IV.3 *Załącznik nr 3 – Zakres realizacji audytu IT*

LISTA KONTROLNA			
Nazwa i numer zadania audytowego:	**Zakres realizacji audytu IT**	Nr:	
Wykonał:		Data:	
Organizacja:		Strona:	... / ...

Lp	PYTANIE	TAK	NIE	ND
AUDYT WEWNĘTRZNY IT				
1.	Czy w analizie ryzyka przeprowadzonej przez audyt wewnętrzny uwzględniono zagadnienia IT?			
2.	Czy audyt wewnętrzny realizuje zadania audytowe z zakresu IT?			
3.	Czy audytorzy wewnętrzni realizujący audyt IT są niezależni od Zespołu Informatyki?			
4.	Czy pracownicy odpowiedzialni za audyt informatyczny mają odpowiednie kwalifikacje i doświadczenie?			
5.	Czy Kierownictwo jest informowane o wynikach przeprowadzanych audytów IT?			
6.	Czy zakres audytu IT obejmuje:			
6.1	zarządzanie projektami informatycznymi			
6.2.	środowisko informatyczne			
6.3.	zarządzanie zespołem IT			
6.4.	plany awaryjne			
6.5.	bezpieczeństwo danych			
6.6.	zakupy sprzętu i oprogramowania			
6.7.	utrzymanie sprzętu i oprogramowania			
6.8.	sieci [LAN, WAN]			
6.9.	kontrola zmian oprogramowania			
6.10.	ocena zgodności działań w obszarze IT z obowiązującymi przepisami			
7.	Czy istnieje procedura wymiany informacji pomiędzy Zespołem Informatyki a audytem wewnętrznym w sytuacjach kryzysowych?			
AUDYT ZEWNĘTRZNY IT				
1.	Czy w ciągu ostatnich 3 lat był przeprowadzony audyt informatyczny przez audytora zewnętrznego?			
2.	Czy audyt zewnętrzny zakończony został raportem, w którym przedstawiono rekomendacje dotyczące obszaru IT?			
3.	Czy rekomendacje audytora zewnętrznego zostały zrealizowane?			
4.	Czy zakres audytu IT przeprowadzonego przez audytora zewnętrznego obejmował:			
4.1.	zarządzanie projektami informatycznymi			
4.2.	zarządzanie zespołem IT			
4.3.	plany awaryjne			

LISTA KONTROLNA				
Nazwa i numer zadania audytowego:	**Zakres realizacji audytu IT**		Nr:	
Wykonał:			Data:	
Organizacja:			Strona:	... / ...

LP	PYTANIE	TAK	NIE	ND
4.4.	bezpieczeństwo danych			
4.5.	zakupy sprzętu i oprogramowania			
4.6.	utrzymanie sprzętu i oprogramowania			
4.7.	sieci [LAN, WAN]			
4.8.	kontrolę zmian oprogramowania			
4.9.	ocenę zgodności działań IT z obowiązującymi przepisami			

.....
Podpis audytora

.....
Podpis audytowanego

IV.4 *Załącznik nr 4 – Karta zasobów stanowiska komputerowego*

KARTA OBOWIĄZUJĄCYCH PRACOWNIKA ZASOBÓW INFORMATYCZNYCH I TECHNICZNYCH STANOWISKA KOMPUTEROWEGO			
Data wypełnienia karty		**Wypełniający kartę**	
Dane pracownika			
Imię i nazwisko Nr ewidencyjny			Identyfikator:
Stanowisko			
Bezpośredni przełożony			
Dane kontaktowe	Tel: pokój: Mail:		
Stacja robocza			
Identyfikacja stacji	Komputer: nr ewidencyjny		Monitor: nr
Identyfikator użytkownika	Nazwa sieciowa komputera:		Drukarka: nr
Podstawowa Identyfikacja techniczna komputera-model-typ-wielkość	☐ Procesor		
	☐ Dyski twarde		
	☐ Pamięć RAM		
	☐ CD / CDRW		
	☐ Płyta główna		
	☐		
	☐		
Zainstalowane Aplikacje jako standard dla stacji roboczej	☐ Word	Nr	
	☐ Excel	nr	
	☐ Power-Point	nr	
	☐ Open office	Oprogramowanie typu :	
	☐ LEX	nr	
	☐	.....	
	☐ Poczta elektroniczna :	☐ Rodzaj: Adres:	
	☐ Antywirus		

	☐ Antyspamer	
	☐ Firewall	
	☐ Acrobat Reader	
	☐	
Aplikacje nad standard a zatwierdzone	☐	
	☐	
	☐	
	Uwagi:	

Uprawnienia – udziały sieciowe i usługi		
odczyt/zapis/ modyfikacja	Dostęp do dysków lokalnych:	☐
odczyt/zapis/ modyfikacja	Dostęp do dysków sieciowych:	☐
System operacyjny	Typ- Rodzaj	☐
	Nr klucza:	
	Nr licencji	

Hasła twarde	☐ Do Admin. systemu	☐ Do BIOS	☐ Stacji roboczej

Dostęp do innych przydzielonych własnych zasobów technicznych

Rodzaj zasobu		Nazwa i model	Nr ewidencyjny	Uwagi
Telefon	☐			
Telefon GSM	☐			
Fax	☐			
Kserokopiarka	☐			
Drukarki	☐			
Pendrive	☐			
Monitor	☐			
Dostęp do internetu	☐	MAC:	IP:	ograniczony
Karta wejścia-wyjścia	☐	nr		

Dostęp do internetu oraz poczty elektronicznej jest **monitorowany i nadzorowany** poprzez zapisy logów, daty, czasu i adresu w trybie on-line. Dostęp ten jest ograniczony poprzez ABI.

Lokalizacja zapisu lokalnych plików tekstowych i innych materiałów służbowych: *podaj ścieżki*

Zakres dostępu do stron internetowych:			
☐ Sejm i Senat ☐ Ministerstwa	☐ WSA, ☐NSA, ☐LEX ☐ Antywirus	☐ onet.pl; ☐ wp.pl	☐ inne: *wymień jakie*
Uprawnienia *Użytkownik ma blokowane wszystkie pozycje*	☐ Blokada w BIOS napędu CD / CDRW ☐ Blokada w BIOS napędu FDD ☐ Blokada uprawnień w Windows do zmiany rejestru przy instalacji nowego oprogramowania ☐ Brak uprawnień do funkcji ADMINISTRATORA w Windows		

Zatwierdzenia końcowe	
Wnioskujący o nadanie uprawnień	ADO:
Zatwierdzający nadanie uprawnień	ABI:
Realizujący wpisy uprawnień	ASI:
Pracownik	Potwierdzam zapoznanie się z przydzielonym mi przydzielonym zakresem uprawnień. Zobowiązuję się do nieujawniania przekazanych mi haseł dostępu do maszyny/systemu / aplikacji. Zobowiązuję się do zachowania odpowiedniej dbałości o przekazane mi zasoby. Zobowiązuje się do bezwzględnego stosowania zasady użytkowania powierzonych mi zasobów tylko i wyłącznie do celów służbowych Podpis pracownika

Informacje o zasadach stosowania przydzielonych uprawnień oraz zasadach monitoringu:

- stacja robocza przeznaczona jest wyłącznie do prac i czynności służbowych
- stacja robocza może zawierać tylko i wyłącznie oprogramowanie ujęte w standardzie karty zasobów
- Instalowanie innego zasobu informatycznego (dowolnego typu oprogramowania) poza udostępnionym i wskazanym w karcie zasobu stacji jest zabronione
- rozszerzenie zasobu oprogramowania poprzez dodatkową instalację może nastąpić tylko i wyłącznie wnioskiem i uzasadnieniem pracownika, a zgodą ABI i dokonane przez ASI. Fakt instalacji dodatkowego oprogramowania musi być ujęty jako zapis w karcie zasobów
- na służbowej stacji roboczej zabronione jest przechowywanie jakichkolwiek **własnych, prywatnych** plików typu doc, bmp, PDF, JPG, mp3, mp4, avi, waw (zdjęcia, muzyka, e-booki, teksty, filmy)
- zabronione jest użytkowanie oprogramowania typu P2P oraz komunikatorów (np. gadu-gadu, skype itp.)
- na służbowej stacji roboczej zabronione jest przeglądanie jakichkolwiek **własnych, prywatnych** plików typu doc, bmp, PDF, JPG, mp3, mp4, avi, waw (zdjęcia, muzyka, e-booki, teksty, filmy, korespondencji mailowej)
- poczta elektroniczna oraz przydzielone skrzynki pocztowe mogą być wykorzystywane tylko i wyłącznie do korespondencji służbowej: jej wysyłania i odbierania. Poczta elektroniczna wraz z dostępem do Internetu jest monitorowana przez służby informatyczne urzędu wraz z prowadzonym zapisem logów.

Przyjmuję określony stan do wiadomości i akceptuję jako obowiązujące – podpis pracownika

Daty i podpisy

Podpis prowadzącego ABS data:

Przydzielony lub działający zasób należy potwierdzić „krzyżykiem w kratce" - ☒

IV.5 *Załącznik nr 5 – Zadania i obowiązki administratora systemu lub sieci teleinformatycznej*

Urząd Gminy Wilkowice	**PROCEDURA BEZPIECZEŃSTWA**	Data: Wersja:
Tytuł:	**ZADANIA I OBOWIĄZKI ADMINISTRATORA SYSTEMU LUB SIECI TELEINFORMATYCZNEJ**	Strona ... z ...

Administrator systemu lub sieci teleinformatycznej odpowiada za:

1) codzienną obsługę techniczną systemu lub terminala;
2) sprawdzenie poprawności działania systemu;
3) opracowywanie projektów szczególnych wymagań bezpieczeństwa systemu lub sieci teleinformatycznej oraz propozycji ich uaktualnienia;
4) wdrażanie procedur bezpieczeństwa oraz nadzór nad funkcjonowaniem systemu lub sieci teleinformatycznej;
5) wdrażanie procedur ochrony antywirusowej;
6) opracowanie planów awaryjnych i planu napraw systemu lub sieci teleinformatycznej;
7) informowanie pełnomocnika ochrony oraz właściwego organu bezpieczeństwa systemów łączności i informatyki o stwierdzonych naruszeniach bezpieczeństwa systemu, sieci teleinformatycznej oraz wykrytych wirusach;
8) proponowanie zmian mających na celu poprawę bezpieczeństwa systemu lub sieci teleinformatycznej.

Ponadto:

9) jest odpowiedzialny za bezpieczeństwo oraz prawidłowe funkcjonowanie systemu komputerowego;
10) zapewnia by wszyscy użytkownicy stosowali się do Procedur Bezpieczeństwa;
11) utrzymuje i aktualizuje listę autoryzowanych użytkowników systemu komputerowego;
12) upewnia się, czy cały personel posiadający dostęp do systemu komputerowego posiada stosowne dopuszczenia do pracy z informacją niejawną – w przypadku dostępu do systemu komputerowego osób nie posiadających stosownych dopuszczeń, zapewnia odpowiednie zabezpieczenie systemu komputerowego;
13) prowadzi osobiście lub nadzoruje profilaktykę antywirusową systemu komputerowego;
14) prowadzi nadzór sprzętu oraz oprogramowania pod kątem kontroli nieuprawnionych zmian ich konfiguracji;
15) zatwierdza oraz akceptuje wszelkie zmiany w konfiguracji sprzętu lub oprogramowania mające wpływ na bezpieczeństwo systemu komputerowego;
16) dokonuje analizy zgłoszonych przypadków incydentów infekcji wirusowych lub innych, wskazujących na nieautoryzowane próby ingerencji w systemie bezpieczeństwa oraz,

w zależności od stopnia zagrożenia funkcjonowania systemu bezpieczeństwa, podejmuje odpowiednie kroki zaradcze zapewnienie strategii, uregulowań i procedur bezpieczeństwa;

17) przeprowadza okresowe kontrole klasyfikowanych mediów magnetycznych, poprawności ich opisu oraz utrzymuje ewidencję tych kontroli;

18) zabezpiecza niszczenie niejawnych odpadów w regularnych odstępach czasu, zgodnie z obowiązującymi procedurami;

19) doradza użytkownikom systemu komputerowego w zakresie bezpieczeństwa;

20) prowadzi szkolenia użytkowników z zakresu bezpieczeństwa systemu komputerowego lub występuje z wnioskiem o przeprowadzenie szkolenia użytkowników z zakresu bezpieczeństwa systemu komputerowego;

21) wykonuje archiwizację danych systemu komputerowego, zgodnie z obowiązującymi procedurami;

22) doskonali się z zakresu wiedzy o bezpieczeństwie systemu komputerowego;

23) dokonuje analizy zagrożeń oraz ryzyka i melduje do Pionu Ochrony o wszelkich wykrytych lukach, naruszeniach i zagrożeniach.

Pieczęć	*Data:*	*Zatwierdził:* Podpis:

IV.6 *Załącznik nr 6 – Oświadczenie administratora serwisu*

Urząd Gminy Wilkowice	**PROCEDURA BEZPIECZEŃSTWA**	Data: Wersja:
Tytuł:	**Oświadczenie administratora serwisu**	Strona ... z...

Oświadczenie składa:

Nazwisko	
Imię	
Stanowisko	
Funkcja	
Firma	
Adres	
Tel. stacjonarny	
Tel. Komórkowy	
Adres e-mail	

iż:

1. zgodnie z zakresem obowiązków nałożonych i zaakceptowanych na podstawie opisu z procedury bezpieczeństwa – Zadania i obowiązki administratora sieci i systemu informatycznego i zawartej umowy o nadzorze technicznym obowiązują mnie wszelkie normy bezpieczeństwa i ochrony danych obowiązujące w Urzędzie Gminy Wilkowice

2. w przypadku koniecznym i niezbędnym co do serwisu powierzonego mi sprzętu w ramach realizacji zadań umowy poza siedzibą urzędu sprzęt **ten może być pobrany tylko i wyłącznie na podstawie procedury i poświadczony protokołem odbiorczym za zgodą na przemieszczenie danych**, a zwrócony z protokołem zdawczym wraz z opisem wykonanych czynności. Ochronie szczególnej podlegają dane na nośnikach odebranych ze sprzętem (dyski twarde, zipy, pamięci masowe itp.) W związku z powyższym czynności serwisowe mogą być wykonywane tylko przez uprawnionych i wskazanych oświadczeniem pracowników firmy.

3. posiada możliwości techniczne i prawne co do zachowania bezpieczeństwa i ochrony nad powierzonym sprzętem i danymi na nośnikach elektronicznych.

4. w przypadku ujawnienia danych przekazanych lub ich zaginięcia, ze względu na niedochowanie warunków procedur bezpieczeństwa i ochrony wszelkie konsekwencje prawne, finansowe ponoszę osobiście i bezwarunkowo akceptuję ich skutki.

Pieczęć	Data:	Administrator serwisu Nazwisko: Podpis:

IV.7 *Załącznik nr 7 – Oświadczenie pracownika urzędu*

OŚWIADCZENIE dotyczące Polityki Bezpieczeństwa Informatycznego

Urzędu Gminy Wilkowice

..... dnia .....

Ja - niżej podpisany(a) - pracując na sprzęcie komputerowym Urzędu Gminy Wilkowice, zlokalizowanym w zajmowanym przeze mnie pokoju lub przekazanym mi w wyłączne użytkowanie zobowiązuję się:

1. niezależnie od okoliczności, nie udostępniać nikomu haseł dostępowych do przydzielonych mi zasobów - sieci, aplikacji, poczty elektronicznej, wiedząc, że każdy pracownik podejmujący pracę w Urzędzie Gminy Wilkowice otrzymuje indywidualne identyfikatory i hasła dostępowe pozwalające na pracę w zakresie przydzielonych mu uprawnień,
2. używać wyłącznie oprogramowania zainstalowanego przez informatyka będącego jednocześnie Administratorem Bezpieczeństwa Systemu (ASI) Urzędu Gminy Wilkowice lub dostarczonego przez administrację państwową w celu realizacji zadań przez nią zleconych,
3. nie instalować programów pochodzących z innych źródeł, ani nie udostępniać programów będących własnością Urzędu Gminy Wilkowice,
4. w przypadku wątpliwości co do legalności bądź funkcji (celu zastosowania) oprogramowania zainstalowanego na moim dysku zgłaszać ten fakt Sekr etarzowi Urzędu Gminy Wilkowice notatk ą służbową, w celu pozostawienia zapisu zgłoszenia,
5. dbać o bezpieczeństwo zgromadzonych zasobów przez dokonywanie zapisu istotnych danych na zasobach sieciowych, które są centralnie archiwizowane,
6. dbać o bezpieczeństwo wszystkich danych, do których posiadam dostęp, zarówno na dyskach lokalnych, jak i na dyskach sieciowych oraz wymienialnych nośnikach danych,
7. nie używać oprogramowania oraz zasobów nie mających żadnego związku z wykonywaną przeze mnie pracą,
8. sprawdzać przy pomocy aktualnego programu antywirusowego zakupionego przez Urząd, czy wszystkie używane przeze mnie wymienialne nośniki danych nie są zawirusowane,
9. wszelkie usterki zgłaszać do Sekretarza Urzędu Gminy Wilkowice drogą mailową lub zgodnie z procedurą notatką służbową
10. przestrzegać przepisów ustawy o prawie autorskim i prawach pokrewnych (ustawa z dnia 4 lutego 1994r. - tekst jednolity Dz. U. z 2000 r nr 80, poz. 904 z późniejszymi zmianami).
11. in formować Sekretarza Urzędu Gminy Wilkowice o wszelkich zmianach dotyczących konfiguracji i lokalizacji sprzętu komputerowego.
12. przejmo wać pełną odpowiedzialność prawną na okoliczność dostępu do dokumentów i związanej z tym informacją, także w trybie dokumentu elektronicznego, szczególnie w przypadku dysponowania dokumentami poza siedzibą urzędu,
13. zacho wać bezwzględną i bezterminową tajemnicę służbową z obszaru dostępu do informacji i baz danych na okoliczność rozwiązania stosunku pracy i podległości służbowej.

Korzystanie z komputerów przenośnych w celu wykonywania czynności związanych z dostępem do danych osobowych lub dokumentów znajdujących się w elektronicznym obiegu możliwe jest wyłącznie w trybie terminalowym, z użyciem silnie szyfrowanego kanału VPN. Osoba używająca komputera przenośnego powinna zapewnić sobie warunki pracy uniemożliwiające niekontrolowany wgląd osób postronnych w przetwarzane dane.

Przyjmuję do wiadomości, że ponoszę pełną odpowiedzialność za stan i bezpieczeństwo danych oraz programów zainstalowanych na dyskach twardych używanych przeze mnie - zgodnie z przyjętymi wyżej zasadami - komputerów. Równocześnie przyjmuję do wiadomości, że Administrator Bezpieczeństwa Systemów Informatycznych (ASI) wraz z Sekretarzem Urzędu Gminy Wilkowice może dokonywać bieżącej kontroli (bez ingerencji w zawartość) zasobów użytkowanych przeze mnie komputerów i sporządzania raportów z kontroli.

Oświadczam, iż miał(a)em możliwość zapoznania się z dokumentem Polityki Bezpieczeństwa wraz z ujętymi tam podstawami obowiązującego prawa oraz uczestnictwa w szkoleniu z zakresu tej dokumentacji i stosowania zasad Polityki Bezpieczeństwa.

Jestem świadomy/a, iż w przypadku nieprzestrzegania zawartych w oświadczeniu zasad zostaną wyciągnięte sankcje służbowe wynikające z przepisów prawa pracy oraz pozostałych ustaw i rozporządzeń z obszaru nadzoru nad bezpieczeństwem informacji.

Imię , nazwisko pracownika .....

Stanowisko .....

Zatrudniony na podstawie .....

Miejscowość, dnia .....

Podpis .....