OPIS STANOWISKA PRACY
I PROFILU WYMAGAŃ KWALIFIKACYJNYCH NA STANOWISKO
Administratora

w Referacie Organizacyjnym w Urzędzie Gminy w Sadkach

NAZWA STANOWISKA	KOMÓRKA ORGANIZACYJNA
Administrator	**RO**
LICZBA PODLEGŁYCH PRACOWNIKÓW	**OSOBY PODLEGAJĄCE**
0	0
BEZPOŚREDNI PRZEŁOŻONY	Sekretarz Gminy Kierownik Referatu Organizacyjnego

CEL STANOWISKA

Zapewnienie prawidłowego i bezpiecznego funkcjonowania systemu informatycznego i prowadzenie gospodarki zaopatrzeniowej w materiały biurowe i środki czystości w Urzędzie.

ZAKRES ZADAŃ

1. Zakres wykonywanych zadań na stanowisku, w szczególności:

1) zarządzanie systemem informatycznym, w którym przetwarzane są informacje chronione, posługując się hasłem dostępu do wszystkich stacji roboczych z pozycji administratora,
2) przeciwdziałanie dostępowi osób niepowołanych do systemu informatycznego, w którym przetwarzane są informacje chronione,
3) analizowanie tendencji rozwojowych technologii informatycznych i technik bezpieczeństwa, pod kątem podatności, zagrożeń i zabezpieczeń,
4) okresowe raportowanie o stanie bezpieczeństwa systemów teleinformatycznych, odnotowanych incydentach bezpieczeństwa oraz statusie podejmowanych działań w odpowiedzi na incydenty,
5) przygotowanie procedur określających zasady zarządzania systemami lokalnymi,
6) przygotowanie procedur bezpieczeństwa danego systemu przetwarzania informacji,
7) formułowanie, w uzgodnieniu z Administratorem Danych Osobowych i/lub osobami upoważnionymi przez Administratora Danych Osobowych uprawnień w systemach informatycznych,
8) realizowanie decyzji Administratora Danych Osobowych dotyczących nadania użytkownikom uprawnień dostępu do danych i wybranych funkcji, w środowisku IT:
    a) tworzenie kont użytkowników w systemach informatycznych,
    b) przypisywanie do kont startowych haseł uwierzytelniających użytkowników kont,

c) przypisywanie do założonych kont polityk odnośnie jakości haseł i częstotliwości ich zmiany,
d) resetowanie utraconych haseł,
e) usuwanie kont i uprawnień dla kont osób, które zakończyły pracę w Urzędzie,
f) przekazanie ABI informacji sprzętowo-programowych do oceny prawidłowości ich funkcjonowania,

9) zapewnienie serwerom i stacjom roboczym niezbędnych licencji programowych,
10) systematyczne aktualizowanie oprogramowania systemowego, aplikacyjnego i ochronnego,
11) aktualizowanie systemu antywirusowego,
12) koordynowanie działaniami zapewniającymi sprawne funkcjonowanie i zabezpieczenie systemów teleinformatycznych przed niepowołanym dostępem,
13) zapewnienie prawidłowego dostępu do informacji chronionych wyłącznie przez osoby mające stosowne upoważnienie,
14) kontrolowanie procesu przyznawania praw dostępu,
15) kontrolowanie jakie dane osobowe, kiedy i przez kogo zostały do zbioru danych wprowadzone oraz komu są przekazywane,
16) przeciwdziałanie próbom naruszenia bezpieczeństwa informacji,
17) prowadzenie szczegółowej dokumentacji naruszeń bezpieczeństwa danych chronionych przetwarzanych w systemie informatycznym,
18) wykonywanie kopii zabezpieczających, w terminach określonych w Polityce Bezpieczeństwa, ich przechowywanie oraz okresowe sprawdzanie pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu informatycznego,
19) prowadzenie rejestru- dziennika kopii zapasowych, wykonywanych kopii zabezpieczających oraz dziennika systemu informatycznego,
20) podejmowanie działań służących zapewnieniu niezawodności zasilania komputerów, innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych oraz zapewnienie bezpiecznej wymiany danych w sieci wewnętrznej i bezpiecznej teletransmisji,
21) przeprowadzanie inwentaryzacji sprzętu komputerowego i oprogramowania oraz utrzymanie ich w aktualności,
22) współtworzenie analizy ryzyka dla systemu informatycznego,
23) zapewnienie przeprowadzania okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji,
24) dokonywanie zmian treści informacji publicznych udostępnionych na stronie podmiotowej RBIP,
25) zapewnienie utrzymania ciągłości Internetu, sprzętu komputerowego oraz urządzeń biurowych,
26) prowadzenie instruktażu dla pracowników z zakresu pracy systemu informatycznego i programów użytkowych,
27) usuwanie podstawowych problemów związanych z działaniem komputerów, drukarek i oprogramowania,
28) zakładanie profili zaufanych i elektronicznego podpisu oraz prowadzenie ich ewidencji,
29) nadzorowanie i kontrolowanie funkcjonowania systemu wspomagającego Mdok,
30) udzielanie pomocy pracownikom Urzędu w zakresie obsługi systemu Mdok,
31) przyjmowania zgłoszeń braku ciągłości działania systemu monitorującego i zgłoszenie do wykonawcy systemu;
32) zapewnienie narzędzi i środków do bezpiecznego przechowywania nagrań z monitoringu np. w celu przygotowania materiału na żądanie policji, prokuratury i innych organów ścigania,

33) prowadzenie gospodarki zaopatrzeniowej materiałów biurowych i środków czystości,
34) wykonywanie innych zadań zleconych przez bezpośredniego przełożonego i Wójta Gminy.

ZAKRES ODPOWIEDZIALNOŚCI

1) prawidłowe funkcjonowanie i zapewnienie bezpieczeństwa działania systemu informatycznego,
2) przygotowywanie procedur dotyczących funkcjonowania systemów informatycznych,
3) zapewnienie funkcjonowania i bezpieczeństwa systemów informatycznych w Urzędzie,
4) terminowe, rzetelne i staranne wykonywania kopii zapasowych, składanie raportów o stanie bezpieczeństwa, nadawanie uprawnień i wykreślanie użytkowników w systemach, prowadzenia ewidencji stanu sprzętu IT, aktualizowanie oprogramowani,
5) zapewnienie legalności oprogramowania wykorzystywanego na stacjach roboczych,
6) przestrzeganie zasad bezpiecznego użytkowania sprzętu IT, Internetu, poczty elektronicznej oraz bankowości elektronicznej,
7) terminowe wprowadzanie danych na stronę RBIP,
8) sprzęt informatyczny i zapewnienie sprawności jego działania (komputerów, laptopów, drukarek i zainstalowanego oprogramowania, konserwację sprzętu),
9) terminowe i rzetelne wprowadzanie danych do Portalu Usług Elektronicznych – CRPO,
10) zapewnienie sprawnego funkcjonowania systemu Mdok,
11) zapewnienie ważności podpisu elektronicznego uprawnionych pracowników,
12) gospodarkę zaopatrzeniową w materiały biurowe i środki czystości w urzędzie.

UPRAWNIENIA

1) nadzorowania i realizowania zasad bezpieczeństwa przetwarzania i ochrony osobowych w systemach informatycznych Urzędu Gminy i działanie zgodne z obowiązującą Polityką Bezpieczeństwa Informacji,
2) nadzorowania i kontrolowania realizacji przedsięwzięć określonych w art. 36 ust. 1 i w art. 38 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych oraz w rozporządzeniu Rozporządzenie 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,
3) współdziałanie z Administratorem Bezpieczeństwa Informacji w zakresie opracowywania i wdrażania polityk, procedur i instrukcji,
4) monitorowanie stanu środowiska IT, stanu sprzętu IT i wykorzystywanego oprogramowania oraz aktywności sieciowej użytkowników,
5) monitorowanie legalności oprogramowania wykorzystywanego na stacjach roboczych,
6) nadzorowanie zgłaszanych incydentów i zdarzeń bezpieczeństwa dotyczących systemów teleinformatycznych,
7) niezwłocznego reagowania na zgłaszane incydenty dotyczące zabezpieczenia systemów informatycznych,
8) nadzorowanie prac nad wykonywaniem napraw, przeglądu, konserwacji oraz likwidacji urządzeń komputerowych, na których zapisane są dane osobowe,

9) przydzielanie każdemu użytkownikowi identyfikatora oraz hasła do systemu informatycznego oraz dokonywanie ewentualnych modyfikacji uprawnień, a także usuwanie lub wyłączanie kont użytkowników zgodnie z zasadami określonymi Polityce Bezpieczeństwa,
10) wyrejestrowania użytkowników,
11) podejmowania działań w zakresie ustalania i kontroli identyfikatorów dostępu do systemu informatycznego,
12) przeprowadzanie kontroli uprawnień i kont użytkowników,
13) przeprowadzanie kontroli sposobu korzystania przez użytkowników z Internetu, poczty elektronicznej i bankowości elektronicznej,
14) zmiany w poszczególnych stacjach roboczych hasła dostępu, ujawniając je wyłącznie danemu użytkownikowi oraz, w razie potrzeby Administratorowi Bezpieczeństwa Informacji lub Administratorowi Danych,
15) informowanie Administratora Bezpieczeństwa Informacji o naruszeniu zabezpieczeń systemu informatycznego i współdziałania z nim przy usuwaniu skutków naruszenia,
16) nadzorowania działań mechanizmów uwierzytelniania użytkowników oraz kontrolowania dostępu do danych,
17) opiniowania umów zawieranych z podmiotami trzecimi w zakresie powierzenia danych do przetwarzania,
18) wprowadzania danych na stronę podmiotową RBIP,
19) przeprowadzania kontroli sprzętu informatycznego i oprogramowania,
20) obsługi Portalu Usług Elektronicznych Centralnego Rejestru Pełnomocnictw Ogólnych – CRPO,
21) sprawowania nadzoru nad funkcjonowaniem systemu Mdok,
22) przyjmowanie zapotrzebowania na materiały biurowe i środki czystości,
23) sporządzanie zbiorczego zapotrzebowania na materiały biurowe i środki czystości.

1.

WYMAGANIA KWALIFIKACYJNE

WYKSZTAŁCENIE	NIEZBĘDNE	**wyższe**
	DODATKOWE	wyższe informatyczne
DOŚWIADCZENIE	NIEZBĘDNE	-
	DODATKOWE	-
UMIEJĘTNOŚCI	NIEZBĘDNE	umiejętności interpersonalne,
	DODATKOWE	administrowanie siecią informatyczną, umiejętność tworzenia baz danych
KURSY, SZKOLENIA, INNE	NIEZBĘDNE	Specjalistyczne szkolenie dla administratorów systemów i inspektorów bezpieczeństwa teleinformatycznego
	DODATKOWE	
SPECJALNE	NIEZBĘDNE	

WYMAGANIA WOBEC STANOWISKA	DODATKOWE	

WARUNKI PRACY

Zgodnie z oceną ryzyka zawodowego opracowana przez Głównego Specjalistę ds. BHP.

1. **Istota ryzyka:**
   Na stanowisku pracy mamy do czynienia z wieloma rodzajami zagrożeń:

   - **typowe urazy mechaniczne związane z możliwością przewrócenia się na tym samym poziomie, pracą na terenie firmy, kontakt z urządzeniami, itp.** Urazy mogą mieć bardzo różną formę: urazy kończyn górnych i dolnych (złamania, urazy stóp), otarcia naskórka, zranienia, urazy kręgosłupa, uderzenie, zmiażdżenie, przerwanie ciągłości skóry, urazy oczu, osłabienie wzroku.
   - **Możliwość porażenia prądem. Efektem może być:** uczucie bólu, kurcze mięśni, zatrzymanie oddechu, utrata przytomności, bardzo groźne dla człowieka, migotanie komór serca.
   - **Obciążenia psychonerwowe. Mogą się one ujawniać w następujący sposób:** symptom wypalenia się, problemy z psychiką (depresje, nerwowość i inne.), zaburzenia w przemianie metabolicznej (otyłość, cukrzyca i inne.), problemy zdrowotne (choroba wrzodowa, nadciśnienie, wrzody trawienne, choroby skóry i inne.).
   - **Pożar, którego skutkiem może być:** śmierć, poparzenia różnego stopnia.
   - **Stanowisko pracy. Skutki:** bóle szyi, barków i karku, cierpnięcie nóg, mrowienie, drętwienie, bóle nadgarstka i przedramion, bóle głowy, ogólne obciążenie układu mięśniowo – szkieletowego, przeciążenie strun głosowych.
2. **Cechy ryzyka:** akceptowalne, małe, istotne, **AKCEPTOWALNE.**
3. **Kontakt z zagrożeniem:** lekceważenie przepisów i zasad bhp, nie zachowywanie wystarczającej ostrożności, lekkomyślność, lekceważenie przepisów i zasad ppoż. Niestosowanie się do zaleceń zawartych w instrukcjach bhp.
4. **Skutki ryzyka:** wypadkowe: śmierć, kalectwo, całkowita niezdolność do pracy, konieczność zmiany zawodu lub stanowiska, stałe obniżenie sprawności, czasowe obniżenie sprawności.
5. **Prawdopodobieństwo skutków:** jak do tej pory nie odnotowano wypadków na stanowisku. Nie odnotowano także zachorowania na choroby zawodowe.
6. **Wykrywanie zagrożenia:** codzienne sprawdzanie przygotowania i wyposażenia stanowiska pracy – "lustracja miejsca pracy". Należy dokonać oględzin pod względem bezpieczeństwa i higieny pracy, jak: stan techniczny eksploatowanych urządzeń . Stwierdzone w czasie lustracji miejsca pracy nieprawidłowości, należy określić w sposób jednoznaczny z umiejscowieniem występowania tej nieprawidłowości.
7. **Sposób reagowania w sytuacji zagrożenia:** stwierdzone w czasie codziennej "lustracji miejsca pracy", nieprawidłowości zgłaszamy do bezpośredniego przełożonego,

nieprawidłowości stanowiące bezpośrednie zagrożenie, należy usunąć w trybie natychmiastowym lub dokonać zabezpieczenia miejsca, stanowiska pracy, na którym występuje zagrożenie. O podjętej decyzji i poczynionych działaniach na rzecz wyeliminowania niebezpieczeństwa, należy powiadomić niezwłocznie bezpośredniego przełożonego.

Sporządziła: ***Renata Jesionowska-Zawieja***

Sekretarz Gminy

Sadki, dnia 2 października 2017 r.

Zatwierdził:

Z up. WÓJTA

.....

Następca Wójta