WÓJT
GMINY WIENIAWA

Zarządzenie 109/2017

Wójta Gminy Wieniawa z dnia 28 grudnia 2017 r., w sprawie powołania zespołu do przeprowadzenia weryfikacji polityki bezpieczeństwa obowiązującej w Urzędzie Gminy w Wieniawie

Na podstawie art. 33 ust. 1, ust. 3 i ust. 5 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (t.j. Dz. U. z 2017 r. poz. 1875), w związku z art. 26 ust. 1 pkt 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2016 r. poz. 922) oraz § 4 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r., Nr 100, poz. 1024)

§ 1

Powołuję zespół do przeprowadzenia weryfikacji polityki bezpieczeństwa obowiązującej w Urzędzie Gminy w Wieniawie, przyjętej Zarządzeniem Wójta Gminy Wieniawa nr 62/2007 z dnia 10 grudnia 2017r., w sprawie opracowania „Polityki Bezpieczeństwa dla systemu SOO" oraz „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w systemie SSO", w następującym składzie:

1. Edyta Wielgo – Przewodniczący Zespołu
2. Paweł Kołtonowicz – Zastępca Przewodniczącego
3. Magdalena Lipińska – Członek Zespołu
4. Karolina Kępczyńska – Członek Zespołu
5. Katarzyna Banasik – Członek Zespołu
6. Anna Tokarz – Członek Zespołu
7. Ewelina Augustyniak – Członek Zespołu
8. Marzena Siara – Członek Zespołu

§ 2

Zobowiązuje się Zespół do:

1. Dokonania analizy Polityki Bezpieczeństwa obowiązującej w Urzędzie Gminy w Wieniawie
2. Przeprowadzenia audytu ochrony danych osobowych według załączników 1-6, do niniejszego zarządzenia.
3. Sporządzenia protokołu prac komisji zawierającego wyniki audytu i wnioski oraz zalecenia do realizacji
4. Protokół z prac zespołu, zawierający wyniki audytu, należy przedstawić Wójtowi Gminy Wieniawa, do dnia 09 stycznia 2018r.

§ 3

Wykonanie zarządzenia zleca się Przewodniczącemu Komisji.

§ 4

Zarządzenie wchodzi w życie z dniem podpisania.

GMINY WIENIAWA WÓJT

WÓJT

mgr inż. Krzysztof Sobczak

Załącznik nr 1

Dzień 1

Przedział czasowy	**Dział/obszar**	**Wstępny zakres wywiadu audytowego**
30 minut	Spotkanie otwierające	Cele audytu, zasady współpracy, przepływ informacji itp. Odpowiedzi na pytania uczestników.
90–120 minut	Informatyzacja	Zabezpieczenia infrastruktury IT, inwentaryzacja aplikacji – lista, funkcjonalności, zabezpieczenia.
30–60 minut	Referat Finansowy	Zakres przetwarzanych danych, przesłanki dopuszczalności, obowiązki informacyjne, dostęp do danych klientów (podstawa), udostępnianie danych, bezpieczeństwo fizyczne danych osobowych.
60 minut	Referat Gospodarki Nieruchomościami Rolnictwa i Ochrony Środowiska	Zakres przetwarzanych danych, przesłanki dopuszczalności, obowiązki informacyjne, dostęp do danych klientów (podstawa), udostępnianie danych, bezpieczeństwo fizyczne danych osobowych.
60 minut	Opłaty za wodę, ścieki i odpady komunalne	Zakres przetwarzanych danych, przesłanki dopuszczalności, obowiązki informacyjne, dostęp do danych klientów (podstawa), udostępnianie danych, bezpieczeństwo fizyczne danych osobowych.
60 minut	USC	Zakres przetwarzanych danych, przesłanki dopuszczalności, obowiązki informacyjne, dostęp do danych klientów (podstawa), udostępnianie danych, bezpieczeństwo fizyczne danych osobowych.
30–60 minut	Referat Zamówień Publicznych Inwestycji Oświaty i Sportu	Zakres przetwarzanych danych, przesłanki dopuszczalności, obowiązki informacyjne, dostęp do danych klientów (podstawa), udostępnianie danych, bezpieczeństwo fizyczne danych osobowych.

WÓJT

mgr inż. Krzysztof Sobczak

Dzień 2

Przedział czasowy	**Dział/obszar**	**Wstępny zakres wywiadu audytowego**
30–60 minut	Kadry i Płace	Zakres przetwarzanych danych, przesłanki dopuszczalności, obowiązki informacyjne, dostęp do danych klientów (podstawa), udostępnianie danych, bezpieczeństwo fizyczne danych osobowych.
30 minut	Sekretariat	Zakres przetwarzanych danych, przesłanki dopuszczalności, obowiązki informacyjne, dostęp do danych klientów (podstawa), udostępnianie danych, bezpieczeństwo fizyczne danych osobowych.
15 minut	Referat Organizacyjny	Zakres przetwarzanych danych, przesłanki dopuszczalności, obowiązki informacyjne, dostęp do danych klientów (podstawa), udostępnianie danych, bezpieczeństwo fizyczne danych osobowych.
15 minut	Punkt Obsługi Beneficjenta	Zakres przetwarzanych danych, przesłanki dopuszczalności, obowiązki informacyjne, dostęp do danych klientów (podstawa), udostępnianie danych, bezpieczeństwo fizyczne danych osobowych.
60-90 minut	Jednostki Organizacyjne obsługiwane w UG, w zakresie usług finansowo księgowych	Zakres przetwarzanych danych, przesłanki dopuszczalności, obowiązki informacyjne, dostęp do danych klientów (podstawa), udostępnianie danych, bezpieczeństwo fizyczne danych osobowych.

Załącznik nr 2

Ankieta dotycząca bezpieczeństwa obszaru, w którym przetwarzane są dane osobowe

W jaki sposób zabezpieczony jest fizyczny dostęp do biura (np. poprzez drzwi antywłamaniowe, dostęp na kartę)?
[W przypadku biura znajdującego się na parterze] Czy okna zostały zabezpieczone np. kratami, roletami lub folią antywłamaniową?
Czy biuro jest zabezpieczone systemem alarmowym? Jeśli tak, to kto jest informowany o aktywacji alarmu?
Czy biuro jest zabezpieczone poprzez monitoring? Jeśli tak, to kto sprawuje nadzór nad monitoringiem?
Czy biuro jest chronione przez pracowników ochrony w czasie nieobecności pracowników (po godzinach pracy)? Czy (ewentualnie) mają Państwo podpisaną z firmą ochroniarską umowę zobowiązującą patrol interwencyjny do gotowości i przyjechania do biura w razie konieczności interwencji?
Czy dane osobowe przetwarzane papierowo są przechowywane w zamykanej szafie (szafach): drewnianej, metalowej, pancernej, sejfie [wybrać właściwe]?
Czy biuro jest wyposażone w system przeciwpożarowy lub gaśnicę?
Czy w biurze znajduje się niszczarka dokumentów?
Czy są jakieś osoby/podmioty, które mają dostęp do biura przed lub po godzinach pracy (np. firma sprzątająca)?
[W przypadku istnienia osób/podmiotów, o których mowa w pkt powyżej] Czy zawarto stosowne umowy, w których znajdują się zapisy dotyczące konieczności zapewnienia poufności wszystkich danych znajdujących się w biurze? Proszę o przytoczenie stosownego zapisu.

WÓJT

mgr inż. Krzysztof Sobczak

Załącznik nr 3

Ankieta dotycząca zabezpieczeń serwerowni

Czy serwerownia stanowi wyodrębnione pomieszczenie, oddzielone od innych pomieszczeń zlokalizowanych w budynku?
Czy serwerownia ma okna? Jeśli tak, to w jaki sposób je zabezpieczono?
Ile jest wejść do serwerowni? Czy drzwi do serwerowni są wyposażone w zamki? Czy prowadzona jest kontrola dostępu?
Kto ma dostęp do serwerowni? Jakie są zasady przebywania w serwerowni przez osoby nieuprawnione (np. z firm serwisujących urządzenia)?
Czy jest prowadzona ewidencja osób wchodzących do serwerowni?
Czy w serwerowni jest prowadzony monitoring? Kto ma do niego dostęp?
Jakie zabezpieczenia przeciwpożarowe zastosowano w serwerowni?
Czy serwerownia została wyposażona w urządzenia klimatyzacyjne? Czy jest prowadzony pomiar temperatury/wilgotności?
Czy i w jaki sposób serwery zostały zabezpieczone przed awarią, taką jak brak prądu, przepięcia itd. (np. UPS, spalinowy generator prądu)?

WÓJT

mgr inż. Krzysztof Sobczak

Załącznik 4

Ankieta dotycząca komputerów i urządzeń mobilnych wykorzystywanych do przetwarzania danych

Uprawnienia

Kto nadaje uprawnienia dostępu do komputerów wykorzystywanych przez spółkę? Jaka jest formalna bądź nieformalna procedura postępowania w tym zakresie?
Kto odbiera uprawnienia dostępu do komputerów wykorzystywanych przez spółkę? Jaka jest formalna bądź nieformalna procedura postępowania w tym zakresie?
Na jakiego rodzaju kontach pracują pracownicy (konto administratora, użytkownika)?

Uwierzytelnienie

Czy uwierzytelnienie do systemu operacyjnego wymaga podania loginu?
Czy uwierzytelnienie do systemu operacyjnego wymaga podania hasła?
Z ilu znaków składa się hasło?
Czy znaki stosowane w haśle to kombinacja zawierająca wielką i małą literę oraz znak specjalny bądź cyfrę?
Czy hasło jest zmieniane? Jeśli tak, to jaka jest częstotliwość zmiany hasła?

Ochrona przed szkodliwym oprogramowaniem

Czy stosowane jest oprogramowanie antywirusowe? Jeśli tak, to proszę o podanie nazwy programu.
Czy stosowane jest oprogramowanie typu *firewall*? Jeśli tak, to proszę o podanie jego nazwy.
Czy oprogramowanie antywirusowe jest zarządzane w sposób centralny (konsola)?

Czy użytkownik może samodzielnie odinstalować oprogramowanie antywirusowe / *firewall*?
Czy użytkownik może samodzielnie dezaktywować skaner antywirusowy?
Czy stosowane są jeszcze jakieś inne zabezpieczenia programowe niż oprogramowanie antywirusowe i *firewall* (np. oprogramowanie antyspamowe)?
Czy pracownik może samodzielnie instalować oprogramowanie na swoim komputerze?

Kopie zapasowe dla zasobów przechowywanych na komputerach

Czy wykonywane są kopie zapasowe dla zasobów przechowywanych na komputerach?
Jaka jest częstotliwość wykonywania kopii zapasowych (dzienna, tygodniowa, miesięczna itd.)?
Na jakim nośniku wykonuje się kopie (kasetki streamera, dysk zewnętrzny, FTP, mirroring na drugi dysk itd.)?
Proszę wskazać sposób wykonywania kopii zapasowych (np. kopie pełne, przyrostowe).
Proszę wskazać miejsce przechowywania kopii zapasowych.
Kto posiada dostęp do kopii zapasowych?

Komputery przenośne (laptopy). Praca zdalna

Czy komputery przenośne zostały wyposażone w oprogramowanie zapewniające szyfrowanie danych (szyfrowany dysk, szyfrowana partycja)?
Czy w organizacji dopuszczalna jest praca zdalna? Jeśli tak, to jakie trzeba spełnić warunki techniczne oraz kto i w jakiej formie wyraża zgodę na ten rodzaj pracy?

Nośniki danych

Czy spółka stosuje nośniki danych typu pendrive?
Czy nośniki typu pendrive są zabezpieczone (np. poprzez szyfrowanie)?
Czy dopuszczalne jest korzystanie z własnych nośników typu pendrive?
W jaki sposób niszczone są stare/zepsute dyski twarde?

Urządzenia mobilne (smartfony, tablety)

W jaki sposób zostały zabezpieczone urządzenia mobilne (hasło, szyfrowanie danych, antywirus, zdalny dostęp z możliwością wyczyszczenia danych itd.)?

WÓJT

mgr inż. Krzysztof Sobczak

Załącznik 5

Ankieta dotycząca aplikacji wykorzystywanych do przetwarzania danych

Uprawnienia

Kto nadaje uprawnienia dostępu do aplikacji? Jaka jest formalna bądź nieformalna procedura postępowania w tym zakresie?
Kto odbiera uprawnienia dostępu do aplikacji? Jaka jest formalna bądź nieformalna procedura postępowania w tym zakresie?
Czy aplikacja umożliwia przydzielanie zróżnicowanych poziomów uprawnień? Jeśli tak, to proszę wskazać stosowane poziomy uprawnień.

Uwierzytelnienie

Czy uwierzytelnienie do aplikacji wymaga podania loginu?
Czy uwierzytelnienie do aplikacji wymaga podania hasła?
Z ilu znaków składa się hasło?
Czy znaki stosowane w haśle to kombinacja zawierająca wielką i małą literę oraz znak specjalny bądź cyfrę?
Czy hasło jest zmieniane? Jeśli tak, to jaka jest częstotliwość zmiany hasła?
[W przypadku gdy aplikacja jest dostępna przez przeglądarkę] Czy proces uwierzytelniania do aplikacji oraz praca w niej są szyfrowane, np. protokołem SSL (https)?

Kopie zapasowe dla zasobów przechowywanych na komputerach

Czy wykonywane są kopie zapasowe?
Jaka jest częstotliwość wykonywania kopii zapasowych (dzienna, tygodniowa, miesięczna itd.)?
Na jakim nośniku są wykonywane kopie (kasetki streamera, dysk zewnętrzny, FTP, mirroring na drugi dysk itd.)?
Proszę wskazać sposób wykonywania kopii zapasowych (np. kopie pełne, przyrostowe).
Proszę wskazać miejsce przechowywania kopii zapasowych.
Czy miejsce przechowywania kopii zapasowych pokrywa się z miejscem usytuowania serwerów, których zasoby podlegają backupowi?
Kto posiada dostęp do kopii zapasowych?

Funkcjonalności aplikacji

Czy aplikacja zapewnia funkcjonalność polegającą na automatycznym odnotowaniu daty pierwszego wprowadzenia danych do bazy danych?
Czy aplikacja zapewnia funkcjonalność polegającą na automatycznym odnotowaniu identyfikatora (loginu) użytkownika (pracownika) wprowadzającego dane osobowe do bazy danych?
Czy aplikacja zapewnia funkcjonalność polegającą na odnotowaniu źródła zbieranych danych, w przypadku gdy nie jest nim osoba, której dotyczą (np. w przypadku zakupu bazy danych)? Czy (ewentualnie) jest jakieś pole, w którym można ręcznie wpisać takie dane?
Czy aplikacja zapewnia funkcjonalność polegającą na odnotowaniu informacji o odbiorcach (innych administratorach danych osobowych, np. klientach/partnerach firmy), którym dane osobowe zostały udostępnione, oraz o dacie i zakresie tego udostępnienia?
Czy aplikacja zapewnia funkcjonalność polegającą na odnotowaniu sprzeciwu na przetwarzanie danych w celach marketingowych oraz na przekazywanie danych do innych administratorów danych osobowych? Czy (ewentualnie) jest jakieś pole, w którym można ręcznie wpisać takie informacje?
Czy można wygenerować raport dla pojedynczego rekordu, zawierający informacje wskazane w pkt powyżej?

WÓJT

mgr inż. Krzysztof Sobczak

Załącznik 6

Wykaz kopii zapasowych

Nazwa aplikacji, dla której wykonywana jest kopia / wskazanie, co podlega backupowi	
Sposób wykonania kopii zapasowej (kopia pełna/przyrostowa/różnicowa)	
Rodzaj nośnika, na którym wykonywana jest kopia	
Częstotliwość wykonywania kopii	
Czas przechowywania kopii	
Miejsce przechowywania kopii i sposób jej zabezpieczenia	
Osoba odpowiedzialna za wykonywanie kopii	
W jaki sposób pracownik wykonujący kopie dowiaduje się o poprawnym ich wykonaniu	

WÓJT

mgr inż. Krzysztof Sobczak