

Nie dotyczy.

8. Obowiązywanie procedury

8.1. Wejście w życie procedury

Procedura wchodzi w życie z dniem zatwierdzenia.

8.2. Termin obowiązywania

Bezterminowo.

8.3. Uregulowania przejściowe

Nie dotyczy.

9. Załączniki

Wzór protokołu trwałego usunięcia informacji.

Załącznik 1. Wzór protokołu trwałego usunięcia informacji.

Urząd Gminy w Jedwabnie, dnia.....

Protokół nr ..... /.....
trwałego usunięcia informacji

(*) Należy wpisać numer protokołu (nr kolejny / rok)

Pieczęć nagłówkowa

Stwierdza się, że w dniu .....w Urzędzie Gminy w Jedwabnie w pomieszczeniu nr .....
usunięto w sposób trwały informacje z niżej wymienionych nośników

Lp.	Typ nośnika (*)	Identyfikator (**)	Ilość (szt.)	Sposób usunięcia informacji (***)

(*) Należy podać typ nośnika (np. Dysk twardy, pamięć FLASH, taśma DDS4, nośnik optyczny CD, DVD itp.)
(**) W przypadku dysków twardych należy podać ich numery fabryczne i ew. numery inwentarzowe sprzętu, z którego pochodzą, jeśli są dostępne.
(***) W przypadku wykorzystania programu do wymazywania informacji należy podać nazwę programu i liczbę cykli nadpisywania powierzchni nośnika. W przypadku zastosowania demagnetyzera należy napisać „demagnetyzer" W przypadku fizycznego zniszczenia
nośnika należy podać sposób zniszczenia.

Informacje usunął w sposób trwały: .....
Imię i nazwisko Stanowisko

Stwierdza się, że informacje z wyżej wymienionych nośników usunięto trwale, w sposób uniemożliwiający odczytanie zapisanych na nich danych.

1. Imię i nazwisko ..... Stanowisko ..... Podpis.....
2. Imię i nazwisko ..... Stanowisko ..... Podpis.....
3. Imię i nazwisko ..... Stanowisko ..... Podpis.....

Załącznik 17. Zasady postępowania z pamięciami przenośnymi.

1. Cel i zakres zasad

Niniejsze zasady określają sposób przyznawania i używania pamięci przenośnych, o której mowa w § 2 ust.1. pkt 5. Niniejsze zasady dotyczą również krótkotrwałego przenoszenia informacji, zawierających dane osobowe sporządzane na podstawie informacji zawartych w zbiorach osobowych prowadzonych w systemach informatycznych w Urzędzie Gminy.

2. Definicje i określenia używane w zarządzeniu

Pojęcie/skrót	Definicja
UG	Urząd Gminy w Jedwabnie.
Administrator danych	Wójt Gminy Jedwabno
IOD	Inspektor Ochrony Danych osoba realizujący zadania określone w Ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. poz. 1000, dalej zwanej ustawą lub u.o.d.o.) oraz Rozporządzeniu Parlamentu Europejskiego i Rady 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
ASI	Informatyk, realizujący zadania związane z informatyzacją w Urzędzie Gminy
Użytkownik	Pracownik Urzędu Gminy, któremu przyznano i przekazano do użytkowania służbową pamięć przenośną (dysk zewnętrzny lub Pendrive)
Pamięć „Pendrive", dysk przenośny	Urządzenie, które nie jest na stałe połączone z komputerem (jednostką centralną), służące do przechowywania i przenoszenia danych, do których odczytywania bądź zapisywania konieczne jest użycie odpowiedniego innego urządzenia, podłączane poprzez interfejs USB. Wszystkie dostępne dla użytkownika nośniki zewnętrzne muszą być zaszyfrowane a za ten proces odpowiada ASI
Likwidacja	Proces wycofania środka trwałego z użytkowania obejmujący jego usunięcie z ewidencji środków trwałych oraz utylizację. Likwidację przeprowadza komisja likwidacyjna.
Pamięć flash	Rodzaj pamięci pozwalającej na zapisywanie lub kasowanie wielu komórek pamięci podczas jednej operacji programowania. Jest to pamięć trwała, po odłączeniu zasilania nie traci zapisanych w niej danych. Pamięci FLASH są stosowane we wszelkich kartach pamięci oraz pamięciach USB

Wymagania podane w dokumencie spełniają zalecenia zawarte w normie PN-ISO/IEC 27001 w zakresie wskazanym w punkcie 8,11, 12, 18.

3. Zasady przyznawania służbowych pamięci przenośnych.

1. Pracownik zwraca się pisemnie do ASI o przyznanie i przekazanie jej służbowej pamięci przenośnej.
2. Pamięci przenośne pozostają na stanie osoby zatrudnionej.
3. ASI przekazuje urządzenie osobie wnioskującej o przydzielenie pamięci zewnętrznej po zapoznaniu ich z postanowieniami niniejszych zasad oraz po zaszyfrowaniu. Hasło szyfrowania ASI przekazuje wraz z instrukcją zmiany hasła.
4. ASI nadaje pamięciom przenośnym unikalny numer ewidencyjny.
5. Fakt przekazania pamięci przenośnej użytkownikowi poświadcza się w druku oświadczenia, którego wzór określa załącznik nr 1, do niniejszych zasad.
6. Oryginał oświadczenia, o którym mowa w ust.5 przechowuje ASI, Kopię oświadczenia otrzymuje użytkownik.
7. Użytkownik jest zobowiązany do przestrzegania warunków gwarancji powierzonej pamięci w szczególności do zachowania oryginalnego opakowania, jeżeli wymaga tego umowa gwarancyjna.
8. Użytkownik jest zobowiązany do rozliczenia się z powierzonej pamięci podczas kontroli inwentaryzacyjnej lub na wezwanie przełożonego.

9. Użytkownik zdaje pamięć ASI w przypadku rozwiązania umowy o pracę, zmiany wydziału lub oddelegowania go do innej pracy.
10. Uszkodzoną pamięć należy przekazać do ASI wraz ze zgłoszeniem, którego wzór stanowi załącznik nr 2 do niniejszych zasad.
11. W przypadku nieodwracalnego uszkodzenia pamięć zostaje zniszczona przez ASI.
12. W przypadku utracenia pamięci użytkownik o tym fakcie niezwłocznie zawiadamia pisemnie IOD i ASI.
13. Po otrzymaniu pisemnego powiadomienia o utraceniu pamięci przenośnej IOD przeprowadza czynności wyjaśniające, a po ich zakończeniu przedstawia wnioski Administratorowi danych.
14. W przypadku utracenia lub uszkodzenia pamięci IOD przeprowadza postępowanie wyjaśniające w celu ustalenia czy do zdarzenia doszło z winy użytkownika. Użytkownik, z którego winy doszło do utracenia lub uszkodzenia pamięci przenośnej ponosi odpowiedzialność materialną oraz cywilną.

4. Zasady eksploatacji pamięci przenośnych.
1. Służbowe pamięci przenośne służą do przechowywania i przenoszenia wyłącznie danych zawierających informacje służbowe, przechowywane wyłącznie w obszarze szyfrowanym dysku.
2. Pamięć przenośna winna być przechowywana w sposób uniemożliwiający dostęp do niej osobom niepowołanym.
3. Pamięć przenośna winna być chroniona przed utratą lub uszkodzeniem (np. na skutek uderzenia, a także wystawienia na działanie wysokich temperatur, wilgoci, agresywnych środków chemicznych, silnych pól magnetycznych).
4. Przenoszenie danych służbowych za pomocą pamięci przenośnych poza teren Urzędu Gminy jest dopuszczalne wyłącznie w celach służbowych za zgodą Administratora lub w przypadku posiadania pisemnej zgody na używanie nośnika poza siedzibą.
5. Pamięć przenośną należy sprawdzać oprogramowaniem antywirusowym na obecność wirusów lub innego szkodliwego oprogramowania.
6. Do pamięci przenośnych, z których dane zostały usunięte nadal stosuje się zalecenia określone w ust. 2 i 3. Standardowe usunięcie danych nie powoduje ich fizycznego, trwałego skasowania.
7. Przed przekazaniem pamięci przenośnej innemu użytkownikowi zawarte w niej dane należy zarchiwizować (o ile zachodzi taka potrzeba), a następnie usunąć za pomocą programu służącego do trwałego kasowania zawartości danych.
8. Do celów służbowych nie wolno używać prywatnych pamięci przenośnych.
9. Zabrania się stosowania pamięci przenośnych do wykonywania kopii zapasowych danych przetwarzanych na twardych dyskach komputerów służbowych. Pamięć przenośna może być traktowana jedynie jako krótkotrwały nośnik danych wytwarzanych w systemie komputerowym, a po wykorzystaniu dane te powinny być z niej usunięte.

5. Kontrola pamięci przenośnych

Pamięci przenośne podlegają kontroli przeprowadzanej przez ASI. Dostęp do pamięci przenośnej w przypadku nieobecności użytkownika musi posiadać przełożony.

Załącznik nr 1 do zasad postępowania z pamięciami przenośnymi

O Ś W I A D C Z E N I E

Oświadczam, że zapoznałem się z Polityką Bezpieczeństwa Urzędu Gminy w zakresie postępowania z pamięciami przenośnymi w Urzędzie Gminy w Jedwabnie wraz z załącznikiem do niego i zobowiązuję się przestrzegania jego postanowień.

w odniesieniu do powierzonej mi pamięci typu .....numer .....

....
Podpis ASI Podpis pracownika

Załącznik nr 2 *do zasad postępowania z pamięciami przenośnymi*

(miejscowość i data)
Administrator Systemów Informatycznych

ZGŁOSZENIE

Informuję, że w dniu w trakcie wykonywania czynności służbowych uszkodziłem/am lub utraciłem/am* przenośną pamięć typu: .....
o numerze .....
Powyższa pamięć została .
uszkodzona bądź utracona* w następujących okolicznościach:

.....

.....
Jednocześnie zobowiązuję się do natychmiastowego zwrócenia pamięci w przypadku jej odnalezienia.

.....
(data i podpis użytkownika)

Potwierdzenie odbioru zgłoszenia:
ASI -.....

Załącznik nr 3 do zasad postępowania z pamięciami przenośnymi

Wniosek

Oświadczam, że zapoznałem się z Polityką Bezpieczeństwa Urzędu Gminy w zakresie postępowania z pamięciami przenośnymi w Urzędzie Gminy w Jedwabnie wraz z załącznikiem do niego i zobowiązuję się przestrzegania jego postanowień w odniesieniu do powierzonej mi pamięci typu .....numer .....

Proszę o wyrażenie zgody na .....

....
Podpis ASI Podpis pracownika

Opinia Administratora: .....

Załącznik nr.18. Procedura zgłaszania incydentów informatycznych.

Definicje.

UG	Urząd Gminy
CSIRT NASK	CERT Polska zostały powierzone obowiązki CSIRT NASK wynikające z ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. 1560)
Incydent bezpieczeństwa	Niepożądane zdarzenie związane z dostępem do Internetu lub seria zdarzeń, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji.
Kwalifikacja incydentu	Oznaczenie kategorii incydentu i podjęcie decyzji o zgłoszeniu incydentu do CERT (zgodnie z legendą do załącznika 1 oraz aktualnymi zaleceniami)
ASI	Administrator Systemu Informatycznego

2 CEL DOKUMENTU

Celem procedury jest określenie zasad zgłaszania incydentów bezpieczeństwa do CERT NASK.

3 ODPOWIEDZIALNOŚĆ

Procedura realizowana jest przez osoby odpowiedzialne za kwalifikację i zgłaszanie incydentów bezpieczeństwa do zespołu CERT. Za realizację tego zadania w jednostce odpowiadają osoby wskazane przez kierownika jednostki oraz ASI.

4 ZAKRES I WARUNKI STOSOWANIA

Incydent w podmiocie publicznym to incydent, który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez podmiot publiczny, o którym mowa w art. 4 pkt 7–15 ustawy z dnia 5 lipca 2018 (Dz. U. poz 1560) o krajowym systemie cyberbezpieczeństwa. Zgodnie z ustawą z dnia 5 lipca 2018 (Dz. U. poz. 1560) o krajowym systemie cyberbezpieczeństwa.
Urząd Gminy jest jednostką zobowiązaną do zgłaszania incydentów. Realizacja obowiązku odbywa się poprzez wypełnienie zgłoszenia na stronie https://incydent.cert.pl/.

Procedurę stosuje się w przypadku wykrycia incydentu bezpieczeństwa w systemie informatycznym.
Do CSIRT NASK należy zgłaszać wszelkie działania zagrażające i/lub naruszające bezpieczeństwo
sieciowe systemów teleinformatycznych w domenie jedwabno.pl a także innych systemów należących do Urzędu Gminy, np. stron www, hostowanych przez operatorów zewnętrznych. W szczególności należy zgłaszać:

- włamania lub próby włamań,
- ograniczanie dostępności zasobów sieciowych (np. ataki typu DoS - Denial Of Service),
- działania z użyciem kodów złośliwych (np. rozsyłanie wirusów),
- skanowania,
- rozpowszechnianie nielegalnych treści,
- inne ważne przypadki naruszenia bezpieczeństwa teleinformatycznego.

Wymagania podane w dokumencie spełniają zalecenia zawarte w normie PN-ISO/IEC 27001 w zakresie wskazanym w punkcie 16.

5 DOKUMENTY ZWIĄZANE

Dokumenty udostępnione na https://incydent.cert.pl/
- formularz zgłoszenia incydentów,
- formularz zgłoszenia osób do kontaktów z CSIRT NASK,

6 PRZEBIEG PROCEDURY

1. Należy prowadzić ewidencję incydentów bezpieczeństwa, zgodnie z wzorem w załączniku 1. Ewidencję incydentów prowadzą komórki właściwe do zarządzania bezpieczeństwem teleinformatycznym.
2. Osoba odpowiedzialna za kwalifikację incydentów do zgłoszenia do CERT klasyfikuje incydent (zgodnie z legendą w załączniku 1) i decyduje czy incydent podlega zgłoszeniu do CERT.
3. Jeśli incydent nie podlega zgłoszeniu do CERT, to należy to zaznaczyć w ewidencji incydentów zgodnie z legendą w załączniku 1. Dalsze działania dotyczące zgłoszenia do CERT, określone w punkcie 4 nie są podejmowane.
4. Jeśli incydent podlega zgłoszeniu do CERT to należy postępować zgodnie z aktualnymi zaleceniami CERT NASK.

Załącznik 1

Wzór

Pieczątka z nazwą
jednostki organizacyjnej

Ewidencja incydentów

LP	Opis incydentu	Nazwa systemu i/lub usługi	Kateg. Incydentu	Wykrycie			Podjęcie działań		Data za-mknięcia incydentu	Kwalifikacja zgłoszenia do CERT			Data zgłoszenia do CERT	Zgłoszenie do ADOI	Uwagi
				Data	Godz.	Czas trwania	Data	Godz.		T/N	Data	Imię i Nazwisko			
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

Legenda:

W kol. 3 należy podać nazwę systemu i/lub usługi, w którym wystąpił incydent.

W kol. „kategoria incydentu" należy podać jedną lub więcej z poniższych kategorii:

1. Obraźliwe i nielegalne treści,
2. Złośliwe oprogramowanie,
3. Gromadzenie informacji,
4. Próby włamań,
5. Włamania,
6. Ataki na dostępność zasobów,
7. Atak na bezpieczeństwo informacji,
8. Oszustwa komputerowe,
9. Inne.

Jeśli incydent został zakwalifikowany do zgłoszenia do CERT, to w kol. 11 należy wpisać T, w przeciwnym wypadku N

Uwaga:

Numer incydentu w kolumnie LP powinien odpowiadać numerowi teczki z dokumentacją incydentu.

Załącznik nr 19. Procedura przygotowania stanowiska komputerowego przeznaczonego dla Rady Gminy oraz usuwania danych audio.

ZAKRES I WARUNKI STOSOWANIA

Procedura ma charakter ogólny, jednak w kilku aspektach precyzuje minimalne wymagania, które powinny zostać spełnione. Wymagania podane w dokumencie spełniają zalecenia zawarte w normie PN-ISO/IEC 27001 w zakresie wskazanym w punkcie 11, 12, 14.

POSTANOWIENIA OGÓLNE

- Użytkownik stanowiska komputerowego na którym przechowywane są dane musi posiadać własne konto lokalne bez uprawnień administracyjnych, na którym może pracować z zachowaniem rozliczalności działań podejmowanych w systemie.
- Pracownikowi nie wolno ingerować w konfigurację sprzętową stacji roboczej.
- Pracownikowi nie wolno samodzielnie instalować na stacji roboczej oprogramowania (w tym dodatków do przeglądarek), ani używać aplikacji w wersji portable (programów nie wymagających instalacji, przenoszonych na różnych nośnikach pamięci).
- Administrator Systemów Informatycznych konfiguruje stanowisko komputerowe zgodnie z następującymi zasadami:

- Obowiązuje zakaz podłączania zdalnego do zasobów pracownika w jakiejkolwiek formie. Wszystkie działania informatyczne na zasobach pracownika odbywają się w jego obecności;
- Wszystkie operacje dostępu do zasobów pracownika muszą być wykonywane za jego wiedzą i zgodą.
- Stosuje się zasadę, że wszystkie logi komputera administrator przechowuje przez okres minimum 2 lat.

Logi systemowe muszą zachowywać **co najmniej** następujące informacje: uruchomienie i wyłączenie komputera, zalogowanie i wylogowanie użytkownika, podłączanie zewnętrznych nośników informacji, wszystkie aspekty zdalnego podłączenia do komputera, kopiowanie lub próby kopiowania zbiorów, usuwanie lub próby usuwania zbiorów. Konieczne jest włączenie: inspekcji użycia uprawnień, inspekcji zarządzania kontami, inspekcji dostępu do obiektów, inspekcji zmian zasad, konto gościa musi być wyłączone, wyłączona jest możliwość zmiany nazwy konta gościa i administratora, włączona opcja „wyczyść plik stronicowania pamięci wirtualnej".

- W przypadku zastosowania przenośnej jednostki komputerowej obowiązuje obowiązek szyfrowania partycji dyskowych np. z wykorzystaniem BitLockera. Kopię hasła szyfrowania ASI przekazuje Administratorowi Danych. Fakt przekazania hasła ASI dokumentuje w dzienniku systemu.
- Administrator Danych przechowuje także aktualną kopię hasła administratora komputera, którą otrzymuje od ASI po każdej zmianie. Administrator Danych może podjąć decyzję o przechowywaniu hasła przez inną osobę. Fakt przekazania hasła ASI dokumentuje w dzienniku

systemu. Zasady tworzenia haseł, przechowywania i niszczenia określa procedura „***Zasady tworzenia haseł administratorów***".

- Zewnętrzne nośniki informacji podłączane do jednostki komputerowej spełniają wymagania zawarte w dokumencie *Zasady postępowania z pamięciami przenośnymi w Urzędzie Gminy w Jedwabnie*

TREŚĆ PROCEDURY

PRZYGOTOWANIE STANOWISKA KOMPUTEROWEGO

Administrator Systemów Informatycznych przygotowuje stanowisko komputerowe do pracy, przekazuje je do eksploatacji, przeprowadza szkolenie stanowiskowe pracownika a także wskazuje materiały przydatne do prawidłowej eksploatacji stacji roboczej. Fakt przygotowania stanowiska potwierdza protokołem, który stanowi *Załącznik 1* do niniejszej procedury.

STANDARDOWE WYPOSAŻENIE STANOWISKA KOMPUTEROWEGO

Użytkownik stacji roboczej zostaje wyposażony w sprzęt i oprogramowanie adekwatne do zakresu wykonywanych obowiązków, minimalne wymagania określone są w punktach 7.1 i 7.2.

SPRZĘT

- **Jednostka komputerowa;**
- **Klawiatura;**
- **Mysz.**

W przypadku zastosowania urządzenia przenośnego klawiatura i mysz są urządzeniami opcjonalnymi.

OPROGRAMOWANIE

- **System operacyjny** – zaktualizowany system operacyjny z rodziny MS Windows w wersji PRO;
- **Open Office lub inny edytor**– najbardziej aktualna stabilna wersja oprogramowania;
- **Przeglądarka internetowa** – Internet Explorer/Edge adekwatny do wersji systemu operacyjnego i/lub alternatywna przeglądarka np. Mozilla Firefox;
- **Przeglądarka plików pdf** – np. Adobe Reader;
- **Kompresor plików** – np. 7 Zip;
- **Oprogramowanie antywirusowe (aktualizowane na bieżąco)**;
- **Podłączenie drukarek** – zainstalowanie drukarek (podstawowej i alternatywnej) umożliwiające użytkownikowi wydrukowanie dokumentów w przypadku, gdy zachodzi taka konieczność.

ASI umożliwia nowemu użytkownikowi korzystanie ze skonfigurowanej stacji roboczej.

W celu uzyskania dostępu do pozostałych zasobów informatycznych (indywidualny dostęp do systemu operacyjnego, wybranych aplikacji użytkowych) należy zastosować *Procedurę*

postępowania w zakresie nadawania/odbierania uprawnień do systemów informatycznych zawartą w *Polityce Bezpieczeństwa w Załączniku nr 3.*

DOKUMENTOWANIE ZLECEŃ WYKONANIA ZADANIA

ASI ewidencjonuje dokument potwierdzający skonfigurowanie stacji roboczej do pracy po potwierdzeniu przez Administratora Danych zapoznania się z dokumentem (*Załącznik 1*).

CZAS REALIZACJI ZADANIA

Stanowisko komputerowe powinno zostać przygotowane/dostosowane do eksploatacji w możliwie najkrótszym czasie.

SPOSÓB USUWANIA DANYCH

W sytuacji, gdy przechowywany plik audio nie jest już niezbędny, stworzony na jego podstawie dokument tekstowy został podpisany, pracownik po uzyskaniu zgody Administratora Danych usuwa zbiór audio z wykorzystaniem aplikacji do kasowania plików i folderów bez późniejszej możliwość ich odzyskania. Pracownik prowadzi rejestr usuniętych zbiorów stanowiący *Załącznik nr 2* do dokumentu.

Załącznik 1. Protokół konfiguracji stacji roboczej oraz przeszkolenia pracownika.

W dniu ..... w Urzędzie Gminy w Jedwabnie Administrator Systemów Informatycznych przekazał do eksploatacji stację roboczą (nr inwentarzowy .....). Jednostka komputerowa została skonfigurowana do pracy zgodnie z dokumentem „Procedura Przygotowania stanowiska komputerowego oraz usuwania danych audio".

.....

(data, imię i nazwisko)

W dniu ..... W Urzędzie Gminy w Jedwabnie Administrator Systemów Informatycznych przeszkolił .....
(imię i nazwisko)
do pracy na stacji roboczej przeznaczonej do obsługi Rady Gminy.
Szkolenie zawierało następujące elementy:
- *bezpieczne posługiwanie się komputerem,*
- *zasady tworzenia haseł,*
- *zasady korzystania z zewnętrznych nośników informacji,*
- *obsługa aplikacji do kasowania plików i folderów bez późniejszej możliwość ich odzyskania.*

Szkolenie trwało: .....

.....

(data, imię i nazwisko ASI)

.....

(data, imię i nazwisko)

Załącznik 2. Wzór rejestru usuniętych zbiorów audio.

Dokument prowadzi pracownik odpowiedzialny za obsługę Rady Gminy.

Data dokumentu audio.	Data przyjęcia protokołu wytworzonego z wykorzystaniem dokumentu audio.	Podpis osoby zezwalający na usunięcie zbiorów.	Data usunięcia zbiorów, podpis osoby wykonującej.	UWAGI

Załącznik nr.20. Procedura usuwania oprogramowania typu BOTNET.

1. Definicje

Słownik pojęć i skrótów

Pojęcie/skrót	Definicja
BOT (KOMPUTER ZOMBIE)	Urządzenie/komputer zainfekowany złośliwym oprogramowaniem, ·które pozwala na wykonywanie operacji bez wiedzy i zgody użytkownika oraz może służyć do wykradania jego poufnych danych.
BOTNET	Sieć zbudowana z zainfekowanych komputerów (zombie, botów), nad którymi kontrolę sprawuje serwer C&C (bot master). Przejęcie kontroli nad komputerami wykorzystywane jest do działań takich jak, rozsyłanie spamu, bądź realizacja ataków na inne systemy teleinformatyczne.
UG	Urząd Gminy w Jedwabnie
ASI	Administrator Systemów Informatycznych
Ochrona AV	Oprogramowanie chroniące system i pliki użytkownika przed destrukcyjnym działaniem złośliwego oprogramowania. Program zaprojektowany do wykrywania wirusów i złośliwego oprogramowania oraz do podejmowania lub zalecania działania naprawczego. Jego celem jest także zabezpieczanie systemów operacyjnych przed działaniem ww. zagrożeń.
IOD	Inspektor Ochrony Danych
Administrator danych	Wójt Gminy Jedwabno.

2. Cel dokumentu

Celem niniejszego dokumentu jest określenie procedury usuwania złośliwego oprogramowania z komputerów zidentyfikowanych jako Boty - opisuje ona sposób usunięcia/wyłączenia ich z sieci *Botnet,* a tym samym zapewnienia bezpieczeństwa danych przetwarzanych na tych komputerach.

Niniejsza procedura dotyczy działań w następujących obszarach związanych z bezpieczeństwem teleinformatycznym (norma PN-ISO/IEC 27001 - Załącznik A): 10.

3. Odpowiedzialność

Za stosowanie zasad zawartych w niniejszym dokumencie odpowiadają:

1) Administrator Systemów Informatycznych, w zakresie realizacji i kontroli nad bezpieczeństwem danych przetwarzanych przez komputery.
2) IOD w zakresie weryfikacji skutków ochrony danych.

4. Zakres, warunki i wyłączenie stosowania

Niniejszą procedurę należy stosować w celu usuwania złośliwego oprogramowania z komputerów zidentyfikowanych jako Boty. Procedury nie stosuje się do systemów informatycznych przetwarzających informacje niejawne w myśl ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U.2010.182.1228 z późn. zm.).

5. Dokumenty związane

Brak.

6. Procedura usuwania złośliwego oprogramowania z urządzeń zidentyfikowanych jako Boty

Po pozyskaniu informacji o prawdopodobnym zainfekowaniu komputera (informacja zawierać powinna adres IP zainfekowanego komputera oraz nazwę *Botnetu*) zaleca się odłączenie go od sieci LAN. Ponadto ASI zobowiązany jest do podjęcia następujących działań:

1. Sprawdzić, czy na komputerze jest zainstalowane i aktywne resortowe oprogramowanie antywirusowe. W przypadku stwierdzenia braku oprogramowania należy:
   a. dokonać jego instalacji;
   b. uaktywnić - jeśli oprogramowanie jest nieaktywne (np. właściwy w tym zakresie proces został zatrzymany);
   c. dokonać aktualizacji bazy sygnatur wirusów;

   Po wykonaniu powyższych czynności należy przeprowadzić pełne skanowanie komputera.

   Jeżeli czynności wymienione w punkcie 1 nie doprowadziły do wykrycia i usunięcia oprogramowania typu Botnet, należy odinstalować oprogramowanie antywirusowe, a następnie zrealizować kolejne punkty tej procedury;

2. Wykorzystując nazwę Botnetu przekazaną w informacji o prawdopodobnym zainfekowaniu komputera, należy przeszukać sieć Internet w celu zweryfikowania czy istnieją dedykowane dla konkretnego zagrożenia narzędzia;
3. W przypadku braku dedykowanych rozwiązań mających na celu usunięcie konkretnego oprogramowania typu Botnet należy pobrać, a następnie zapisać na dysku twardym zainfekowanego komputera ogólnodostępne oprogramowanie do usuwania złośliwego oprogramowania, które pobrać można np. z poniższych adresów:
   a. http://www.mcafee.com/uk/downloads/free-tools/stinger.aspx;
   b. *http://www. Symantec. com/pl/pl/products-solutions/trialware/?pcid=pcat security,*
   c. *http://www. trendmicro. pl/products/free-tools-and-services/index, htmk*
   d. *http://kaspersky-av.pl/index.php/do pobrania/;*
   e. http://www.eset.pl/Pobierz.

   Wymienione powyżej adresy z oprogramowaniem do zwalczania oprogramowania typu Botnet są tylko przykładowymi do wykorzystania. Specyfika tego typu oprogramowania złośliwego nie daje jednak pewności, że wymienione narzędzia będą skuteczne w przypadku każdego zagrożenia tego typu.
4. Następnie należy:
   a. wyłączyć przywracanie systemu;
   b. uruchomić komputer w trybie awaryjnym;
5. Po wykonaniu czynności opisanych w rozdziałach od 6.1. do 6.3. niniejszej procedury należy uruchomić komputer w trybie normalnym oraz ponownie zainstalować (jeśli zostało odinstalowane) resortowe oprogramowanie antywirusowe;
6. Zaleca się powtórzenie działań opisanych w rozdziałach 6.1. do 6.3. niniejszej procedury przy wykorzystaniu kilku narzędzi do usuwania złośliwego oprogramowania.

6.1. Weryfikacja obecności złośliwego oprogramowania

W celu zabezpieczenia próbki z zainfekowanym oprogramowaniem ze stacji zidentyfikowanej jako Bot należy postępować zgodnie z poniższym schematem, który został przedstawiony na przykładzie narzędzia *Stinger.*

1. Gdy pojawi się monit, należy wybrać przycisk *Save*, aby zapisać plik w dogodnej lokalizacji na dysku twardym.
2. Po zakończeniu pobierania należy przejść do folderu, w którym został zapisany plik Stinger32.exe, a następnie należy go uruchomić.
3. Po uruchomieniu pliku należy zaakceptować warunki licencji poprzez wybranie przycisku *Accep*t.
4. Następnie w celu konfiguracji skanowania należy wybrać opcję Advanced, a następnie należy wybrać *Settings*.
5. W polu ustawień należy skonfigurować narzędzie zgodnie z poniższym rysunkiem (ważne, aby w tym kroku procedury wybrana została opcja Report), a następnie należy wybrać przycisk *Save*. Należy wybrać przycisk *Customize my scan.*
6. Następnie należy zaznaczyć opcję Mój komputer w celu przeskanowania całej przestrzeni pamięci zainfekowanego komputera.
7. Po dokonaniu powyższych czynności należy uruchomić przycisk Scan w celu sprawdzenia komputera pod kątem obecności złośliwego oprogramowania.
8. Po zakończeniu procesu skanowania należy przejść do sekcji *Log*, w której należy odszukać i przeanalizować plik wskazujący na przeprowadzone przed chwilą skanowanie.

Zabezpieczenie próbki z zainfekowanym oprogramowaniem

W przypadku, gdy w wyniku realizacji działań wymienionych w rozdziale 6.1. zidentyfikowano infekcję skanowanego komputera, należy zidentyfikować poziom zagrożenia i jeśli spełnione są warunki należy dokonać zgłoszenia zgodnie z procedurą zgłaszania incydentów informatycznych.

6.2. Usuwanie złośliwego oprogramowania

Jeżeli w wyniku działań wykonanych zgodnie z rozdziałem 6.1. na sprawdzanym komputerze zidentyfikowano złośliwe oprogramowania, po wykonaniu czynności opisanych w rozdziale 6.2. należy wykonać działania mające na celu usunięcie go. W tym celu należy:

1. Wykonać czynności opisane w punktach od 3 do 5 rozdziału 6.1 niniejszej procedury;

2. W polu ustawień skonfigurować narzędzie zgodnie z poniższym rysunkiem (ważne, aby w tym kroku procedury wybrana została opcja ***Repair*** - narzędzie *Stinger* domyślnie naprawi wszystkie pliki zidentyfikowane przez niego jako zainfekowane), a następnie należy wybrać przycisk *Save.*
3. Następnie należy wykonać czynności opisane w punktach od 7 do 9 rozdziału 6.1 niniejszej procedury w celu uruchomienia procesu skanowania zainfekowanego komputera.
4. Po zakończeniu procesu skanowania narzędzie wyświetli informację o przeskanowanych plikach oraz podjętych działaniach w celu usunięcia zidentyfikowanych zagrożeń.

W przypadku, gdy mimo zastosowania różnych narzędzi do usuwania złośliwego oprogramowania nie udało się skutecznie usunąć infekcji, należy sformatować dysk twardy komputera wraz z zastosowaniem nowego podziału na partycje, a następnie ponownie zainstalować system operacyjny. Przedmiotową czynność należy poprzedzić backupem dokumentów oraz poczty (jeśli nie zostały zainfekowane).

6.3. Działania po usunięciu złośliwego oprogramowania

Po zakończeniu procesu usuwania szkodliwego oprogramowania z komputera zidentyfikowanego jako Bot, należy w trybie natychmiastowym przekazać niezwłocznie Administratorowi Danych Osobowych oraz IOD następujące informacje:

- Czy zainfekowany komputer pracował również poza siecią LAN;
- Nazwa i rodzaj wykrytego szkodliwego oprogramowania;
- Jakie narzędzia zostały wykorzystane do usunięcia szkodliwego oprogramowania;
- Przypisanie nazwy szkodliwego oprogramowania do nazwy narzędzia, przy pomocy którego udało się usunąć to oprogramowanie;
- Opis pozostałych działań, które zostały podjęte w celu usunięcia szkodliwego oprogramowania;
- Uwagi dotyczące zagrożeń, które mogło spowodować zainfekowanie złośliwym oprogramowaniem.

7. Wyjątki w przebiegu procedury

Nie przewiduje się wyłączenia w stosowaniu niniejszej procedury.

8. Załączniki

Brak.

Załącznik nr .21 Instrukcja postępowania z kluczami kryptograficznymi oraz certyfikatami.

1. Kryptografia

1.1. Stosowanie zabezpieczeń kryptograficznych

Zabezpieczenia kryptograficzne stosowane są w szczególności dla:

a. Zabezpieczenia danych znajdujących się na komputerach przenośnych, przenośnych nośnikach danych i urządzeniach mobilnych takich jak smartphony, tablety itp. Dostęp do tych urządzeń powinien być realizowany po podaniu loginu i hasła, hasła lub użycia klucza kryptograficznego zapisanego na urządzeniu zewnętrznym.
b. Zabezpieczania połączeń zdalnych do infrastruktury jednostki za pośrednictwem kanałów cyfrowych VPN. W tym przypadku zależnie od konfiguracji sprzętowej i oprogramowania należy stosować protokoły SSL/TLS lub SSH.
c. Bezpiecznego logowania przez sieć Internet do usług administrowanych przez podmioty trzecie. W tym przypadku zależnie od konfiguracji sprzętowej i oprogramowania należy wykorzystywać dostęp https oraz protokoły SSL.
d. Do przesyłania danych przy użyciu poczty elektronicznej. W przypadku przesyłania danych osobowych których ujawnienie może powodować ryzyko lub wysokie ryzyko naruszenia praw i wolności podmiotów danych, przesyłane pliki należy szyfrować przy użyciu dostępnych w jednostce programów np. 7zip, a hasło do pliku należy przekazać odbiorcy innym kanałem komunikacji. Wykorzystywany dostęp do poczty elektronicznej poprzez strony www. powinien być realizowany wyłącznie dla stron zabezpieczonych protokołem SSL oraz posiadających oznaczenie https i ważny podpisany certyfikat.

1.2. Zarządzanie kluczami kryptograficznymi

1. Za prawidłowe zarządzanie kluczami kryptograficznymi odpowiada ASI.
2. Klucze kryptograficzne generowane są i wykorzystywane zgodnie z zaleceniami i instrukcjami udostępnionymi przez dostawcę oprogramowania kryptograficznego, oprogramowania wykorzystującego zabezpieczenia kryptograficzne.
3. Kopie wykorzystywanych kluczy kryptograficznych (prywatnych lub/i publicznych) zapisywane są na zabezpieczonym zewnętrznym nośniku danych, który przechowywany jest w szafie pancernej lub sejfie dostępnych w jednostce.
4. Dostęp do nośnika danych, na którym zapisane są klucze kryptograficzne możliwy jest tylko przez ASI i kierownika jednostki.
5. Wykorzystywane klucze kryptograficzne zmieniane są zawsze w momencie:
   a. zauważenia incydentu związanego z bezpieczeństwem stosowanych rozwiązań kryptograficznych,
   b. w sytuacji podejrzenia ujawnienia klucza osobie nieuprawnionej,
   c. zakończenia współpracy z osobą realizującą zadania na podstawie umowy o pracę, umowy cywilnoprawnej lub innego instrumentu prawnego, która miała dostęp do kluczy kryptograficznych.

1.3. Obowiązki użytkowników kluczy kryptograficznych

1. Klucze kryptograficzne wydane użytkownikom (upoważnionym pracownikom jednostki) na zewnętrznych nośnikach danych (np. karty kryptograficzne kwalifikowanego podpisu elektronicznego) są ewidencjonowane przez ASI.
2. Wzór ewidencji stanowi załącznik nr 1 do niniejszej instrukcji.
3. Każdy użytkownik odpowiada za bezpieczeństwo otrzymanego klucza w tym za:

a. nieujawnianie haseł, kodów PIN i PUK nadanych w celu umożliwienia autoryzacji wykorzystania klucza kryptograficznego,
b. zmiana haseł, kodów PIN i PUK nadanych w celu umożliwienia autoryzacji wykorzystania klucza kryptograficznego zgodnie z zaleceniami dostawcy,
c. nieudostępnianie nośnika wraz z kluczem osobom nieuprawnionym,
d. niepozostawianie nośników, na których zapisane są klucze kryptograficzne bez nadzoru, a w szczególności po zakończeniu pracy przechowywanie kluczy w bezpiecznym miejscu,
e. stosowanie zaleceń i instrukcji przekazanych przez dostawcę nośnika, na którym dostarczony jest klucz kryptograficzny.

ASI może przechowywać ewidencję kluczy w formie elektronicznej.

Wzór ewidencji kluczy kryptograficznych

2.

L.p.	Przeznaczenie	Dostawca	Użytkownik, któremu wydano klucz (imię, nazwisko)	Data wydania klucza	Data wygaśnięcia klucza
1.					
2.					
3.					
4.					
5.					
6.					

Certyfikaty.

Certyfikaty SSL chronią wrażliwe informacje biznesowe dzięki szyfrowaniu wysyłanych danych, a następnie rozszyfrowaniu ich przez odbiorcę.

Certyfikat SSL jest wystawiany dla wskazanej domeny lub poszczególnych subdomen. Ważne, aby przy ubieganiu się o wydanie certyfikatu, posiadać prawa własności domeny, którą chcemy zabezpieczyć. Należy również dysponować aktywną skrzynką pocztową w adresie certyfikowanej domeny, np. admin@nazwa_certyfikowanej_domeny, na którą zostaną wysłane wiadomości instalacyjne i konfiguracyjne.

Certyfikaty wraz z hasłami przechowuje się tak, jak nośniki kopii zapasowych. ASI może przechowywać ewidencję certyfikatów w formie elektronicznej.

Wzór ewidencji certyfikatów.

L.p.	Nazwa certyfikatu i przeznaczenie	Dostawca	Użytkownik, któremu wydano klucz (imię, nazwisko, organizacja)
1.			
2.			
3.			

Załącznik nr 22. Instrukcja uwzględniania ochrony danych w fazie projektowania oraz domyślna ochrona danych.

Uwzględnianie ochrony danych w fazie projektowania.

1. ADO planując nowe zadania lub usługi zapewnia środki organizacyjne i techniczne służące bezpieczeństwu danych osobowych.
2. W fazie planowania nowych zadań lub usług ADO lub osoba upoważniona realizująca zadanie poddaje analizie:
    a. czy przetwarzanie danych osobowych będzie spełniało wymagania RODO, w szczególności czy zapewnione jest spełnienie podstawowych zasad przetwarzania danych osobowych, o których mowa w art. 5 RODO,
    b. czy przetwarzanie danych osobowych będzie spełniało wymagania art. 20 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r. poz. 2247),
    c. czy możliwa będzie realizacja praw i wolności podmiotów danych, którzy będą korzystali z nowego zadania lub usługi,
    d. czy ADO jest w stanie zapewnić odpowiednie środki organizacyjne i techniczne, w tym pseudonimizację i minimalizację, zapewniające bezpieczeństwo przetwarzanych danych w kontekście zidentyfikowanych ryzyk.
3. Uwzględnienie ochrony danych osobowych w fazie projektowania należy stosować także w sytuacji, gdy dokonywane są zakupy, produkcja lub wdrożenia systemów informatycznych służących lub mających wpływ na przetwarzanie danych osobowych.

Osoby realizujące:

- w zakresie zapewnienia ochrony danych w fazie projektowania – ADO,
- w zakresie dokonywania zakupów dostaw i usług, informowania ADO o zamiarze podjęcia nowych zadań obejmujących przetwarzanie danych osobowych – osoby upoważnione odpowiedzialne za przygotowanie zapytania ofertowego lub SIWZ, ASI.

Domyślna ochrona danych

1. W celu zapewnienia domyślnej ochrony danych osobowych ADO wdraża i stosuje odpowiednie środki techniczne i organizacyjne mające na celu minimalizację przetwarzania danych osobowych.
2. Minimalizacja osiągana jest poprzez przetwarzanie wyłącznie tych danych osobowych, które są niezbędne dla osiągnięcia konkretnego celu przetwarzania. Obowiązek ten oznacza:
    a. minimalizację ilości danych osobowych,
    b. minimalizację zakresu danych osobowych,
    c. określenie niezbędnego czasu przetwarzania danych osobowych,
    d. określenie minimalnej grupy osób, które będą miały dostęp do tych danych,
    e. zapewnienie dostępności do danych w niezbędnym zakresie.
3. ADO stosuje środki organizacyjne i techniczne mające na celu zapewnienie poufności, integralności i dostępności przetwarzanych danych osobowych.
4. Uwzględnienie domyślnej ochrony danych osobowych należy stosować także w sytuacji, gdy dokonywane są zakupy, produkcja lub wdrożenia systemów informatycznych służących lub mających wpływ na przetwarzanie danych osobowych.

Osoby realizujące:

- w zakresie zapewnienia ochrony przetwarzanych lub planowanych do przetwarzania danych – ADO,
- w zakresie dokonywania zakupów dostaw i usług, informowania ADO o zamiarze podjęcia nowych zadań obejmujących przetwarzanie danych osobowych – osoby upoważnione odpowiedzialne za przygotowanie zapytania ofertowego lub SIWZ, ASI.

Metodologia oceny planowanych czynności przetwarzania w celu uwzględnienia ochrony danych w fazie projektowania oraz domyślnej ochrony danych

1. W celu spełnienia ww. zasad osoby wskazane przez ADO przeprowadzają ocenę planowanego zadania.
2. Ocena dokonywana jest zgodnie z załącznikiem nr 1.1. – arkuszem oceny planowanego zadania.
3. Pracownik przygotowujący Arkusz oceny planowanego zadania, przekazuje go do oceny IOD.
4. IOD ocenia planowane do wdrożenia zadania, w szczególności weryfikując, czy spełnione zostały podstawowe zasady przetwarzania danych osobowych, o których mowa w art. 5 RODO, czy zapewnione zostały metody wypełnienia praw podmiotów danych, o których mowa w Rozdziale III RODO oraz czy spełnione zostały wymagania dotyczące stosowanych środków technicznych i organizacyjnych zapewniających bezpieczeństwo danych osobowych.
5. IOD po dokonaniu oceny i wydaniu zaleceń przekazuje arkusz ADO do zatwierdzenia.
6. Planowane zadanie może być wdrożone do realizacji wyłącznie z uwzględnieniem zasad określonych w Arkuszu oceny planowanego zadania.

Osoby realizujące:

- w zakresie przygotowania Arkusza oceny planowanego zadania – ADO,
- w zakresie zaopiniowania Arkusza oceny planowanego zadania – IOD,
- w zakresie zatwierdzenia Arkusza oceny planowanego zadania – ADO.