ZARZĄDZENIE Nr 46/2019
WÓJTA GMINY JEDWABNO
z 20 maja 2019 r.

w sprawie wprowadzenia procedur informatycznych.

Na podstawie Rozporządzenie Parlamentu Europejskiego i rady Europy (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE z dnia 27 kwietnia 2016r. (Dz. Urz. UE nr 119) a także ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz.U.2019.506) **zarządzam, co następuje:**

§1.

Wprowadza się do stosowania:

„Zasady tworzenia haseł administratorów".

„Procedurę usuwania danych z nośników"

„Procedurę usuwania oprogramowania typu *BOTNET*"

„Procedurę przygotowania stanowiska komputerowego".

§2.

Dokumenty stanowią załączniki do niniejszego Zarządzenia.

§3.

Terminy pierwszego wykonania określam na:
- w przypadku „Procedury zasady tworzenia haseł administratorów" na maksimum 3 dni robocze od dnia podpisania.
- w przypadku „Procedury dostępu administratora do komputerów użytkowników" na maksimum 7 dni roboczych od dnia podpisania.

§4.

Administrator Systemów Informatycznych w okresie do 10 dni roboczych dostarczy do akceptacji procedurę tworzenia i odtwarzania kopii zapasowych systemów i baz danych.

§5.

Zarządzenie wchodzi w życie z dniem podpisania.

Wójt

(Sławomir Ambroziak)

ZASADY TWORZENIA HASEŁ ADMINISTRATORÓW

1. Definicje

UG	Urząd Gminy w Jedwabnie
Administrator danych	Wójt Gminy Jedwabno.
Administrator, ASI	Osoba zajmująca się zarządzaniem systemem informatycznym, jego wydzieloną częścią lub urządzeniem komputerowym (np. systemem operacyjnym, serwerem, bazą danych, aplikacja, siecią). Odpowiada za ich poprawne, bezpieczne funkcjonowanie.
Konto administratora	Zbiór zasobów i uprawnień w ramach danego systemu informatycznego lub urządzenia komputerowego, przypisanych konkretnemu administratorowi, dostępny po podaniu unikalnej nazwy konta administratora oraz hasła.
Ratunkowa kopia hasła administratora	Każda wersja hasła do konta administratora zapisana w formie papierowej, umożliwiająca dostęp do systemu informatycznego lub urządzenia komputerowego w sytuacji awaryjnej.

2. Cel dokumentu

Dokument określa zasady tworzenia bezpiecznych haseł administratorów do eksploatowanych systemów informatycznych i urządzeń komputerowych.

3. Odpowiedzialność

Za przestrzeganie zasad wymienionych w niniejszej procedurze odpowiadają: administrator lub administratorzy odpowiedzialni za poszczególne systemy informatyczne i urządzenia komputerowe.

4. Zakres i warunki stosowania

Procedurę stosuje się w celu ochrony przed nieuprawnionym dostępem do systemów informatycznych i urządzeń komputerowych eksploatowanych w Urzędzie Gminy w Jedwabnie, dla których są konta administratorów oraz system autoryzacji wykorzystujący hasła.
Do wszystkich kont administratorów należy zawsze tworzyć hasła przy wykorzystaniu niniejszych zasad.
W szczególności procedura dotyczy kont:

- administratorów systemów operacyjnych,
- administratorów domen,
- administratorów systemów baz danych,
- administratorów serwerów,
- administratorów komputerów lokalnych,
- administratorów aplikacji biznesowych, konsol administracyjnych,
- administratorów aplikacji antywirusowych, narzędziowych i innych tego typu,
- innych kont administratorów.
- użytkowników uprzywilejowanych, którzy mają podobne uprawnienia, jak zwykły użytkownik, lecz mogą zmieniać ustawienia wpływające na pracę wszystkich użytkowników lub zasobów (czas komputera, zainstalowane programy, itp.).

Zasady stosuje się także do haseł dostępu do BIOS, firmware, twardych dysków, elementów infrastruktury sieciowej jak router, switch oraz innych urządzeń komputerowych.

Procedura nie ma zastosowania dla systemów i urządzeń, w których stosowane są generatory haseł oraz inne sposoby kontroli tożsamości administratorów np. karty, tokeny, certyfikaty itp. Procedury nie stosuje się również w przypadkach, gdy stosownie haseł i zarządzanie nimi zgodnie z poniższą procedurą jest niemożliwe ze względu na zastosowane rozwiązania techniczne.

W przypadku systemów informatycznych, dla których opracowane zostały indywidualne procedury dotyczące ww. zagadnień stosuje się procedurę o wyższych wymaganiach.

5. Dokumenty związane

- Norma PN-EN ISO/IEC 27002:2017-06.
- Guide to Enterprise Password Management (Draft), NIST Special Publication 800-118 (Draft), Recommendations of the National Institute of Standards and Technology.
- Password (Jsage, FIPS PUB 112, Federal Information Processing Standards Publications.
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie

swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE.
- Ustawa z dnia. o ochronie danych osobowych (Dz. U. z 2018 r., poz. 1000 z późn. zm.).
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakimi powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r., Nr 100, poz. 1024).

6. Przebieg procedury

6.1 Klasy krytyczności

W zależności od stopnia krytyczności systemów informatycznych oraz urządzeń komputerowych, a także rodzaju danych przy pomocy nich przetwarzanych, wprowadza się następujące klasy krytyczności dla systemów i urządzeń:
- systemy i urządzenia pomocnicze - m.in. systemy szkoleniowe, systemy testowe, serwery pomocnicze,
- systemy i urządzenia o normalnej klasie krytyczności,
- systemy i urządzenia o podwyższonej klasie krytyczności - m.in. serwery produkcyjne, aplikacje przetwarzające informacje stanowiące dane osobowe i dane organizacji, routery dostępowe.

Administrator prowadzi ewidencje systemów i urządzeń należących do poszczególnych klas krytyczności.

6.2 Wymagania dotyczące tworzenia haseł

Na siłę bezpiecznego hasła wpływa przede wszystkim jego długość oraz sposób tworzenia. Im dłuższe hasło i bardziej skomplikowane, tym potrzebne jest więcej kombinacji i czasu do jego złamania. Hasła administratorów ze względu na szerokie uprawnienia muszą spełniać bardziej restrykcyjne zasady niż hasła użytkowników. Administrator powinien zawsze definiować hasła stosunkowo skomplikowane, trudne do odgadnięcia.

Długość hasła administratora powinna być:
- dla systemów i urządzeń pomocniczych - min. 8 znaków,
- dla systemów i urządzeń o normalnej klasie krytyczności - min. 10 znaków,
- dla systemów i urządzeń o podwyższonej klasie krytyczności - min. 14 znaków.

Hasła muszą zawierać duże litery alfabetu (od *A* do Z), małe litery alfabetu (od a do z) oraz cyfry (od *0* do 9) i znaki specjalne (np. /, $, #, %). Należy zwrócić uwagę na fakt, że w przypadku niektórych systemów lub urządzeń, ze względów technicznych, nie można stosować do konstruowania haseł niektórych znaków specjalnych oraz polskich znaków diakrytycznych.

Hasło nie może być:
- tworzone według stałego schematu uwzględniającego upływ czasu lub inne łatwe do odgadnięcia czynniki, np. zawierające nazwę miesięcy,
- konstruowane przez administratora identycznie lub w znaczący sposób podobnie do wcześniej używanych,
- słowem występującym w słowniku języka polskiego lub jakiegokolwiek innego słownika, również słowem o odwróconej kolejności liter,
- tworzone w oparciu o elementy danych osobistych typu: data urodzenia, nr dokumentu, imię, nazwisko itp.,
- ciągiem znaków występujących obok siebie na klawiaturze, np.: qwerty, 12345.

Hasła administratorów należy utrzymywać w tajemnicy i nie powinny być ujawniane innym osobom, przełożonym, pracownikom działów ochrony itp. Nie wolno także ujawniać haseł zdezaktualizowanych.
Hasła administratorów nie powinny być zapisywane. Każde przedstawienie hasła administratora w formie pisemnej powoduje, że zapis taki jest traktowany jako ratunkowa kopia hasła administratora.

Nie należy stosować takich samych haseł do różnych systemów i urządzeń.

Administratorzy nie powinni korzystać z takich samych haseł w celach służbowych oraz prywatnych.

6.3 Wymagania systemowe dla haseł administratora

O ile nie ma przeciwwskazań technicznych powinny być dla haseł administratora stosowane w systemach informatycznych i urządzeniach komputerowych reguły:
- wymuszające odpowiednią częstotliwość zmiany hasła,
- wymuszające minimalną długość hasła,
- wymuszające właściwa strukturę hasła,
- zabraniające powtarzania ostatnich 10 haseł.

W przypadku, gdy dla systemu lub urządzenia zdefiniowane są polisy wymuszające stosowanie właściwych haseł i są one mniej restrykcyjne niż te, które wynikają z niniejszej procedury, administrator jest zobowiązany do stosowania haseł konstruowanych zgodnie z powyższymi zaleceniami.

Bezpieczeństwo systemów zależy w dużej mierze od sposobu prezentacji i przechowywania haseł w systemie. Zaleca się, o ile jest to możliwe:
- stosowanie procedury zmiany hasła, obejmującej powtórne wpisanie nowego hasła w celu uniknięcia błędów przy jego wprowadzeniu,
- podczas procesu uwierzytelniania wprowadzane hasło nie powinno być widoczne na ekranie,

- hasła administratorów powinny być przechowywane i przesyłane w formie zaszyfrowanej,
- baza haseł w systemie informatycznym powinna być przechowywana w innym miejscu niż dane aplikacji.

6.4 Wykonanie ratunkowej kopii hasła administratora

Administrator systemu informatycznego lub urządzenia komputerowego, dla którego wykonuje się kopie ratunkowe haseł, w przypadku pierwszego wprowadzenia hasła administratora lub każdorazowej jego zmiany, dokonuje zapisu ratunkowej kopii hasła na formularzu wykonanym zgodnie z wzorem, wpisując minimum następujące informacje:
- nazwa systemu/urządzenia,
- imię i nazwisko administratora zmieniającego hasło,
- nazwa użytkownika/konta (wpisana odręcznie, w sposób czytelny), która jest podawana podczas logowania,
- treść hasła (wpisana odręcznie, w sposób czytelny),
- data i godzina zmiany hasła,
- powód zmiany hasła.

Formularz jest podpisywany przez administratora sporządzającego ratunkową kopię hasła.
Formularz z ratunkową kopią hasła jest pakowany w kopertę opatrzoną etykietą zawierającą minimum następujące informacje:
- nazwa systemu/urządzenia i jego lokalizacja,
- imię i nazwisko administratora,
- data zmiany hasła,
- data ważności hasła (dopuszcza się stosowanie określeń „bezterminowo", „do czasu zdeponowania nowego hasła"),
- ew. inne uwagi (np. dotyczące ilości przechowywanych ostatnich haseł).

Koperta jest zaklejana i zabezpieczana przed niepowołanym dostępem.
W celu zabezpieczenia kopert przed odczytaniem hasła bez ich otwierania, informacje są zapisane na formularzu zawierającym dwie tabele, z których jedna zawiera hasło, natomiast druga nadruk. Tak stworzony formularz po zgięciu w połowie utworzy treść uniemożliwiającą nieuprawnione odczytanie hasła.
Zapieczętowana koperta jest przekazywana osobiście przez administratora bezpośrednio do komórki lub osoby prowadzącej archiwum ratunkowych kopii haseł administratorów. Należy zachować szczególną ostrożność w czasie transportu tak, aby hasła nie dostały się w ręce osób niepowołanych bądź nie zostały zgubione czy zniszczone.

6.5 Przechowywanie ratunkowych kopii haseł

Ratunkowe kopie haseł administratorów należy przechowywać w zapieczętowanych kopertach opatrzonych właściwą etykietą. Zbiór haseł należy przechowywać w zamykanych sejfach lub szafach, które są niedostępne po godzinach pracy.
Osoba odpowiedzialna za prowadzenie archiwum ratunkowych kopii haseł administratorów prowadzi ewidencję, w której odnotowuje się fakt umieszczenia kopert z hasłami ratunkowymi. Ewidencja zawiera następujące informacje: nazwa systemu/urządzenia, data i godzinę przekazania hasła, imię i nazwisko oraz podpis osoby przekazującej hasło, data zniszczenia hasła, imię i nazwisko oraz podpis osoby, która zniszczyła kopertę z hasłem. Ewidencja może być prowadzona łącznie dla wszystkich przechowywanych haseł bądź w podziale na administratorów, systemy lub urządzenia.
Ratunkową kopię hasła administratora należy przechowywać, co najmniej do dnia upłynięcia jego ważności i otrzymania kolejnej wersji kopii hasła administratora do danego systemu informatycznego lub urządzenia komputerowego.
W niektórych przypadkach kopia hasła powinna być przechowywana w dłuższym okresie czasu mimo zmiany hasła (np. hasło administratora wykorzystane przy tworzeniu nośników ratunkowych, potrzeba przechowywania kliku kolejnych haseł itp.). W takiej sytuacji na kopercie powinna być wpisana odpowiednia adnotacja określająca właściwy czas przechowywania.

6.6 Zasady niszczenia kopert z zdezaktualizowanymi ratunkowymi kopiami haseł

Za niszczenie kopert z hasłami odpowiada osoba prowadząca archiwum. Koperta ze zdezaktualizowanym hasłem może być zniszczona dopiero po złożeniu nowego hasła do tego samego systemu informatycznego lub urządzenia komputerowego oraz po upływie okresu ważności. Koperty ze zdezaktualizowanym hasłami powinny być niszczone bez otwierania, w sposób trwały, najlepiej w niszczarce dokumentów o klasie bezpieczeństwa min. 3. Osoba, która dokonuje zniszczenia kopert z hasłami dokumentuje ten fakt w prowadzonej ewidencji przechowywania ratunkowych kopii haseł administratorów.

6.7 Udostępnianie ratunkowych kopii haseł.

W uzasadnionych przypadkach hasło ratunkowe przechowywane w archiwum jest udostępniane upoważnionej

osobie. Upoważnienie do pobrania hasła powinno być imienne i mieć charakter jednorazowy W sytuacjach awaryjnych możliwe jest upoważnienie ustne, jednak powinno być ono potwierdzone później w formie pisemnej. Zasada ta dotyczy również wydania haseł właściwym administratorom. Wydanie hasła ratunkowego należy zarejestrować w ewidencji, która zawiera następujące informacje: data udostępnienia hasła, nazwa systemu/urządzenia, imię, nazwisko oraz podpis osoby pobierającej hasło. Do ewidencji dołączane są również upoważnienia.

Po wykorzystaniu hasła ratunkowego, hasło administratora systemu informatycznego lub urządzenia komputerowego powinno zostać zmienione na nowe. W niektórych przypadkach zmiana hasła może nie być wymagana.

6.8 Odstępstwa od procedury

Wszelkie odstępstwa od procedury zmiany haseł administratorów wymagają pisemnej zgody Administratora Danych UG w Jedwabnie.

7. Załączniki

Lista systemów, dla których tworzy się hasła awaryjne.
Wzór formularza zmiany hasła administratora.
Ewidencja ratunkowych kopii haseł administratora.
Ewidencja udostępnienia ratunkowych kopii haseł administratorów.
Wzór upoważnienie do pobrania ratunkowej kopii hasła administratora.

Lista systemów, dla których tworzy się hasła administracyjne.

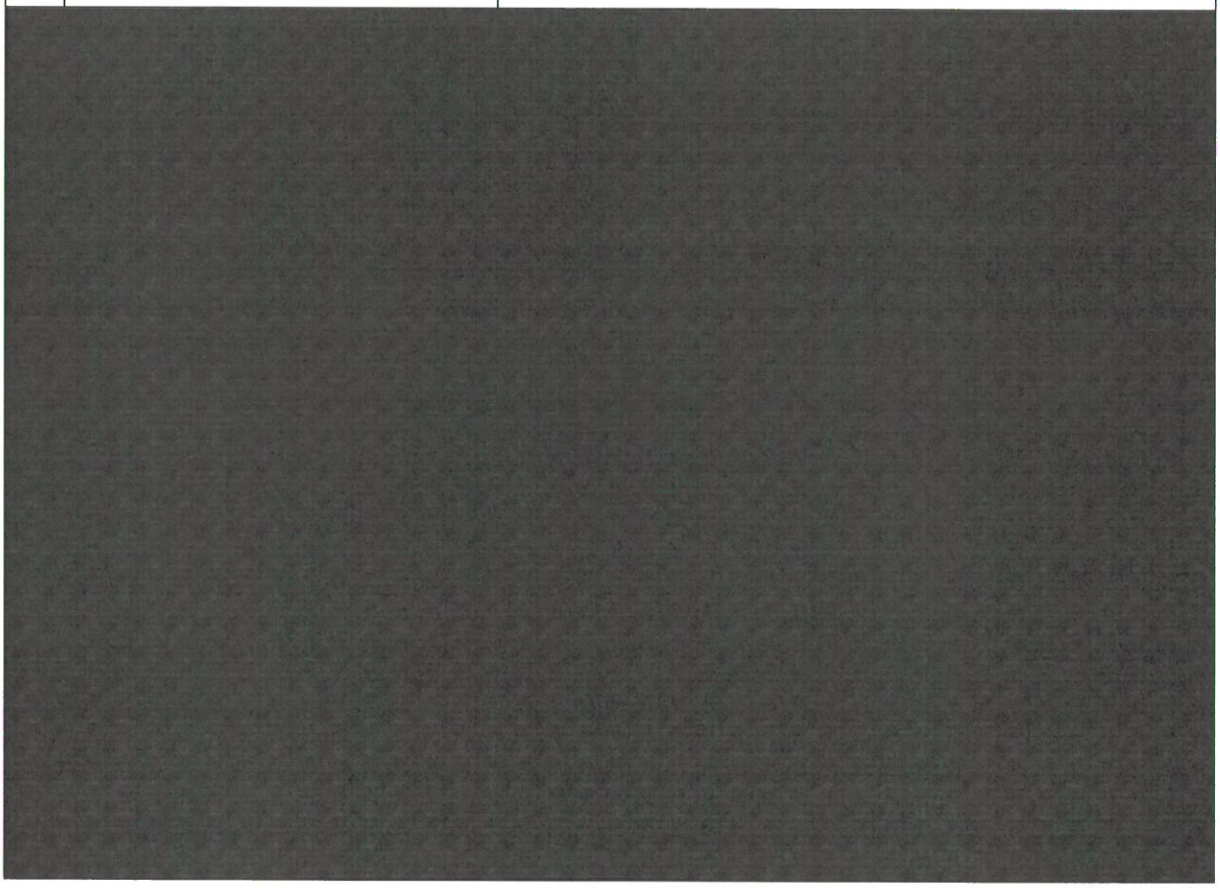
Lp.	Nazwa systemu/urządzenia/adres IP	Login konta administracyjnego	Istotność systemu/urządzenia	Uwagi
1	2	3	4	6

*Należy uwzględnić wszystkie systemy i urządzenia zgodnie z pkt. 6.1

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	

Ewidencja ratunkowych kopii haseł administratora.

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	6	7

Ewidencja udostępnienia 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

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: .....

UWAGI:

_____
podpis osoby upoważniającej

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. Wymagania podane w dokumencie spełniają zalecenia zawarte w Załączniku A do normy PN-ISO/IEC 27001 w zakresie wskazanym w punkcie 4.1.

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 departamentu

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 .....

PROCEDURA USUWANIA OPROGRAMOWANIA TYPU BOTNET

SPIS TREŚCI

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):

A.10.4.1 - Zabezpieczenie przed kodem złośliwym.

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 wykonać następujące działania:

1. Zidentyfikować poziom zagrożenia.
2. Jeżeli spełnione są warunki zgłoszenia incydentu zgłosić do CSIRT NASK
CSIRT NASK koordynuje incydenty zgłaszane przez operatorów usług kluczowych, dostawców usług cyfrowych, samorząd terytorialny oraz wszystkie te podmioty, których nie obsługują CSIRT GOV i MON.
3. Formą zgłoszenia incydentu jest przesłanie zgłoszenia elektronicznego do CERT Polska, który odpowiada za operacyjną działalność CSRIT NASK. Najlepiej wykorzystać formularz online na stronie https://incydent.cert.pl, który krok po kroku podpowie jakie informacje zawrzeć w zgłoszeniu. Ostatecznie można wysłać zgłoszenie pocztą elektroniczną na adres cert@cert.pl. Formularz do wydruku dostępny jest na BIP NASK.

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 wyłączeń w stosowaniu niniejszej procedury.

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

Brak.

PROCEDURA
PRZYGOTOWANIA STANOWISKA KOMPUTEROWEGO

Spis treści

1. WYKAZ SKRÓTÓW I TERMINÓW

Administrator danych, ADO – Rada Gminy reprezentowana przez Przewodniczącego Rady (organ, jednostka organizacyjna, podmiot lub osoba, decydująca o celach i środkach przetwarzania danych osobowych),

IOD – Inspektor Ochrony Danych Osobowych,

ASI – Administrator Systemów Informatycznych, osoba upoważniona do zarządzania systemem informatycznym,

Pracownik – osoba zatrudniona w Urzędzie Gminy.

Zasoby pracownika – dane oraz informacje, urządzenia, narzędzia informatyczne oraz dostępna infrastruktura informatyczna wykorzystywana podczas wykonywania czynności służbowych.

2. CEL PROCEDURY

Celem procedury jest określenie zasad dostępu do stanowiska komputerowego pracownika oraz jego zasobów, a także wskazanie szczegółowych parametrów monitorowania tych zasad.

3. ODPOWIEDZIALNOŚĆ

Za przestrzeganie zasad wymienionych w niniejszej procedurze odpowiadają:

a. Administrator Systemów Informatycznych – odpowiada za prawidłowe skonfigurowanie stanowiska komputerowego oraz przeszkolenie użytkownika;
b. Pracownicy korzystający ze stanowiska komputerowego oraz zasobów udostępnionych, na których przechowywane są dane.

4. ZAKRES I WARUNKI STOSOWANIA

Procedura ma charakter ogólny, jednak w kilku aspektach precyzuje minimalne wymagania, które powinny zostać spełnione.

5. 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*

6. TREŚĆ PROCEDURY

6.1. 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.

7. 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.

7.1. SPRZĘT

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

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

7.2. OPROGRAMOWANIE

- **System operacyjny** – zaktualizowany system operacyjny z rodziny MS Windows nie starszy niż MS Windows 8.1 Professional PL
- **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)** z domyślnym ustawieniem skanowania całego systemu na min. 1 raz w tygodniu;
- **Podłączenie drukarek** – zainstalowanie drukarek (podstawowej i alternatywnej) umożliwiające użytkownikowi wydrukowanie dokumentów w przypadku, gdy zachodzi taka konieczność.
- **Inne aplikacje niezbędne do pracy a wynikające z wymogów producenta,**

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*.

8. DOKUMENTOWANIE ZLECEŃ WYKONANIA ZADANIA

ASI ewidencjonuje dokument potwierdzający skonfigurowanie stacji roboczej do pracy po potwierdzeniu przez Administratora Danych zapoznania się z dokumentem (*Załącznik 1*). Skan dokumentu przekazuje w formie elektronicznej do IOD.

9. CZAS REALIZACJI ZADANIA

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

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".

.....

(data, imię i nazwisko)

W dniu ..... w Urzędzie Gminy w Jedwabnie Administrator Systemów Informatycznych przeszkolił .....

(imię i nazwisko)

do pracy na stacji roboczej .....

(numer inwentarzowy)

Szkolenie zawierało następujące elementy:

- bezpieczne posługiwanie się komputerem,

- zasady tworzenia haseł,

- zasady korzystania z zewnętrznych nośników informacji,

- obsługa oprogramowania: .....

Szkolenie trwało: .....

.....

(data, imię i nazwisko ASI)

.....

(data, imię i nazwisko pracownika)