WÓJT GMINY SANOK
woj. podkarpackie

Zarządzenie Nr 155/2020
Wójta Gminy Sanok
z dnia 22 lipca 2020 r.

w sprawie wyznaczenia Autonomicznego Stanowiska Komputerowego do przetwarzania informacji niejawnych oznaczonych klauzulą "zastrzeżone" w Urzędzie Gminy Sanok

Na podstawie art. 30 ust. 1 i art. 31 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz.U.2020.713 t.j.), art. 48 ust. 9 i 11 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U.2019.742 t.j.) oraz § 25 rozporządzenia Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz.U.2011.159.948) zarządzam co następuje:

§ 1

Wyznaczam w Urzędzie Gminy Sanok Autonomiczne Stanowisko Komputerowe zlokalizowane w pomieszczeniu Biura Zarządzania Kryzysowego i Obrony Cywilnej, które ma na celu zapewnienie bezpieczeństwa teleinformatycznego i ochrony informacji niejawnych oznaczonych klauzulą "zastrzeżone" przy ich przetwarzaniu. Wytwarzanie i przetwarzanie dokumentów papierowych oraz na nośnikach oznaczonych klauzulą "zastrzeżone" może się odbywać tylko na Autonomicznym Stanowisku Komputerowym.

§ 2

Udzielam akredytacji bezpieczeństwa teleinformatycznego dla systemu Autonomiczne Stanowisko Komputerowe „ASK" w Urzędzie Gminy Sanok przeznaczonego do przetwarzania informacji niejawnych o klauzuli „ZASTRZEŻONE".

§3

Użytkownicy Autonomicznego Stanowiska Komputerowego Urzędu Gminy Sanok muszą posiadać aktualne poświadczenie bezpieczeństwa lub upoważnienie Wójta Gminy uprawniające do dostępu do informacji niejawnych oznaczonych klauzulą "zastrzeżone".

§ 4

Uprawnieni użytkownicy Autonomicznego Stanowiska Komputerowego przed rozpoczęciem pracy w systemie są zobowiązani odbyć szkolenie z zakresu bezpieczeństwa

teleinformatycznego oraz zapoznać się z procedurami bezpiecznej eksploatacji. Szkolenia w tym zakresie prowadzone są przez Pełnomocnika do Spraw Ochrony Informacji Niejawnych.

§5

Użytkownik Autonomicznego Stanowiska Komputerowego przed rozpoczęciem pracy zgłasza się do Pełnomocnika do Spraw Ochrony Informacji Niejawnych. Przy stanowisku prowadzona jest ewidencja osób korzystających z Autonomicznego Stanowiska Komputerowego. Wpisu do wykazu uzytkowników dokonuje się osobiście.

§ 6

Użytkownik Autonomicznego Stanowiska Komputerowego obowiązany jest do informowania Pełnomocnika do Spraw Ochrony Informacji Niejawnych o wszelkich problemach związanych z obsługą stanowiska.

W czasie prac personelu technicznego lub sprzątającego zabroniona jest praca na stanowisku komputerowym, a dokumenty niejawne należy zabezpieczyć.

§ 7

W związku z wyznaczeniem Autonomicznego Stanowiska Komputerowego wprowadza się do stosowania następujące dokumenty:

1. "Dokumentacja bezpieczeństwa systemu teleinformatycznego dla stacji komputerowej przetwarzającej informacje niejawne o klauzuli "zastrzeżone" w Urzędzie Gminy Sanok - załącznik nr 1.
2. Wykaz użytkowników Autonomicznego Stanowiska Komputerowego - załącznik nr 2.

§ 8

Nadzór nad realizacją niniejszego zarządzenia powierza się Pełnomocnikowi do Spraw Ochrony Informacji Niejawnych

§ 9

Zarządzenie wchodzi w życie z dniem podpisania.

WÓJT GMINY SANOK
mgr Anna Hałas

Załącznik Nr 1
do zarządzenia Nr 155/2020
Wójta Gminy Sanok
z dnia 22 lipca 2020r.

ZATWIERDZAM

WÓJT GMINY SANOK

mgr Anna Hałas

.....

DOKUMENTACJA BEZPIECZEŃSTWA SYSTEMU TELEINFORMATYCZNEGO DLA STACJI KOMPUTEROWEJ PRZETWARZAJĄCEJ INFORMACJE NIEJAWNE O KLAUZULI "ZASTRZEZONE" W URZĘDZIE GMINY SANOK.

OPRACOWAŁ:

.....

SANOK 2020 r.

SPIS TREŚCI

I. WPROWADZENIE

1. Informacje ogólne
2. Klauzula tajności autonomicznej stacji komputerowej
3. Dopuszczenie autonomicznej stacji komputerowej
4. Opis autonomicznej stacji komputerowej

II. ADMINISTRACJA I ORGANIZACJA BEZPIECZEŃSTWA

1. Informacje ogólne
2. Inspektor Bezpieczeństwa Teleinformatycznego
3. Administrator Systemu Teleinformatycznego
4. Użytkownik autonomicznej stacji komputerowej
5. Informowanie o naruszeniu bezpieczeństwa stacji komputerowej
5. Informacje o wykryciu wirusa w autonomicznej stacji komputerowej

III. BEZPIECZEŃSTWO PERSONELU

1. Informacje ogólne
2. Użytkownicy autonomicznej stacji komputerowej
3. Personel sprzątający
4. Osoby wizytujące

IV. BEZPIECZEŃSTWO FIZYCZNE

1. Informacje ogólne
2. Ochrona autonomicznej stacji komputerowej oraz nośników
3. Kontrola dostępu użytkowników do sprzętu
4. Zasady kontroli sprzętu

V. BEZPIECZEŃSTWO DOKUMENTÓW

1. Informacje ogólne
2. Wymiana informacji
3. Oznaczenie klasyfikacji dokumentów
4. Zmiana klasyfikacji dokumentów
5. Kontrola dokumentów
6. Niszczenie dokumentów
7. Biblioteka nośników

VI. BEZPIECZEŃSTWO SPRZĘTU I OPROGRAMOWANIA

1. Informacje ogólne
2. Bezpieczeństwo sprzętu
3. Bezpieczeństwo oprogramowania

VII. BEZPIECZEŃSTWO ŁĄCZNOŚCI

1. Bezpieczeństwo kryptograficzne
2. Bezpieczeństwo elektromagnetyczne
3. Bezpieczeństwo transmisji

VIII. MONITOROWANIE BEZPIECZEŃSTWA

1. Informacje ogólne.

IX. KONSERWACJE I NAPRAWY.

1. Konserwacje sprzętu i oprogramowania
2. Naprawa sprzętu

X. PLANY AWARYJNE I ZAPOBIEGAWCZE

1. Zasilanie
2. Kopie zapasowe
3. Klęski żywiołowe
4. Sytuacje specjalne

XI. POLITYKA ANTYWIRUSOWA

1. Informacje ogólne
2. Świadomość użytkownika
3. Zasady higieny
4. Infekcja stacji komputerowej
5. Postępowanie w przypadku wykrycia wirusa

I. WPROWADZENIE

1. Informacje ogólne

Niniejszy dokument zawiera procedury bezpieczeństwa teleinformatycznego dla Autonomicznej Stacji Komputerowej w Urzędzie Gminy Sanok przetwarzającej informacje niejawne oznaczone klauzulą **"zastrzeżone"**.

Opracowanie procedur bezpieczeństwa wynika z wymagań zawartych w ustawie o ochronie informacji niejawnych oraz w rozporządzeniu Prezesa Rady Ministr6w w sprawie podstawowych wymagań bezpieczeństwa system6w i sieci teleinformatycznych.

Niniejsze procedury bezpieczeństwa są obowiązujące dla wszystkich użytkowników autonomicznej stacji komputerowej.

2. Klauzula tajności autonomicznej stacji komputerowej

Autonomiczna stacja komputerowa w Urzędzie Gminy Sanok opisana w szczegółowych wymaganiach bezpieczeństwa jest stanowiskiem przetwarzającym informacje niejawne o klauzuli "zastrzeżone". Wszystkie informacje przechowywane lub przetwarzane oraz wyprowadzane na urządzenia zewnętrzne są traktowane jako "zastrzeżone".

3. Dopuszczenie autonomicznej stacji komputerowej

Akredytacji bezpieczeństwa teleinformatycznego dla systemu teleinformatycznego przeznaczonego do przetwarzania informacji niejawnych o klauzuli "zastrzeżone" udziela Wójt Gminy Sanok przez zatwierdzenie dokumentacji bezpieczeństwa systemu teleinformatycznego.

W ciągu 30 dni od udzielenia akredytacji bezpieczeństwa teleinformatycznego Wójt przekazuje ABW dokumentację bezpieczeństwa systemu teleinformatycznego. W ciągu 30 dni od otrzymania dokumentacji bezpieczeństwa systemu teleinformatycznego ABW może przedstawić zalecenia dotyczące konieczności przeprowadzenia dodatkowych czynności związanych z bezpieczeństwem informacji niejawnych. W szczególnie uzasadnionych przypadkach ABW może nakazać wstrzymanie przetwarzania informacji niejawnych w systemie teleinformatycznym posiadającym akredytację bezpieczeństwa teleinformatycznego.

4. Opis autonomicznej stacji komputerowej

Autonomiczna Stacja Komputerowa zlokalizowana jest w budynku Urzędu Gminy Sanok, ul. Kościuszki 23, pok. nr 512 w Biurze Zarządzania Kryzysowego i Obrony Cywilnej. Wyposażona jest w komputer spełniający wymogi przetwarzania danych do klauzuli

"zastrzeżone". System nie posiada połączeń z innymi systemami i sieciami teleinformatycznymi.

II. ADMINISTRACJA I ORGANIZACJA BEZPIECZEŃSTWA.

1. Informacje ogólne

Kierownik jednostki organizacyjnej zobowiązany jest zapewnić bezpieczeństwo teleinformatyczne przy przetwarzaniu informacji niejawnych za pośrednictwem Autonomicznej Stacji Komputerowej.

Wójt Gminy Sanok wyznaczył Administratora Systemu Teleinformatycznego oraz Inspektora Bezpieczeństwa Teleinformatycznego, odpowiedzialnych za funkcjonowanie i przestrzeganie zasad oraz wymagań bezpieczeństwa teleinformatycznego.

Pełnomocnik ds. Ochrony Informacji Niejawnych Urzędu Gminy zwany dalej pełnomocnikiem ochrony, odpowiada za zapewnienie przestrzegania przepisów o ochronie informacji niejawnych. Pełnomocnik ochrony jest odpowiedzialny za funkcjonowanie autonomicznej stacji komputerowej. Przed rozpoczęciem korzystania ze stacji komputerowej, każdy użytkownik zapoznaje się z procedurami bezpieczeństwa, co potwierdza podpisem.

2. Inspektor Bezpieczeństwa Teleinformatycznego.

Sprawdza zgodność stanu faktycznego ze szczególnymi wymaganiami bezpieczeństwa oraz przestrzeganie procedur bezpieczeństwa. Inspektor Bezpieczeństwa Teleinformatycznego służy pomocą Administratorowi Systemu Teleinformatycznego i użytkownikom w zakresie bezpieczeństwa i przepisów dotyczących obiegu dokumentów wytwarzanych za pomocą stacji komputerowej.

Pełnomocnik ds. Ochrony Informacji Niejawnych akceptuje listę osób upoważnionych do pracy z Autonomiczną Stacją Komputerową.

3. Administrator Systemu informatycznego.

Administrator Systemu Teleinformatycznego wykonuje prace niezbędne do efektywnego oraz bezpiecznego zarządzania Autonomiczna Stacją Komputerową w Urzędzie Gminy. Zobowiązany jest on do zapewnienia fachowej pomocy użytkownikom w celu utrzymywania odpowiedniego stanu bezpieczeństwa Stacji Komputerowej, a we współpracy z Inspektorem Bezpieczeństwa Teleinformatycznego prowadzi szkolenia w zakresie bezpieczeństwa przetwarzania. Określa także warunki oraz sposób przydzielania użytkownikom Stacji Komputerowej kont oraz haseł. Administrator Systemu Teleinformatycznego posiada listę użytkowników Autonomicznej Stacji Komputerowej zaakceptowaną przez Pełnomocnika

ds. Ochrony Informacji Niejawnych. Zapewnia dostęp wyłącznie autoryzowanym użytkownikom Stacji Komputerowej na podstawie listy osób uprawnionych do pracy według zarządzenia Wójta Gminy w sprawie określenia stanowisk i osób mogących mieć dostęp w związku z wykonywaną pracą do informacji niejawnych.

4. Użytkownik autonomicznej stacji komputerowej

Jest to osoba posiadająca stosowny dokument bezpieczeństwa osobowego, dopuszczający do pracy z wykorzystaniem Autonomicznego Stanowiska Komputerowego na podstawie listy uprawnionych osób zaakceptowanej przez Pełnomocnika ds. Ochrony Informacji Niejawnych.

5. Informowanie o naruszeniu bezpieczeństwa stacji komputerowej

Wszelkie zauważone przez uzytkownik6w zjawiska mogące naruszyć bezpieczeństwo Stacji Komputerowej, osób, sprzętu, oprogramowania, dokument6w lub bezpieczeństwa fizycznego muszą być niezwłocznie zgłoszone do Administratora Systemu Teleinformatycznego lub Inspektora Bezpieczeństwa Teleinformatycznego.

6. Informowanie o wykryciu wirusa w autonomicznej stacji komputerowej

Przypadki wykrycia wirusa lub nieprawidłowości w pracy Stacji Komputerowej należy zgłosić do Administratora Systemu Teleinformatycznego w celu przeprowadzenia analizy i badania przyczyn nieprawidłowego działania. Po stwierdzeniu obecności wirusa, Administrator Systemu Teleinformatycznego przeprowadza działania zgodne z procedurą antywirusową.

III. BEZPIECZEŃSTWO PERSONELU

1. Informacje ogólne

Każda osoba mająca dostęp do pomieszczenia, w którym znajduje się Autonomiczna Stacja Komputerowa może spowodować jej uszkodzenie lub uzyskać dostęp do informacji niejawnych wyświetlanych na monitorze lub wydrukowanych.

Zagrożenia w stosunku do Stacji Komputerowej mogą pochodzie od każdej osoby posiadającej wystarczające umiejętności i wiedzę pozwalającą na uzyskanie dostępu do Stacji Komputerowej.

2. Użytkownicy autonomicznej stacji komputerowej

Użytkownicy Stacji Komputerowej muszą stosować się do niniejszych Procedur Bezpieczeństwa. Zapoznanie z tymi procedurami użytkownik potwierdza podpisem na liście użytkowników.

Użytkownicy Stacji Komputerowej Urzędu Gminy posiadają odpowiednie dokumenty uprawniające do dostępu do informacji co najmniej o klauzuli "zastrzeżone" oraz korzystają z informacji przechowywanej i przetwarzanej za pośrednictwem Stacji Komputerowej na zasadach wiedzy koniecznej.

Osoba uprawniona do otwierania pomieszczenia, gdzie zainstalowana jest Stacja Komputerowa zobowiązana jest do nadzorowania pracy i wyłączenia Stacji Komputerowej oraz zabezpieczenia pomieszczenia.

Inspektor Bezpieczeństwa Teleinformatycznego oraz Administrator Systemu Teleinformatycznego zobowiązani są do szkolenia użytkowników Stacji Komputerowej oraz egzekwowania przestrzegania Procedur Bezpieczeństwa.

Każdy użytkownik Stacji Komputerowej zobowiązany jest do przestrzegania Procedur Bezpieczeństwa.

Listę użytkowników Stacji Komputerowej posiada Administrator Systemu Teleinformatycznego oraz Inspektor Bezpieczeństwa Teleinformatycznego.

3. Personel sprzątający

Praca personelu sprzątającego może odbywać się pod nadzorem wyznaczonej osoby jedynie wtedy, gdy nie prowadzi się pracy na stanowisku komputerowym, a dokumenty niejawne są schowane.

4. Osoby wizytujące

Osoby wizytujące pomieszczenie, w którym znajduje się Stanowisko Komputerowe mogą w nim przebywać w towarzystwie pracownika uprawnionego do korzystania ze Stacji Komputerowej oraz gdy posiadają uzasadniony powód wizyty lub zezwolenie Wójta.

W trakcie przebywania osób wizytujących nie może odbywać się przetwarzanie informacji niejawnych, a dokumenty i wydruki zawierające informacje niejawne muszą być schowane.

IV. BEZPIECZEŃSTWO FIZYCZNE

1. Informacje ogólne

Informacja przechowywana w zasobach Stacji Komputerowej jest informacją niejawną o klauzuli "zastrzeżone" i jest zabezpieczona w sposób szczególny.

2. Ochrona autonomicznej stacji komputerowej i nośników.

Środki bezpieczeństwa fizycznego są konieczne dla zapobiegania niepowołanemu dostępowi do informacji niejawnej, kontroli dostępu do zasobów oraz w celu zabezpieczenia

sprzętu teleinformatycznego. Pomieszczenie, w którym usytuowane jest Autonomiczne Stanowisko Komputerowe znajduje się Biurze Zarządzania Kryzysowego i Obrony Cywilnej Urzędu Gminy na V piętrze. Dostęp do pomieszczenia ma dwóch pracowników biura.
W pomieszczeniu znajduje się szafa metalowa WBT-0103-01-01, deklaracja zgodności 33/2005, która spełnia wymagania w SWW 0674-2. W szafie przechowywana jest stacja komputerowa, jak również dyski i inne nośniki informacji oraz dokumentacja niejawna.

3. Kontrola dostępu użytkowników do sprzętu.

Dostęp do zasob6w Stacji Komputerowej chroniony jest poprzez stosowanie haseł. Hasło podlega szczególnej ochronie. Użytkownik ma obowiązek tworzenia haseł o długości min. 8 znaków (w tym cyfry). Wymagane jest stosowanie hasła użytkownika przez okres nie dłuższy niż 30 dni lub wymuszenie przez system operacyjny co 30 dni z zastrzeżeniem nie powtarzania użytych haseł. Użytkownik musi zadbać, aby podczas wprowadzania hasła nikt nie obserwował jego klawiatury. Zabrania się udostępniania hasła innym osobom. Hasło zmienia się natychmiast, gdy zostało ujawnione.

4. Zasady kontroli sprzętu.

Administrator Systemu Teleinformatycznego odpowiedzialny jest za okresową kontrolę zgodności stanu faktycznego zainstalowanego sprzętu i oprogramowania z zapisami w Szczególnych Wymaganiach Bezpieczeństwa. Wyniki kontroli zapisuje w stosownej ewidencji kontroli.

V. BEZPIECZEŃSTWO DOKUMENTÓW

1. Informacje ogólne.

Dokumentem jest każda forma nośnika informacji niejawnej, która została wytworzona lub przetworzona za pośrednictwem Stacji Komputerowej. Pojęcie dokumentu obejmuje nośniki papierowe, nośniki magnetyczne i optyczne, dyski twarde oraz pamięci stale.

2. Wymiana informacji.

W przypadku zaistnienia konieczności wymiany informacji z wykorzystaniem wymiennych nosnik6w magnetycznych, z systemem lub siecią teleinformatyczną funkcjonującą w trybie innym niż "zastrzeżone", użytkownik musi postępować dokładnie wg poniższych zasad:

1) informacje jawne mogą być importowane do Stacji Komputerowej z system6w teleinformatycznych z informacjami jawnymi. W tym celu użytkownik zabezpiecza przed zapisem wkładany do napędu nośnik oraz sprawdza na obecność wirusa programem antywirusowym. Użyty nośnik zachowuje swoją klasyfikację jawności;

2) przekazywanie informacji niejawnych z Autonomicznej Stacji Komputerowej do system6w lub sieci teleinformatycznych z informacjami jawnymi jest zabronione.

3. Oznaczenie klasyfikacji dokumentów.

Wszystkie dokumenty zawierające informacje niejawne oznaczane są stosownie do klauzuli tajności informacji, które zawierają. Oznaczenie dokumentu winno być wykonane zgodnie z wymogami zawartymi w ustawie z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U.2019.732 t.j.) oraz rozporządzeniu Ministrów Spraw Wewnętrznych i Administracji oraz Obrony Narodowej z dnia 22 grudnia 2011 r. r. w sprawie sposobu oznaczania materiałów i umieszczania klauzul na nich klauzul tajności (Dz.U.2011.288.1692) Wszystkie dokumenty (wydruki, nośniki magnetyczne dyski twarde) są zakwalifikowane jako informacje niejawne zgodnie z nadaną przez wykonawcę klauzulą tajności. Wydruki niejawne wyprowadzane na drukarkę wykonawca ewidencjonuje i rejestruje w kancelarii materiałów niejawnych.

4. Zmiana klasyfikacji dokumentów.

Nośniki danych zawierające informacje niejawne o klauzuli „zastrzeżone" mogą być deklasyfikowane.

5. Kontrola dokumentów.

Wszystkie dokumenty niejawne muszą być zarejestrowane przez kancelarię materiałów niejawnych. Inspektor Bezpieczeństwa Teleinformatycznego przeprowadza okresowe kontrole użytkowania Stacji Komputerowej. Kontrola okresowa obejmuje w szczególności sprawdzenie przestrzegania przepisów o ochronie informacji niejawnych w zakresie ewidencji i obiegu dokumentów.

6. Niszczenie dokumentów.

Niszczenie dokumentu niejawnego wykonuje się zgodnie z obowiązującymi przepisami w tym zakresie, wykorzystując do tego celu maszyny tnące (niszczarka odpowiedniej klasy). Magnetyczne nośniki danych oznaczone klauzulą "zastrzeżone" podlegają deklasyfikacji. Płyty CD-R1RW oraz uszkodzone nośniki nie podlegają deklasyfikacji i należy je zniszczyć fizycznie.

7. Biblioteka nośników.

Kancelaria Informacji Niejawnych odpowiada za oznakowanie i ewidencję magnetycznych nośników danych użytkowników Stacji Komputerowej.

VI.BEZPIECZEŃSTWO SPRZĘTU I OPROGRAMOWANIA.

1. Informacje ogólne.

Procedury Bezpieczeństwa muszą być ściśle przestrzegane przez uzytkownik6w Autonomicznej Stacji Komputerowej. Wykorzystywanie Stacji Komputerowej do przetwarzania i wykorzystywania nieautoryzowanych, prywatnie wytwarzanych lub pozyskanych danych lub program6w jest zabronione.

2. Bezpieczeństwo sprzętu

Stanowisko komputerowe jest organizacyjnym i technicznym połączeniem elementów komputera, którego skład jest określony w dokumentacji urządzenia. Zmiany lub modyfikacje konfiguracji oprogramowania i sprzętu może dokonać Administrator Systemu Teleinformatycznego.

Administrator Systemu Teleinformatycznego ma obowiązek sprawdzania, czy nie ma zauważalnych oznak manipulowania przy sprzęcie. Wszelkie nieprawidłowości muszą być niezwłocznie zgłoszone Inspektorowi Bezpieczeństwa Teleinformatycznego.

Bezpieczna Stacja Komputerowa podlega rutynowym czynnościom konserwacyjnym oraz przeglądom wykonywanym przez Administratora Systemu Teleinformatycznego. Każdy przegląd jest odnotowywany w dokumentacji Administratora Systemu Teleinformatycznego.

3. Bezpieczeństwo oprogramowania.

Oprogramowanie instaluje wyłącznie Administrator Systemu Teleinformatycznego. Oprogramowanie systemowe i użytkowe przechowuje Administrator Systemu Teleinformatycznego. Używanie oprogramowania nie licencjonowanego oraz nieujętego w wykazie Stacji Komputerowej jest kategorycznie zabronione. Wykaz aktualnie zainstalowanego oprogramowania znajduje się u Administratora Systemu Teleinformatycznego. Administrator Systemu Teleinformatycznego jest zobowiązany do aktualizacji oprogramowania systemowego oraz użytkowego ujętego w Szczególnych Wymaganiach Bezpieczeństwa.

VII. BEZPIECEŃSTWO ŁĄCZNOŚCI

1. Bezpieczeństwo kryptograficzne.

Przy korzystaniu z Autonomicznego Stanowiska Komputerowego w Urzędzie Gminy przetwarzającym informacje o klauzuli "zastrzeżone" nie stosuje się zabezpieczenia kryptograficznego.

2. Bezpieczeństwo elektromagnetyczne.

Bezpieczeństwo elektromagnetyczne obejmuje spos6b lokalizacji element6w łączności, takich jak np. telefony w wymaganej odległości od Stacji Komputerowej oraz zakaz włączania telefon6w komórkowych w pomieszczeniu Autonomicznej Stacji Komputerowej.

3. Bezpieczeństwo transmisji.

Autonomiczne Stanowisko Komputerowe nie ma żńdnych połączeń z innymi systemami lub sieciami teleinformatycznymi.

VIII. MONITOROWANIE BEZPIECZEŃSTWA

Administrator Systemu Teleinformatycznego oraz Inspektor Bezpieczeństwa Teleinformatycznego zobowiązani są do przeprowadzania okresowych kontroli systemu bezpieczeństwa Stacji Komputerowej. Nieprawidłowości lub rozbieżności wykryte podczas kontroli poddane są szczegółowym badaniom. Jeżeli naruszone zostały warunki bezpieczeństwa natychmiast muszą być zgłoszone do Pełnomocnika do Spraw Ochrony Informacji Niejawnych.

IX. KONSERWACJE I NAPRAWY

1. Konserwacje sprzętu i oprogramowania.

Autonomiczne Stanowisko Komputerowe podlega okresowym czynnościom konserwacyjnym oraz przeglądom wykonywanym przez Administratora Systemu Teleinformatycznego.

2. Naprawa sprzętu.

Naprawa urządzeń Stacji Komputerowej wykonywana jest przez uprawniony personel techniczny. Przekazanie urządzenia do naprawy wymaga uzyskania zgody pełnomocnika ochrony. Decyzję o potrzebie wykonania naprawy podejmuje Administrator Systemu Teleinformatycznego po przeprowadzeniu testów diagnostycznych. Przed rozpoczęciem naprawy Administrator Systemu Teleinformatycznego sprawdza, czy wszystkie niejawne materiały zostały usunięte z dysków.

X. PLANY AWARYJNE I ZAPOBIEGAWCZE

1. Zasilanie.

Autonomiczne Stanowisko Komputerowe jest zabezpieczone urządzeniem podtrzymującym zasilanie (zasilacz awaryjny UPS), które jest w stanie utrzymać pracę przez okres do 30 min.

2. Kopie zapasowe.

Kopie archiwalne programów wykonuje i przechowuje Administrator Systemu Teleinformatycznego.

Kopie plików użytkowników wykonują użytkownicy i przechowują w przeznaczonym do tego sejfie.

3. Klęski żywiołowe.

W przypadku wystąpienia klęski żywiołowej (pożaru, powodzi, itp.) należy zastosować się do aktualnie obowiązujących instrukcji przeciwpożarowych i ewakuacyjnych Urzędu Gminy. Podstawową czynnością użytkowników po zakończeniu pracy jest zabezpieczenie nośników informacji i wyłączenie Stacji Komputerowej.

4. Sytuacje specjalne.

W przypadku wystąpienia sytuacji nadzwyczajnych (atak terrorystyczny, zagrożenie ładunkiem wybuchowym, sabotaż itp.) należy zastosować się do aktualnie obowiązujących procedur postępowania zawartych w instrukcji ewakuacyjnej Urzędu Gminy.

XI. POLITYKA ANTYWIRUSOWA

1. Informacje ogólne.

Potrzeba wprowadzenia danych z zewnętrznego nośnika do Autonomicznej Stacji Komputerowej jest zawsze związana z możliwością wprowadzenia wirusa do środowiska, w którym przetwarzane są informacje niejawne. W związku z tym faktem zakupuje się lub aktualizuje oprogramowanie antywirusowe.

W celu możliwie najskuteczniejszego zabezpieczenia się przed wprowadzeniem wirusa do Stacji Komputerowej definiuje się następujące środki zapobiegawcze:

- świadomość użytkownika,
- zasady higieny,
- kontrola dostępu.

2. Świadomość użytkownika.

Świadomość użytkownika o źródłach, sposobach infekcji i działaniu oprogramowania złośliwego jest istotnym celem w ustanawianiu skutecznej polityki antywirusowej.

Zabrania się użytkownikom używania lub uruchamiania nieautoryzowanego oprogramowania oraz danych z nosnik6w niewiadomego pochodzenia. Może to doprowadzić do utraty danych lub ograniczenia funkcjonalności stacji poprzez infekcję stanowiska komputerowego wirusem.

3. Zasady higieny.

Przestrzeganie zasad tzw. higieny komputerowej jest skutecznym sposobem zabezpieczenia Stacji Komputerowej przed atakiem wirusa. W celu ograniczenia możliwości infekcji oprogramowaniem złośliwym użytkownicy są zobowiązani do:

- użytkowania wyłącznie oprogramowania zainstalowanego przez Administratora Systemu Teleinformatycznego;
- nie używania oprogramowania i danych niewiadomego pochodzenia;
- zgłaszania do Administratora Systemu Teleinformatycznego potrzeb w zakresie instalacji dodatkowego oprogramowania;
- sprawdzania zewnętrznych nośników danych programem antywirusowym.

4. Infekcja stacji komputerowej.

Istnieją dwie zasadnicze drogi infekcji stacji komputerowej wirusem:

- używanie zainfekowanego nośnika;
- uruchamianie zainfekowanego oprogramowania.

Dla uniknięcia ww. przypadków infekcji, uruchamianie nieautoryzowanego oprogramowania jest zabronione. W przypadku konieczności skorzystania z nośników informacji, zawsze muszą one przed użyciem być przetestowane na obecność wirusa.

5. Postępowanie w przypadku wykrycia wirusa.

W przypadku wykrycia wirusa, na ekranie wyświetlony zostanie komunikat programu antywirusowego. Użytkownik Stanowiska Komputerowego ma obowiązek niezwłocznie powiadomić osoby funkcyjne systemu teleinformatycznego i wykonać czynności zgodnie ze skróconą instrukcją programu antywirusowego.

Procedura postępowania po wykryciu wirusa komputerowego:

- zapoznać się z treścią komunikatu programu antywirusowego o wykrytym wirusie;
- nie kasować, kopiować, przenosić plików danych i nie niszczyć nośników danych (zachować dowody);
- jeżeli wirus nie został usunięty przez program antywirusowy zaprzestać dalszego przetwarzania informacji;
- powiadomić osoby funkcyjne systemu teleinformatycznego o wykryciu wirusa.

Załącznik Nr 2
do zarządzenia Nr 155/2020
Wójta Gminy Sanok
z dnia 22 lipca 2020r.

WYKAZ UŻYTKOWNIKÓW AUTONOMICZNEGO STANOWISKA KOMPUTEROWEGO

Lp.	Imię i Nazwisko	Stanowisko Referat	Data przydzielenia uprawnień	Data wygaśnięcia uprawnień	Podpis