2019

REGULAMIN KORZYSTANIA Z KOMPUTERÓW, TELEFONÓW KOMÓRKOWYCH I TABLETÓW SŁUŻBOWYCH

PODMIOT PPK PYRZYCE

ADRES: TADEUSZA KOŚCIUSZKI 26, 74-200 PYRZYCE

POSTANOWIENIA OGÓLNE

§ 1

Pojęcia użyte w regulaminie:

- Pracodawca – PPK Pyrzyce,
- Pracownik – osoba fizyczna pozostająca w stosunku pracy z Pracodawcą,
- ASI – Administrator systemów informatycznych (informatyk),
- służbowa poczta elektroniczna – służbowa skrzynka e-mailowa o adresie e-mail z domeną @ppkpyrzyce.pl

§ 2

1. Niniejszy regulamin ustala zasady:
   - korzystania z komputerów, telefonów komórkowych i tabletów służbowych,
   - monitorowania pracy pracowników przy wykorzystaniu komputerów, telefonów komórkowych i tabletów służbowych,
   - korzystania ze służbowej poczty elektronicznej,
   - nadzoru nad bezpieczeństwem sieci informatycznej.
2. Celem wdrożenia Regulaminu jest zachowanie równowagi pomiędzy uzasadnionym interesem pracownika do ochrony jego prywatności, a prawem do ochrony tajemnic i mienia Pracodawcy, a w szczególności:
   - poprawa jakości i zgodności z procedurami obowiązującymi u Pracodawcy - wykonywania pracy przez pracowników,
   - zabezpieczenie uzasadnionych interesów Pracodawcy,
   - ochrona tajemnicy służbowej Pracodawcy,
   - zabezpieczenie danych oraz mienia Pracodawcy.
3. Niniejszy regulamin uwzględnia prawo do prywatności Pracownika uregulowane w:
   - Konstytucji RP – prawo do prywatności art. 30, art. 31 ust. 1 i 2, ust. 47, ust 51,
   - Kodeksie Cywilnym – ochrona dobra osobistego, jakim jest prywatność w zakresie przepisów art. 23 i art. 24,
   - Kodeks Pracy – obowiązek poszanowania godności i innych dóbr osobistych pracownika wynikających z art. 111,
   - Przepisy o ochronie danych osobowych.

KORZYSTANIE Z KOMPUTERÓW SŁUŻBOWYCH

§ 3

1. Zabronione jest wykorzystywanie przez pracownika komputera, telefonu komórkowego lub tabletu służbowego do celów prywatnych. W szczególności zabronione jest instalowanie i

wykorzystywanie jakiegokolwiek oprogramowania bez wiedzy i udziału osób odpowiedzialnych za tego rodzaju czynności u Pracodawcy.

2. Dostęp do Internetu powinien odbywać się wyłącznie za pośrednictwem środków i rozwiązań dostarczonych przez PPK Pyrzyce. Zabronione jest zestawianie indywidualnych połączeń z Internetem przez poszczególnych pracowników przy wykorzystaniu modemów lub innych urządzeń dostępowych.
3. Hasła dostępu nie mogą być zapisane i pozostawione przy komputerze lub tablecie w dostępnym miejscu.
4. Zabroniony jest dostęp do stron WWW zawierających obraźliwą zawartość (np. strony pornograficzne, propagujące rasizm itp.). PPK Pyrzyce ma prawo blokować strony internetowe zawierające obraźliwą zawartość.
5. Oprogramowanie używane do przeglądania Internetu jest dostarczane wyłącznie przez PPK Pyrzyce i zatwierdzane przez Administratora. Wszystkie dostępne uaktualnienia z dziedziny bezpieczeństwa są regularnie instalowane na komputerach pracowników korzystających z Internetu. Ze względu na negatywny wpływ na bezpieczeństwo systemu poszczególne komponenty stron internetowych mogą być blokowane lub ograniczane do znanych źródeł.
6. Dostęp dla celów służbowych do płatnych usług internetowych (takich jak subskrypcje fachowych czasopism w formie elektronicznej, wyniki badań marketingowych itp.) nie może odbywać się przy użyciu prywatnych kont pracowników za pośrednictwem systemu informatycznego PPK Pyrzyce. Przed użyciem powyższych usług PPK Pyrzyce jako firma musi oficjalnie wykupić do nich dostęp.
7. Działania Pracodawcy zmierzające do poprawy jakości pracy z komputerem polegające w szczególności na eliminowaniu możliwości pobierania określonych danych z Internetu, odciążeniu sieci informatycznej poprzez ograniczenie możliwości transferu danych z lub do komputera pracownika, usuwaniu nielegalnego oprogramowania, blokowania dostępu do nielegalnej treści oraz kontroli antywirusowej nie wymagają zgody Pracownika.
8. Stanowiska komputerowe muszą był zablokowane lub wyłączone, gdy stanowisko pracy nie jest użytkowane. Przy odejściu od komputera pracownik zobowiązany jest do jego zablokowania poprzez np. użycie klawiszy (znak Windows + L).
9. Wymagane jest ustawienie wygaszacza ekranu na wszystkich urządzeniach. Urządzenia powinny się blokować po maksimum 10 minutach. Odblokowanie powinno być możliwe dopiero po podaniu hasła.

§ 4

Pracownik używający komputera przenośnego, telefonu komórkowego lub tabletu zobowiązany jest do:

- transportu komputera w sposób minimalizujący ryzyko kradzieży lub zniszczenia, a w szczególności: transportowania komputera lub tabletu w bagażu podręcznym, nie pozostawiania komputera lub tabletu w samochodzie, przechowalni bagażu, itp.,
- przenoszenia komputera w torbie przeznaczonej do przenoszenia komputerów przenośnych,

- przenoszenie tabletu w etui przeznaczonym do przenoszenia tabletów,
- przenoszenie telefonu komórkowego w etui przeznaczonym do tego celu,
- korzystania z komputera, telefonu komórkowego lub tabletu w sposób minimalizujący ryzyko podejrzenia danych przez osoby nieupoważnione, w szczególności zabrania się korzystania z komputera w miejscach publicznych i w środkach transportu publicznego,
- nie zezwalania osobom nieupoważnionym do korzystania z komputera przenośnego, telefonu komórkowego lub tabletu, na którym przetwarzane są dane osobowe,
- zabezpieczania komputera przenośnego, telefonu komórkowego lub tabletu hasłem i blokowanie dostępu przed użyciem przez osoby postronne,
- kopiowania danych osobowych przetwarzanych na komputerze przenośnym do systemu informatycznego w celu umożliwienia wykonania kopii awaryjnej tych danych,
- umożliwienia, poprzez podłączenie komputera do sieci informatycznej administratora, aktualizacji wzorców wirusów w programie antywirusowym,
- utrzymania konfiguracji oprogramowania systemowego w sposób wymuszający korzystanie z haseł,
- wykorzystywania haseł odpowiedniej jakości zgodnie z wytycznymi dotyczącymi tworzenia haseł w systemie informatycznym przetwarzającym dane osobowe,
- zmiany haseł zgodnie z wymaganiami dla systemu informatycznego przetwarzającego dane osobowe.

§ 5

Zabrania się pracownikom korzystającym z Internetu następujących praktyk:

- przeglądania oraz ściągania materiałów o treściach pornograficznych lub prawnie zakazanych,
- prowadzenia rozmów przez Internet
- prowadzenia gier sieciowych,
- uprawiania hazardu i udziału w grach losowych
- wyrażania osobistych opinii jako opinii placówki,
- wyrażania lub przesyłania nieprzyzwoitych uwag lub propozycji,
- ściągania programów komercyjnych z naruszeniem praw autorskich,
- ściągania programów lub plików elektronicznych bez odpowiedniej ochrony antywirusowej,
- umyślnego zakłócania normalnej pracy urządzeń dostępowych do Internetu,
- uczestniczenia w czynnościach, które powodują zator lub zakłócenia w pracy sieci komputerowej placówki oraz innej działalności naruszającej dobre imię placówki.

POLITYKA HASEŁ

§ 6

1. Przed przekazaniem do użytkowania systemów informatycznych konieczna jest zmiana wszystkich haseł domyślnych ustawionych przez dostawcę lub ich zablokowanie.
2. Wszystkie systemy informatyczne powinny umożliwiać ustalenie minimalnej długości hasła, okresu maksymalnej ważności hasła oraz uniemożliwiać powtórne wykorzystanie tego samego hasła.
3. Oprogramowanie systemowe nie może wyświetlać hasła jawnym tekstem na monitorze komputera.
4. Oprogramowanie nie może przechowywać ani zapisywać hasła w postaci jawnego tekstu.
5. Hasła nie mogą być zapisywane i pozostawione przy komputerze czy innym dostępnym miejscu. W szczególności zabronione jest umieszczanie haseł w treści skryptów systemowych i programów.
6. Pracownik ma obowiązek stosować hasła trudne do odgadnięcia. Standardowa długość hasła minimum 8 znaków w tym duża litera, cyfra lub znak specjalny.
7. Pracownicy nie mogą używać haseł takich samych lub podobnych do używanych przez nich poprzednio.
8. Pracownicy nie powinni używać haseł opartych na ciągu znaków ulegających zmianie w zależności od daty lub innego przewidywalnego czynnika.
9. Hasła nie powinny być wpisywane w obecności osób trzecich, jeśli mogą one zauważyć treść wpisywanego hasła.
10. Bez względu na okoliczności, hasła nie wolno ujawniać. W szczególności nie należy go ujawniać przez telefon lub pocztę elektroniczną osobom, które mogą podawać się za pracowników pomocy technicznej.
11. Hasła pozostają tajne, każdy pracownik jest zobowiązany do zachowania w tajemnicy swego hasła, także po jego zmianie.
12. Wymagana jest zmiana hasła co 30 dni. Za zmianę hasła odpowiedzialne są osoby użytkujące urządzenie.
13. Jeśli istnieje podejrzenie, że hasło zostało ujawnione, należy je natychmiast zmienić i powiadomić Inspektora Danych Osobowych.
14. Pracownik ponosi pełną i absolutną odpowiedzialność za użycie zasobów informatycznych PPK Pyrzyce przy wykorzystaniu jego hasła do momentu powiadomienia Administratora Systemów Informatycznych o ujawnieniu hasła.

OGÓLNE ZASADY MONITOROWANIA

§ 7

1. Monitorowanie pracy pracowników przy wykorzystaniu komputerów służbowych jest dopuszczalne, o ile nie jest sprzeczne z przepisami prawa, w szczególności przepisami o ochronie danych osobowych i prawem Pracowników do poszanowania ich dóbr osobistych.

2. Wszystkie działania pracowników w zakresie korzystania z Internetu mogą być monitorowane, rejestrowane oraz okresowo oceniane w celu zapewnienia prawidłowego działania i zapobiegania nieautoryzowanemu wykorzystaniu Internetu. Dodatkowo PPK Pyrzyce zastrzega sobie możliwość dostępu do profili pracowników istniejących w systemie informatycznym PPK Pyrzyce.
3. Zebrane informacje PPK Pyrzyce ma prawo udostępnić uprawnionym instytucjom państwowym w uzasadnionych przypadkach.
4. PPK Pyrzyce zastrzega sobie prawo do odfiltrowywania wybranych załączników nie związanych z działalnością operacyjną PPK Pyrzyce, na przykład plików wykonywalnych i zawartości multimedialnej.

§ 8

1. Nie jest dopuszczalne ukryte monitorowanie komputerów pracowników.
2. Kontrola jakościowa i ilościowa pracy przy komputerze może być wykonywana pod warunkiem poinformowania o tym Pracownika.
3. Pracownicy zespołów technicznych, obsługujący systemy poczty elektronicznej, nie mogą przeglądać treści przesyłanych wiadomości dla zaspokojenia swojej ciekawości lub na żądanie nieupoważnionych osób.

SŁUŻBOWA POCZTA ELEKTRONICZNA

§ 9

1. Pracownikom nie wolno nikomu udostępniać swojego profilu poczty elektronicznej. Dotyczy to zarówno osób trzecich, jak i innych pracowników PPK Pyrzyce.
2. Poczta elektroniczna jest udostępniana pracownikom wyłącznie do wypełniania obowiązków służbowych.
3. Wszystkie maile wychodzące za skrzynki służbowej powinny być opatrzone klauzulą:
   „*Ta wiadomość i jakiekolwiek pliki przesłane wraz z nią, są poufne i przeznaczone wyłącznie do użytku osób i jednostek, do których wiadomość została adresowana. Może być również objęta tajemnicą zawodową lub być chroniona innymi przepisami prawnymi. Jeśli nie jesteś wymienionym adresatem tej wiadomości, nie powinieneś jej rozpowszechniać, rozsyłać ani kopiować. Prosimy o natychmiastowe powiadomienie, za pośrednictwem poczty elektronicznej, nadawcy o pomyłkowym otrzymaniu tej wiadomości i usunięcie jej z komputera.*

   Z powodu możliwego przechwycenia, uszkodzenia, zgubienia, zniszczenia danych, opóźnień lub niepełnej transmisji oraz obecności wirusów, proces przesyłania poczty elektronicznej nie gwarantuje bezpieczeństwa i braku błędów. Dlatego nadawca nie bierze odpowiedzialności za jakiekolwiek błędy i pominięcia występujące w treści tej wiadomości, które powstały na skutek jej przesyłania. Jeżeli konieczna jest weryfikacja treści tej wiadomości, prosimy przesłać wersję drukowaną.”

4. Wiadomości elektroniczne opracowane i przechowywane przy pomocy systemu informatycznego PPK Pyrzyce stanowią własność PPK Pyrzyce i nie mogą być uważane przez pracowników za prywatne.
5. Wszyscy pracownicy posiadający dostęp do poczty elektronicznej w PPK Pyrzyce reprezentują firmę na zewnątrz. Pracownicy nie powinni wypowiadać się w imieniu lub o PPK Pyrzyce bez uprzedniej zgody Administratora.
6. Pracownicy PPK Pyrzyce używają do wysyłania i odbierania poczty elektronicznej wyłącznie oficjalnie zatwierdzonego oprogramowania.
7. Pracownicy powinni być świadomi, że poczta elektroniczna nie gwarantuje dostatecznej ochrony przesyłanych informacji. Z tego względu jeśli przesłaniu mają podlegać informacje wrażliwe, należy przed wysłaniem przesyłki zaszyfrować ją przy użyciu mechanizmów rekomendowanych przez Administratora Systemów Informatycznych.
8. Maksymalny rozmiar przesyłek pocztowych może zostać ograniczony w zależności od tego, czy odbiorca znajduje się w sieci zewnętrznej lub wewnętrznej, a przesyłki mogą być odrzucane lub przesyłane po określonej godzinie.
9. Wiadomości wychodzące z i przychodzące do PPK Pyrzyce są skanowane pod kątem obecności wirusów.
10. Załączniki do poczty elektronicznej nie powinny być otwierane, jeśli ich otrzymanie nie było wcześniej konsultowane z nadawcą.

§ 10

1. Nie jest dopuszczalne wykorzystywanie służbowej poczty elektronicznej (służbowego adresu e-mail) do celów prywatnych.
2. Wysyłanie pocztą elektroniczną wiadomości zawierających pornografię, treści dyskryminujące przedstawicieli określonej rasy, płci i religii lub dyskryminujące pod innym względem jest zakazane i może stanowić podstawę do podjęcia działań dyscyplinarnych.
3. Nielegalne powielanie lub rozprowadzanie oprogramowania chronionego prawami autorskimi (w tym oprogramowania opracowanego przez Administratora Systemów Informatycznych) za pośrednictwem poczty elektronicznej jest zakazane.
4. Pracownikom nie wolno używać do wypełniania obowiązków służbowych poczty elektronicznej innej niż zarządzana przez PPK Pyrzyce. W szczególności żadne informacje sklasyfikowane jako wrażliwe i strategiczne nie powinny być przesyłane przy użyciu poczty elektronicznej innej niż zarządzana przez PPK Pyrzyce.
5. Spis adresów poczty elektronicznej wszystkich pracowników jest informacją do użytku wewnętrznego i nie może być ujawniany jako całość na zewnątrz PPK Pyrzyce.
6. Surowo wzbronione jest rozpowszechnianie przez pracowników materiałów zawierających logo PPK Pyrzyce lub innych materiałów reklamowych razem z wiadomościami, w których zawarta jest prywatna opinia pracownika.
7. Automatyczne przeadresowywanie i przesyłanie wewnętrznej poczty elektronicznej do serwerów znajdujących się poza PPK Pyrzyce jest zakazane.

§ 11

1. Monitorowanie prywatnej poczty elektronicznej pochodzącej z prywatnego adresu e-mail pracownika jest niedopuszczalne.
2. Pracodawca ma prawo samodzielnie lub poprzez inną wyznaczona przez niego osobę skorzystać ze skrzynki e-mail Pracownika podczas jego dłuższej nieobecności w celu zachowania ciągłości pracy.
3. W celu kontroli treści służbowej korespondencji elektronicznej pracownika, Pracodawca może wprowadzić sporadyczny monitoring służbowej skrzynki poczty elektronicznej.
4. Może być dokonywana kontrola treści służbowej korespondencji elektronicznej pracownika pod warunkiem wcześniejszego jego poinformowania.

POSTANOWIENIA KOŃCOWE

§ 12

1. Jakiekolwiek wykorzystanie systemów informatycznych do działań niezgodnych z prawem lub takich, które mogą zostać uznane za obraźliwe lub łamiące inne zasady obowiązujące w PPK Pyrzyce może stanowić podstawę do podjęcia działań dyscyplinarnych.
2. Każdemu Pracownikowi umożliwia się zapoznanie z pełnym tekstem niniejszego Regulaminu.
3. Każdy Pracownik ma obowiązek przestrzegać ustalonego Regulaminu.
4. Za nieprzestrzeganie przez Pracownika ustalonego Regulaminu Pracodawcy, Pracodawca będzie stosował kary porządkowe zgodnie z Kodeksem Pracy.
5. Regulamin wchodzi w życie z dniem 30.07.2019r.

Podpis:

……
Administrator