Załącznik nr 6
do Instrukcji zarządzania systemami informatycznymi

ZASADY UŻYTKOWANIA ZASOBÓW KOMPUTEROWYCH I SIECI KOMUNIKACYJNYCH Miejskiego Ośrodka Sportu i Rekreacji im. A. Freyera w Tarnobrzegu

Dotyczy komputerów stacjonarnych oraz komputerów przenośnych

ZATWIERDZAM

DYREKTOR
Miejskiego Ośrodka Sportu i Rekreacji
w Tarnobrzegu
Adam Struminski

.....

(data i podpis Administratora danych)

WSTĘP

W oparciu o aktualnie obowiązujące przepisy prawa z zakresu przetwarzania i ochrony danych osobowych wprowadza się zestaw reguł i praktycznych doświadczeń regulujących sposób zarządzania, ochrony i dystrybucji informacji wrażliwej pozwalający na zapewnienie ochrony danych osobowych.

Niniejsze zasady stanowią wyciąg najistotniejszych zapisów zawartych w Polityce Bezpieczeństwa Informacji oraz Instrukcji zarządzania systemami informatycznymi. Obowiązują pracowników etatowych oraz współpracowników (użytkowników), mających upoważnienia do przetwarzania danych osobowych.

Spis treści

1 Zasady bezpiecznego użytkowania sprzętu IT 3
2 Zasady korzystania z oprogramowania 3
3 Zasady korzystania z Internetu 3
4 Zasady korzystania z poczty elektronicznej 4
5 Ochrona antywirusowa 5
6 Nadawanie upoważnień i uprawnień do przetwarzania danych osobowych. 5
7 Polityka haseł 5
8 Procedura rozpoczęcia, zawieszenia i zakończenia pracy. 5
9 Postępowanie z elektronicznymi nośnikami zawierającymi dane osobowe 6
10 Postępowanie z danymi osobowymi w wersji papierowej. 6
11 Zapewnienie poufności danych osobowych 7
12 Skrócona instrukcja postępowania w przypadku naruszenia ochrony danych osobowych 7
13 Prawo Własności Intelektualnej. 7
14 Konsekwencje w przypadku naruszenia niniejszych zasad. 8

1 Zasady bezpiecznego użytkowania sprzętu 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 zagubienie, utratę lub zniszczenie powierzonego mu Sprzętu IT.
4. Samowolne otwieranie (demontaż) Sprzętu IT, instalowanie dodatkowych urządzeń (np. twardych dysków, pamięci) lub podłączanie jakichkolwiek nie zatwierdzonych urządzeń do systemu informatycznego jest zabronione.
5. Za bezpieczne użytkowanie urządzeń przenośnych typu laptop lub pendrive, szczególnie w trakcie transportu, o ile użytkownik otrzymał zgodę na ich wynoszenie poza obszar przetwarzania danych, odpowiada użytkownik.
6. Wszelkie narzędzia pracy przekazane przez pracodawcę, czyli zarówno komputer, jak i dostęp do Internetu są własnością pracodawcy i powinny być wykorzystywane zgodnie z jego wymaganiami.
7. Wykorzystywanie prywatnego sprzętu komputerowego do wykonywania zadań służbowych może mieć miejsce za zgodą pracodawcy. Warunki wykorzystywania prywatnych urządzeń oraz zasady bezpieczeństwa danych określa umowa pomiędzy pracodawcą a pracownikiem regulująca zasady korzystania ze sprzętu i aplikacji.

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. Zakaz dotyczy między innymi instalacji oprogramowania z zakupionych 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 ma prawo niezwłocznie i bez uprzedzenia usunąć nielegalne lub niewłaściwie zainstalowane oprogramowanie.

3 Zasady korzystania z Internetu

1. Użytkownicy mają prawo korzystać z Internetu w celu wykonywania obowiązków służbowych.
2. Przy korzystaniu z Internetu, użytkownicy mają obowiązek przestrzegać prawa własności przemysłowej i praw autorskich.
3. Użytkownicy mają prawo korzystać z Internetu dla celów prywatnych wyłącznie okazjonalnie i powinno być ono ograniczone do niezbędnego minimum.
4. Korzystanie z Internetu dla celów prywatnych 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 mają prawo korzystać z Systemu Poczty Elektronicznej dla celów prywatnych wyłącznie okazjonalnie i powinno być to ograniczone do niezbędnego minimum.
4. Korzystanie z Systemu Poczty Elektronicznej dla celów prywatnych 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 Pracodawcy przetwarzane są wyłącznie na jego własną odpowiedzialność. Użytkownik jest świadom możliwości prowadzenia kontroli tych wiadomości przez Pracodawcę. 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 Systemu Poczty Elektronicznej 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 w rozumieniu tajemnicy przedsiębiorstwa, jego pracowników, 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. Użycie systemów teleinformatycznych i zasobów systemowych Pracodawcy dla własnych celów komercyjnych jest zakazane.
12. Zakazane jest wygłaszanie prywatnych opinii, jako oficjalnego stanowiska Pracodawcy.
13. 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.

14. Cała korespondencja wpływająca na służbową skrzynkę jest korespondencją służbową.

5 Ochrona antywirusowa

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

6 Nadawanie upoważnień i uprawnień do przetwarzania danych osobowych

1. Konto użytkownika w systemie IT i odpowiedni poziom uprawnień zakłada Administrator systemu informatycznego (ASI) oraz pracownicy posiadający uprawnienia administratora w poszczególnych systemach.
2. Inspektor ochrony danych (dalej IOD) i ASI są niezwłocznie informowani o zatrudnieniu nowego pracownika lub współpracownika jak i o zakończeniu stosunku pracy lub umowy zlecenia.
3. Każdy użytkownik systemu przed nadaniem upoważnienia musi:
    a. zapoznać się z niniejszym regulaminem;
    b. odbyć szkolenie z zasad ochrony danych osobowych;
    c. podpisać Oświadczenie o poufności.
4. Upoważnienie nadawane jest do zbiorów w wersji papierowej i elektronicznej.
5. W przypadku, gdy upoważnienie udzielane jest do zbioru w wersji elektronicznej, nadawany jest użytkownikowi identyfikator w systemie.
6. W przypadku anulowania upoważnienia, identyfikator użytkownika jest blokowany w systemie.
7. Szczegółowa procedura nadawania i blokowania uprawnień w systemie opisana jest w załączniku do Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych.

7 Polityka haseł

1. Hasło dostępu do zbioru danych składa się co najmniej z 8 znaków (dużych i małych liter oraz z cyfr lub znaków specjalnych).
2. Zmiana hasła do systemu następuje nie rzadziej, niż co 30 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 nie mogą być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: dat, imion, nazwisk, inicjałów, numerów rejestracyjnych samochodów, numerów telefonów.
6. Użytkownik zobowiązuje się do zachowania hasła w poufności, nawet po utracie przez nie ważności.
7. Zabronione jest zapisywanie haseł w sposób jawny 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 (np. klientom, pracownikom innych działów) 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, 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 firmy wymiennych elektronicznych nośników informacji z zapisanymi danymi osobowymi bez zgody Administratora danych.
3. Dane osobowe wynoszone poza firmę muszą być zaszyfrowane.
4. W przypadku uszkodzenia lub zużycia nośnika zawierającego dane osobowe należy fizycznie zniszczyć nośnik np. przez rozdrobnienie.
5. Przekazywanie nośników z danymi osobowymi powinno być przeprowadzane 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 IOD.

10 Postępowanie z danymi osobowymi w wersji papierowej

1. Za bezpieczeństwo dokumentów i wydruków zawierających dane osobowe odpowiedzialne są osoby upoważnione (użytkownicy) oraz kierownicy właściwych jednostek organizacyjnych.
2. Dokumenty i wydruki zawierające dane osobowe przechowuje się w pomieszczeniach zabezpieczonych fizycznie przed dostępem osób nieupoważnionych.
3. Pomieszczenia w których są przetwarzane dane osobowe muszą być zamykane na klucz. Dostęp do kluczy posiadają tylko upoważnieni pracownicy.
4. Dostęp do pomieszczeń możliwy jest tylko i wyłącznie w godzinach pracy. W wypadku gdy jest wymagany poza godzinami pracy – możliwy jest tylko na podstawie zezwolenia IOD lub Administratora danych.
5. Dostęp do pomieszczeń w których są przetwarzane dane osobowe mogą mieć tylko upoważnieni pracownicy.
6. W przypadku pomieszczeń do których dostęp mają również osoby nieupoważnione, mogą przebywać w tych pomieszczeniach tylko w obecności osób upoważnionych i tylko w czasie wymaganym na wykonanie niezbędnych czynności.
7. Użytkownicy są zobowiązani do stosowania „polityki czystego biurka”. Polega ona na zabezpieczaniu dokumentów np. w szafach, biurkach, pomieszczeniach przed kradzieżą lub wglądem osób nieupoważnionych.
8. Użytkownicy zobowiązani są do przewożenia dokumentów w sposób zapobiegający ich kradzieży, zagubieniu lub utracie.

9. 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 zabezpieczenia 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 IOD w przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych.
2. Typowe sytuacje, gdy użytkownik powinien powiadomić IOD:

a. ślady na drzwiach, oknach i szafach wskazują na próbę włamania;
b. dokumentacja jest niszczona bez użycia 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 IOD;
g. udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej i ustnej;
h. telefoniczne próby wyłudzenia danych osobowych;
i. kradzież komputerów lub 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 Prawo Własności Intelektualnej

1. Całkowity udział Pracownika w jakiejkolwiek formie Prawa Własności Intelektualnej (zdefiniowanego poniżej) staje się, w stosunkach pomiędzy Pracownikiem a Pracodawcą, własnością Pracodawcy, który jest jej pełnym właścicielem, a Pracownikowi nie przysługuje jakakolwiek zapłata z tego tytułu.
2. Pracownik, na żądanie i na koszt Pracodawcy, sporządzi dokumenty oraz wykona wszelkie czynności, które mogą okazać się niezbędne w celu uzyskania przez Pracodawcę ochrony jakiegokolwiek Prawa Własności Intelektualnej, oraz wykorzystania przez Pracodawcę jakiegokolwiek Prawa Własności Intelektualnej.
3. W niniejszym regulaminie "Prawo Własności Intelektualnej" oznacza jakikolwiek wzór, proces, wynalazek, ulepszenie, model, znak handlowy, znak usługowy, firmę, prawa do projektu, patent, know-how, tajemnicę handlową, prawo autorskie oraz wszelkie inne prawa własności intelektualnej jakiejkolwiek natury (zastrzeżone czy też nie, włączając w to zastosowania oraz prawa do stosowania wszelkich elementów wymienionych powyżej) wynalezione, rozwinięte, stworzone lub nabyte przez

Pracownika w trakcie trwania stosunku pracy Pracownika, włączając w to, bez ograniczeń, wszelkie prawa do jakiegokolwiek oprogramowania, sprzętu, materiałów pisemnych lub innych elementów stworzonych, zaprojektowanych, rozwiniętych lub napisanych przez Pracownika w trakcie stosunku pracy Pracownika.

14 Konsekwencje w przypadku naruszenia niniejszych zasad

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 29 sierpnia 1997 roku o ochronie danych osobowych oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.
3. ASI (Administrator systemu informatycznego) rezerwuje sobie prawo do monitorowania systemów, sieci i zasobów komputerowych, tak by zapewnić poprawne funkcjonowanie tych systemów i śledzić ewentualne nieprawidłowości. Informacja o zakresie i celu kontroli zostanie przekazana przed rozpoczęciem działań kontrolnych.
4. ASI rezerwuje sobie prawo do ograniczenia/zabrania dostępu do systemów, sieci i zasobów komputerowych w przypadku uzasadnionych podejrzeń naruszenia warunków niniejszego regulaminu.
5. ASI i IOD są zobowiązani do raportowania każdego naruszenia niniejszego dokumentu, włączając w to warunki zawarte w dokumentach wymienionych wyżej do najbliższego przełożonego, zarządu i/lub organów ścigania, co może prowadzić do wdrożenia postępowania dyscyplinarnego i/lub prawnego i w rezultacie do zawieszenia w prawach dostępu do systemów, sieci i zasobów komputerowych, rozwiązania umowy o pracę i/lub postępowania sądowego.