GMINNE CENTRUM KULTURY W CIESZKOWIE

REGULAMIN OCHRONY DANYCH OSOBOWYCH

W GMINNYM CENTRUM KULTURY W CIESZKOWIE

Załącznik nr 1 do Zarządzenia nr 5/2018 Dyrektora Gminnego Centrum Kultury z dnia 03.09.2018 r.

WSTĘP

Realizując postanowienia ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. 2018 poz. 1000) jak i również Rozporządzenia Ogólnego PE 1 Rady UE o ochronie danych osobowych (DZ. U. UE. L. z 2016 r. 119.1) wprowadza się zestaw reguł i praktycznych doświadczeń regulujących sposób zarządzania, ochrony i dystrybucji informacji wrażliwej pozwalającej na zapewnienie ochrony danych osobowych.

Niniejszy regulamin stanowi wyciąg najistotniejszych zapisów zawartych w polityce bezpieczeństwa oraz instrukcji zarządzania systemem informatycznym. Obowiązuje pracowników etatowych oraz współpracowników (użytkowników), mających upoważnienia do przetwarzania danych osobowych.

SPIS TREŚCI

1. Zasady bezpiecznego użytkowania sprzętu stacjonarnego IT

1. Użytkownik zobowiązany jest korzystać ze sprzętu IT w sposób zgodny z jego przeznaczeniem i chronić go przed jakimkolwiek zniszczeniem lub uszkodzeniem.
2. Użytkownik zobowiązany jest do zabezpieczenia sprzętu IT przed dostępem osób nieupoważnionych, a w szczególności zawartości ekranów monitorów.
3. Użytkownik ma obowiązek natychmiast zgłosić zgubienie, utratę lub zniszczenie powierzonego mu sprzętu IT.
4. Samowolne otwieranie (demontaż) obudowy sprzętu IT, instalowanie dodatkowych urządzeń (np. twardych dysków, pamięci) lub podłączanie jakichkolwiek nie zatwierdzonych urządzeń do systemu informatycznego jest zabronione.

2. Zasady korzystania z oprogramowania

1. Użytkownik zobowiązuje się do korzystania wyłącznie z oprogramowania objętego prawami autorskimi.
2. Użytkownik nie ma prawa kopiować oprogramowania zainstalowanego na sprzęcie IT przez Pracodawcę na swoje własne potrzeby ani na potrzeby osób trzecich.
3. Instalowanie jakiegokolwiek oprogramowania na Sprzęcie IT może być dokonane wyłącznie przez osobę upoważnioną.
4. Użytkownicy nie mają prawa do instalowania ani używania oprogramowania innego, niż przekazane lub udostępnione im przez Pracodawcę / Zleceniodawcę. Zakaz dotyczy między innymi instalacji oprogramowania z zakupionych dyskietek, płyt CD, programów ściąganych ze stron internetowych, a także odpowiadania na samoczynnie pojawiające się reklamy internetowe.
5. Użytkownicy nie mają prawa do zmiany parametrów systemu, które mogą być zmienione tylko przez osobę upoważnioną.
6. W przypadku naruszenia któregokolwiek z powyższych postanowień Pracodawca / Zleceniodawca ma prawo niezwłocznie i bez uprzedzenia usunąć nielegalne lub niewłaściwie zainstalowane oprogramowanie.

3. Zasady korzystania z Internetu

1. Użytkownicy mają prawo korzystać z Internetu wyłącznie w celu wykonywania obowiązków służbowych.
2. Przy korzystaniu z Internetu, użytkownicy mają obowiązek przestrzegać prawa własności przemysłowej i praw autorskich.
3. Użytkownicy nie mogą korzystać z Internetu dla celów prywatnych.
4. Korzystanie z Internetu dla celów służbowych nie może wpływać na jakość i ilość świadczonej przez Użytkownika pracy oraz na prawidłowe i rzetelne wykonywanie przez niego obowiązków służbowych, a także na wydajność systemu informatycznego Pracodawcy.
5. Użytkownicy nie mają prawa korzystać z Internetu w celu przeglądania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec obowiązujących zasad postępowania, a także grać w gry komputerowe w Internecie lub w systemie informatycznym Pracodawcy ściągać z Internetu jakichkolwiek plików muzycznych lub wideo.

6. W zakresie dozwolonym przepisami prawa, Pracodawca zastrzega sobie prawo kontrolowania sposobu korzystania przez Użytkownika z Internetu pod kątem wyżej opisanych zasad. Ponadto, w uzasadnionym zakresie, Pracodawca zastrzega sobie prawo kontroli czasu spędzanego przez Użytkownika w Internecie. Pracodawca może również blokować dostęp do niektórych treści dostępnych przez Internet.

4. Zasady korzystania z poczty elektronicznej

1. System Poczty Elektronicznej jest przeznaczony wyłącznie do wykonywania obowiązków służbowych.
2. Przy korzystaniu z Systemu Poczty Elektronicznej, Użytkownicy mają obowiązek przestrzegać prawa własności przemysłowej i prawa autorskiego.
3. Użytkownicy nie mają prawa korzystać z Systemu Poczty Elektronicznej dla celów prywatnych.
4. Korzystanie z Systemu Poczty Elektronicznej dla celów służbowych, nie może wpływać na jakość i ilość świadczonej przez Użytkownika pracy oraz na prawidłowe i rzetelne wykonywanie przez niego obowiązków służbowych, a także na wydajność Systemu Poczty Elektronicznej.
5. Użytkownik jest świadomy, że wszelkie wiadomości o charakterze prywatnym utworzone lub odebrane za pośrednictwem Systemu Poczty Elektronicznej przetwarzane są wyłącznie na jego własną odpowiedzialność. Użytkownik wyraża zgodę na prowadzenie kontroli tych wiadomości przez Pracodawcę / Zleceniodawcę. Pracodawca nie będzie w tej sytuacji odpowiadać za przypadkowe naruszenie dóbr osobistych Użytkownika w postaci naruszenia tajemnicy korespondencji.
6. Użytkownicy nie mają prawa korzystać z Internetu w celu przeglądania lub rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec powszechnie obowiązujących zasad postępowania.
7. Użytkownik nie ma prawa wysyłać wiadomości zawierających informacje poufne dotyczące Pracodawcy i jego pracowników, pacjentów lub klientów, dostawców lub kontrahentów za pośrednictwem Internetu, w tym przy użyciu prywatnej elektronicznej skrzynki pocztowej.
8. Zakazuje się uczestnictwa w tzw. „łańcuszkach szczęścia".
9. Użytkownicy nie powinni otwierać przesyłek od nieznanych sobie osób, których tytuł nie sugeruje związku z wypełnianymi przez nich obowiązkami służbowymi.
10. Użytkownicy nie powinni uruchamiać wykonywalnych załączników dołączonych do wiadomości przesyłanych pocztą elektroniczną.
11. W przypadku przesyłania plików danych osobowych do podmiotów zewnętrznych, Użytkownik zobowiązany jest do ich spakowania i opatrzenia hasłem (8 znaków: duże i małe litery i cyfry lub znaki specjalne). Hasło należy przesłać odrębnym mailem lub sms.

5. Ochrona antywirusowa

1. Użytkownicy zobowiązani są do skanowania plików wprowadzanych z zewnętrznych nośników programem antywirusowym.
2. Zakazane jest wyłączanie oprogramowania antywirusowego podczas pracy systemu informatycznego przetwarzającego dane osobowe.
3. W przypadku stwierdzenia zainfekowania systemu, użytkownik obowiązany jest poinformować niezwłocznie o tym fakcie Pracodawcę lub osobę upoważnioną.

6. Nadawanie upoważnień i uprawnień do przetwarzania danych osobowych

1. Za nadawanie upoważnień odpowiada Administrator.
2. Każdy użytkownik systemu przed nadaniem upoważnienia musi:
   a. Zapoznać się z niniejszym regulaminem.
   b. Podpisać oświadczenie poufności.
3. Administrator nadaje pisemne upoważnienia Pracownikom.
4. Upoważnienie nadawane jest do zbiorów w wersji papierowej i elektronicznej.
5. Administrator odpowiada za aktualizację i anulowanie upoważnień.

7. Polityka haseł

1. Hasło dostępu do zbioru danych składa się z co najmniej 8 znaków (dużych i małych liter oraz z cyfr lub znaków specjalnych).
2. Zmiana hasła do systemu następuje nie rzadziej, niż co 90 dni oraz niezwłocznie w przypadku podejrzenia, że hasło mogło zostać ujawnione.
3. Zmianę hasła wymusza system lub użytkownik zobowiązany jest do manualnej zmiany hasła.
4. Użytkownik systemu w trakcie pracy w aplikacji może zmienić swoje hasło.
5. Hasła są rejestrowane w taki sposób, że nie jest możliwe ich ujawnienie.
6. Kopia bezpieczeństwa hasła Administratora może być użyta jedynie w wyjątkowych sytuacjach, gdy dostęp do danych umieszczonych na komputerze użytkownika jest niezbędny, a pracownik jest nieobecny w pracy.
7. Hasła nie mogą być powszechnie używanymi słowami. W szczególności nie należy jako hasła wykorzystywać: dat, imion, nazwisk, inicjałów, numerów rejestracyjnych samochodów, numerów telefonów.
8. Użytkownik zobowiązuje się do zachowania hasła w poufności, nawet po utracie przez nie ważności
9. Zabronione jest zapisywanie haseł w sposób jawny (na karteczkach) oraz przekazywanie ich innym osobom.

8. Procedura rozpoczęcia, zawieszenia i zakończenia pracy

1. Użytkownik rozpoczyna pracę z systemem informatycznym przetwarzającym dane osobowe z użyciem identyfikatora i hasła.
2. Użytkownik jest zobowiązany do uniemożliwienia osobom niepowołanym wglądu do danych wyświetlanych na monitorach komputerowych – tzw. Polityka czystego ekranu.

3. Przed czasowym opuszczeniem stanowiska pracy użytkownik zobowiązany jest wywołać blokowany hasłem wygaszacz ekranu lub wylogować się z systemu.
4. Po zakończeniu pracy użytkownik zobowiązany jest:
    a. Wylogować się z systemu informatycznego, a następnie wyłączyć sprzęt komputerowy.
    b. Zabezpieczyć stanowisko pracy, a w szczególności wszelką dokumentację oraz nośniki magnetyczne i optyczne, na których znajdują się dane osobowe.

9. Postępowanie z elektronicznymi nośnikami zawierającymi dane osobowe

1. Elektroniczne nośniki, to: np. wymienne twarde dyski, pen-drive, płyty CD, DVD, pamięci typu Flash.
2. Użytkownicy nie mogą wynosić na zewnątrz miejsca pracy wymiennych elektronicznych nośników informacji z zapisanymi danymi osobowymi bez zgody Administratora.
3. W razie konieczności nadane zostanie upoważnienie do przewożenia dokumentacji na nośnikach lub papierowo.
4. Dane osobowe wynoszone poza miejsce pracy muszą być zaopatrzone hasłem dostępu lub szyfrowane.
5. W przypadku uszkodzenia lub zużycia nośnika zawierającego dane osobowe należy fizycznie zniszczyć nośnik przez spalenie lub rozdrobnienie.
6. Przekazywanie nośników z danymi osobowymi powinno być przeprowadzone z uwzględnieniem zasad bezpieczeństwa. Adresat powinien zostać powiadomiony o przesyłce, zaś nadawca powinien sporządzić kopię przesyłanych danych. Adresat powinien powiadomić nadawcę o otrzymaniu przesyłki. Jeżeli nadawca nie otrzymał potwierdzenia, zaś adresat twierdzi, że nie otrzymał przesyłki, użytkownik będący nadawcą powinien poinformować o zaistniałej sytuacji Administratora Danych Osobowych.

10. Postępowanie z danymi osobowymi w wersji papierowej

1. Za bezpieczeństwo dokumentów i wydruków zawierających dane osobowe odpowiedzialne są osoby upoważnione (użytkownicy) oraz pracownicy właściwych jednostek organizacyjnych.
2. Dokumenty i wydruki zawierające dane osobowe przechowuje się w pomieszczeniach zabezpieczonych fizycznie przed dostępem osób nieupoważnionych.
3. Użytkownicy są zobowiązani do stosowania „polityki czystego biurka". Polega ona na zabezpieczaniu dokumentów np. w szafach, biurkach, pomieszczeniach przed kradzieżą lub wglądem osób nieupoważnionych.
4. Użytkownicy zobowiązani są do przewożenia dokumentów w sposób zapobiegający ich kradzieży, zagubieniu lub utracie.
5. Użytkownicy zobowiązani są do niszczenia dokumentów i tymczasowych wydruków w niszczarkach niezwłocznie po ustaniu celu ich przetwarzania.

11. Zapewnienie poufności danych osobowych

1. Użytkownik zobowiązany jest do zachowania w tajemnicy danych osobowych, do których ma lub będzie miał/a dostęp w związku z wykonywaniem zadań służbowych lub obowiązków pracowniczych lub zadań zleconych przez Pracodawcę.
2. Użytkownik zobowiązany jest do niewykorzystywania danych osobowych w celach pozasłużbowych bądź niezgodnych ze zleceniem o ile nie są one jawne.
3. Użytkownik zobowiązany jest do zachowania w tajemnicy sposobów zabezpieczania danych osobowych o ile nie są one jawne.
4. Zabrania się przekazywania bezpośrednio lub przez telefon danych osobowych osobom nieupoważnionym.

12. Skrócona instrukcja postępowania w przypadku naruszenia ochrony danych osobowych

1. Użytkownik zobowiązany jest do powiadomienia Administratora Danych Osobowych w przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych.
2. Typowe sytuacje, gdy użytkownik powinien powiadomić Administratora lub ASI:
    a. Ślady na drzwiach, oknach i szafach wskazują na próbę włamania,
    b. Dokumentacja jest niszczona z użyciem niszczarki,
    c. Fizyczna obecność w budynku lub pomieszczeniach osób zachowujących się podejrzanie,
    d. Otwarte drzwi do pomieszczeń, szaf, gdzie przechowywane są dane osobowe,
    e. Ustawienie monitorów pozwala na wgląd osób postronnych na dane osobowe,
    f. Wynoszenie danych osobowych w wersji papierowej i elektronicznej na zewnątrz firmy bez upoważnienia Administratora,
    g. Udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej i ustnej,
    h. Telefoniczne próby wyłudzenia danych osobowych,
    i. Kradzież komputerów lub nośników CD, twardych dysków, pen-drive z danymi osobowymi,
    j. Maile zachęcające do ujawnienia identyfikatora i/lub hasła,
    k. Pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów,
    l. Hasła do systemów przechowywane są w pobliżu komputera.

13. Postępowanie dyscyplinarne

1. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także, gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, można wszcząć postępowanie dyscyplinarne.
2. Kara dyscyplinarna orzeczona wobec osoby uchylającej się od powiadomienia nie wyklucza odpowiedzialności karnej tej osoby zgodnie z ustawą z dnia 10 maja 2018 roku o ochronie danych (Dz. U. 2018 poz. 1000) jak i również Rozporządzenia Ogólnego PE I Rady UE o ochronie danych osobowych (Dz. U. UE. L. z 2016 r. 119.1)

oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.

14.

Regulamin dotyczy wszystkich aktów wewnętrznych obowiązujących w Gminnym Centrum Kultury w Cieszkowie, w których są przetwarzane dane osobowe.

15.

Regulamin wchodzi w życie z dniem 03.09.2018 r.

DYREKTOR
GCK w Cieszkowie
Halina Niedbała