REGULAMIN UŻYTKOWANIA SYSTEMÓW INFORMATYCZNYCH I SIECI TELEINFORMATYCZNEJ

Dokument do użytku wewnętrznego
6 marca 2023 r.

SPIS TREŚCI:

I. DEFINICJE

Do celów niniejszego Regulaminu Użytkowania systemów informatycznych i sieci teleinformatycznej, zwanego dalej „Regulaminem", przyjmuje się definicje pojęć przyjęte w Polityce ochrony danych osobowych.

II. ZASADY KORZYSTANIA Z SYSTEMÓW TELEINFORMATYCZNYCH

1. Użytkownikowi systemu informatycznego zostaje nadany dostęp po:
   1) zapoznaniu się przez niego z przepisami, w tym z niniejszym Regulaminem;
   2) podpisaniu przez niego oświadczenia o zachowaniu w tajemnicy danych osobowych, do których będzie miał dostęp podczas wykonywania obowiązków służbowych lub zobowiązań umownych, oraz środków ich zabezpieczania, w tym o powstrzymaniu się od wykorzystywania ich w celach pozasłużbowych – wzór Oświadczenia pracownika, z którego może skorzystać Administrator, zawarty jest w dokumencie: Upoważnienie do przetwarzania danych osobowych, stanowiącym część Dokumentacji ochrony danych osobowych;
   3) nadaniu mu upoważnienia do przetwarzania danych osobowych – wzór Upoważnienia do przetwarzania danych osobowych, z którego może skorzystać Administrator, stanowi część Dokumentacji ochrony danych osobowych;
   4) podpisaniu przez niego protokołu przekazania i odebrania mienia – wzór Protokołu przekazania i odebrania mienia pracownikowi, z którego może skorzystać Administrator, stanowi część Dokumentacji ochrony danych osobowych.
2. Przydzielanie uprawnień do systemu informatycznego jest realizowane na podstawie następujących zasad:
   1) minimalnych przywilejów – każdy Użytkownik posiada prawa dostępu do zasobów, ograniczone wyłącznie do tych, które są niezbędne do wykonywania powierzonych mu obowiązków;
   2) wiedzy koniecznej – Użytkownicy posiadają wiedzę o zasobach, ograniczoną wyłącznie do zagadnień, które są niezbędne do realizacji powierzonych im zadań;
   3) domniemanej odmowy – wszystkie działania, które nie są jawnie dozwolone, są zabronione.
3. W zależności od wykonywanych czynności służbowych lub umownych dostęp do systemu informatycznego mogą posiadać:
   1) pracownicy Administratora Danych Osobowych – w zakresie niezbędnym do właściwego wykonywania obowiązków służbowych;
   2) osoby, przy pomocy których Administrator Danych Osobowych wykonuje swoje czynności, w szczególności:
      a) osoby zatrudnione na podstawie umów cywilnoprawnych,
      b) pracownicy lub osoby działające w imieniu podmiotu zewnętrznego świadczącego usługi na rzecz Administratora Danych Osobowych,
      c) stażyści,
      d) praktykanci,
      e) wolontariusze, na podstawie umowy o wolontariat.
4. Każdy Użytkownik systemu informatycznego musi posiadać unikalny identyfikator i wprowadzone przez siebie hasło, autoryzujące go w systemie informatycznym (dane uwierzytelniające).
5. Identyfikator Użytkownika, nadany przez Administratora Systemu Informatycznego lub Administrator Biznesowy Systemu, składa się z ciągu znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujących osobę, która jest upoważniona do pracy w systemie.
6. Identyfikator w systemach informatycznych nadaje Administrator Systemu Informatycznego lub Administrator Biznesowy Systemu na wniosek bezpośredniego przełożonego, o czym informuje Użytkownika lub wnioskodawcę.
7. Tożsamość każdego Użytkownika musi być uwierzytelniona przed rozpoczęciem pracy w systemie.

8. Niedopuszczalne jest korzystanie z tego samego identyfikatora przez więcej niż jednego Użytkownika.
9. Uprzywilejowane konto (konto administracyjne, tj. konto umożliwiające większy zakres uprawnień, niż jest to konieczne do realizacji codziennych obowiązków pracownika) nie może służyć do realizacji rutynowych zadań przez Użytkownika, a powinno być uruchamiane doraźnie i tylko w razie zaistniałej potrzeby. W uzasadnionych przypadkach dopuszczone jest użytkowanie konta administracyjnych do czynności rutynowych.
10. Konta administracyjne są przyznawane tylko w szczególnie uzasadnionych przypadkach.
11. Zabronione jest:
    1) umożliwianie osobom nieupoważnionym dostępu do systemów informatycznych;
    2) logowanie się w systemie informatycznym na identyfikatorze innego Użytkownika;
    3) korzystanie z konta systemowego innego Użytkownika;
    4) nieuprawnione przenoszenie danych uzyskanych w związku z wykonywanymi zadaniami służbowymi na inne nośniki danych;
    5) udzielanie informacji osobom nieuprawnionym w zakresie zasad ochrony systemów informatycznych, w tym o identyfikatorach używanych w tych systemach;
    6) samowolne modyfikowanie ustawień związanych z bezpieczeństwem w systemach informatycznych;
    7) świadome niszczenie danych mających znaczenie archiwalne;
    8) świadome wprowadzanie błędnych danych do systemów informatycznych;
    9) udostępnianie danych osobom nieupoważnionym;
    10) korzystanie z prywatnych lub innych niezautoryzowanych nośników informacji;
    11) przekazywanie za pomocą urządzeń faksowych dokumentów zawierających dane osobowe szczególnej kategorii;
    12) celowe opracowywanie, generowanie, kompilowanie, kopiowanie, rozpowszechnianie, uruchamianie lub próby wprowadzania kodów komputerowych, mających zdolność samopowielania się, uszkadzania lub innego utrudniania działalności pamięci komputerowej, plików systemowych lub oprogramowania, które służą do omijania lub przełamywania zabezpieczeń i praw dostępu, wymagałyby wykorzystania większej ilości zasobów informatycznych, niż jest to niezbędne do zapewnienia prawidłowego działania systemów, czy powodowałyby zakłócenia w działaniu sieci informatycznej.
12. W przypadku naruszenia lub możliwego naruszenia ochrony danych osobowych pracownik Organizacji jest zobowiązany do niezwłocznego zgłoszenia tego faktu powołanemu przez Organizację Inspektorowi Ochrony Danych Osobowych – zgodnie z Instrukcją postępowania w przypadku naruszenia Ochrony Danych wraz z przykładami naruszeń. Inspektor Ochrony Danych Osobowych następnie jest zobowiązany do postępowania zgodnie z procedurą: Polityka zarządzania naruszeniami ochrony danych osobowych, zawartą w § 23 Polityki ochrony danych osobowych, stanowiącej część Dokumentacji ochrony danych osobowych.
13. Za bezpieczeństwo systemów teleinformatycznych odpowiedzialni są: Administrator Systemu Informatycznego wraz z Administratorem Biznesowym Systemu (administratorzy poszczególnych systemów teleinformatycznych).
14. Niezależnie od powyższego każdy pracownik Administratora jest zobowiązany do informowania upoważnionej osoby (Administratora Systemu Informatycznego, Administratora Biznesowego Systemu, Inspektora Ochrony Danych, Administratora Danych Osobowych) o zauważonych potencjalnych lukach w zakresie bezpieczeństwa.
15. W przypadku stwierdzenia możliwości pojawienia się złośliwego oprogramowania (tj. wirusa) na wykorzystywanym sprzęcie komputerowym i braku możliwości usunięcia go przez program antywirusowy, Użytkownicy obowiązani są natychmiast odłączyć urządzenie od sieci oraz niezwłocznie skontaktować się w przedmiotowej sprawie z Administratorem Systemu Informatycznego.

III. NADAWANIE UPRAWNIEŃ

1. Do złożenia wniosku o nadanie uprawnień do systemu informatycznego zobowiązany jest bezpośredni przełożony Użytkownika lub zobowiązana jest Osoba Upoważniona przez Administratora Danych Osobowych.
2. Wniosek składany jest za pośrednictwem systemu administracyjnego lub za pomocą służbowego emaila przełożonego z opisem wszystkich niezbędnych informacji
3. Bezpośredni przełożony lub Osoba Upoważniona przez Administratora Danych Osobowych, określając zakres uprawnień, o który wnioskują dla Użytkownika, są obowiązani do stosowania zasad sformułowanych w niniejszym dokumencie w rozdziale: **Zasady korzystania z systemów teleinformatycznych**, w szczególności w jego ust. 1 oraz ust. 2.
4. Po dopełnieniu powyższych wymagań wniosek o nadanie uprawnień jest przekazywany do Administratora Systemu Informatycznego lub Administratora Biznesowego Systemu.
5. W przypadku nadania uprawnień wymagających logowania Administrator Systemu Informatycznego lub Administrator Biznesowy Systemu przekazuje Użytkownikowi, w sposób zapewniający poufność danych, informację zawierającą wymienione z nazwy systemy informatyczne, do których Użytkownik otrzymał dostęp, oraz login i hasło na potrzeby pierwszego logowania.
6. Jeśli system nie realizuje funkcjonalności wymuszenia zamiany hasła tymczasowego przy pierwszym logowaniu, Użytkownik jest zobowiązany do jego manualnej zmiany przy pomocy Administratora Systemu Informatycznego lub Administratora Biznesowego Systemu.

IV. MODYFIKACJA UPRAWNIEŃ

1. Do złożenia wniosku o modyfikację uprawnień do systemu informatycznego zobowiązany jest bezpośredni przełożony Użytkownika lub zobowiązana jest Osoba Upoważniona przez Administratora Danych Osobowych.
2. Wniosek składany jest za pośrednictwem systemu administracyjnego lub za pomocą służbowego emaila przełożonego z opisem wszystkich niezbędnych informacji
3. Wniosek o modyfikację uprawnień Użytkownika powinien zostać złożony do Administratora Systemu Informatycznego lub Administratora Biznesowego Systemu w możliwie najkrótszym czasie po wystąpieniu zapotrzebowania na zmianę zakresu dostępu do danego zasobu informatycznego.
4. W przypadku zmiany stanowiska pracownika czynność, o której mowa w ust. 3, powinna zostać wykonana nie później niż ostatniego dnia pracy przed zmianą stanowiska na stanowisko wymagające innego zakresu uprawnień.
5. Dla zmian znacząco zwiększających uprawnienia wniosek o modyfikację uprawnień zawiera uzasadnienie wnoszonych zmian oraz informację o przedmiocie modyfikacji.
6. W przypadku nadania nowych uprawnień wymagających logowania Administrator Systemu Informatycznego lub ABI przekazuje Użytkownikowi, w sposób zapewniający poufność danych, informację zawierającą wymienione z nazwy systemy informatyczne, do których Użytkownik otrzymał dostęp, oraz login i hasło na potrzeby pierwszego logowania.
7. Jeśli system nie realizuje funkcjonalności wymuszenia zamiany hasła tymczasowego, przy pierwszym logowaniu Użytkownik jest zobowiązany do jego manualnej zmiany przy pomocy Administratora Systemu Informatycznego lub Administratora Biznesowego Systemu.

V. ODBIERANIE UPRAWNIEŃ

1. Do złożenia wniosku o odebranie uprawnień do systemu informatycznego zobowiązany jest bezpośredni przełożony Użytkownika lub zobowiązana jest Osoba Upoważniona przez Administratora Danych Osobowych.

8. Wniosek składany jest za pośrednictwem systemu administracyjnego lub za pomocą służbowego emaila przełożonego z opisem wszystkich niezbędnych informacji

~~3.~~2. Terminami obowiązującymi przy składaniu wniosku o odebranie uprawnień są w szczególności:
   1) w przypadku ustania stosunku pracy – wniosek odbierający wszystkie uprawnienia – natychmiast, najpóźniej ostatniego dnia pracy zatrudnionego;
   2) w przypadku rozwiązania lub wygaśnięcia umowy cywilnoprawnej – wniosek odbierający wszystkie uprawnienia – najpóźniej ostatniego dnia świadczenia usług na podstawie tej umowy;
   3) długotrwałe zwolnienie lekarskie – wniosek odbierający wszystkie uprawnienia – natychmiast po upływie 30 (trzydziestu) dni kalendarzowych od dostarczenia zwolnienia lekarskiego;
   4) zmiana stanowiska pracy – wniosek odbierający część uprawnień – natychmiast, najpóźniej ostatniego dnia pracy przed zmianą stanowiska na stanowisko wymagające ograniczenia uprawnień.

~~4.~~3. Po spełnieniu powyższych wymagań wniosek o odebranie uprawnień zostaje przekazany do Administratora Systemu Informatycznego i Administratora Biznesowego Systemu, którzy dokonują weryfikacji jego poprawności, a następnie realizują odebranie uprawnień.

VI. ZASADY STOSOWANYCH METOD I ŚRODKÓW UWIERZYTELNIANIA

1. Hasła Użytkowników lub inne dane uwierzytelniające podlegają szczególnej ochronie.
2. Użytkownik ponosi pełną odpowiedzialność za utworzenie hasła i jego przechowywanie.
3. Hasła tymczasowe, przekazywane Użytkownikowi przez Administratora Systemu Informatycznego lub Administratora Biznesowego Systemu na potrzeby pierwszego lub awaryjnego logowania, powinny być niezwłocznie zmienione przez Użytkownika.
4. Jeżeli system nie wymusza natychmiastowej zmiany hasła tymczasowego, przekazanego przez Administratora Systemu Informatycznego lub Administratora Biznesowego Systemu, Użytkownik jest zobowiązany wykonać tę czynność w sposób manualny.
5. Użytkownik ponosi pełną odpowiedzialność za czynności wykonywane w systemie informatycznym przy użyciu jego identyfikatora i hasła dostępowego.
6. Posługiwanie się identyfikatorem i hasłem innej osoby jest surowo zabronione.
7. Przekazywanie oraz udostępnianie identyfikatora i hasła innej osobie jest surowo zabronione.
8. Hasła zachowują swoją poufność również po ustaniu ich użyteczności.
9. Osoba pełniąca funkcję Administratora Systemu Informatycznego lub Administratora Biznesowego Systemu powinna posiadać dodatkowo odrębne konto, służące tylko i wyłącznie do administracji danym systemem informatycznym, o ile dany system udostępnia taką funkcjonalność (konto administracyjne).
10. Każdy Użytkownik posiadający dostęp do systemu informatycznego wykorzystywanego przez Administratora Danych Osobowych jest obowiązany do niezwłocznej zmiany haseł w razie zaistnienia podejrzenia, że zostały ujawnione, lub w przypadku rzeczywistego ich ujawnienia.
11. Każdy Użytkownik posiadający dostęp do systemu informatycznego wykorzystywanego przez Administratora Danych Osobowych jest obowiązany do stosowania haseł o minimalnej długości 12 znaków, zawierających kombinację małych i dużych liter oraz cyfr lub znaków specjalnych, jak również do ich zmiany nie rzadziej niż raz na 90 dni.
12. Zabronione jest:
    1) zapisywanie haseł w sposób jawny i umieszczanie ich w miejscach dostępnych dla innych osób;
    2) stosowanie haseł mających w swojej strukturze części loginu;
    3) stosowanie haseł będących ciągiem znaków wynikających z układu na klawiaturze (np. 1234QweR, 1QAZ2wsx, 123qweR4 itp.);
    4) stosowanie haseł zbliżonych do poprzednich (np. pa$$w0rd2013, pa$$w0rd2014 itp.);

5) stosowanie haseł opartych na ciągach znaków zmienianych w zależności od daty lub innego przewidywalnego czynnika;
6) stosowanie haseł opartych na skojarzeniach, łatwych do odgadnięcia lub wywnioskowania z informacji dotyczących danej osoby (np. imiona, nazwiska, numery telefonów, daty urodzenia itp.);
7) stosowanie tych samych haseł w różnych systemach operacyjnych i aplikacjach;
8) stosowanie tych samych haseł w celach służbowych oraz prywatnych;
9) udostępnianie haseł innym Użytkownikom;
10) wpisywanie haseł w obecności osób trzecich, jeśli mogą one zauważyć treść wpisywanego hasła;
11) przeprowadzanie prób łamania haseł;
12) wpisywanie haseł „na stałe" (np. w skryptach logowania) oraz wykorzystywanie opcji autozapamiętywania haseł (np. w przeglądarkach internetowych);
13) wprowadzanie haseł w serwisach internetowych, których pozornym zadaniem jest weryfikacja, czy dane hasło już nie wyciekło.

13. Użytkownicy powinni stosować łatwe do zapamiętania hasła, które są jednocześnie trudne do odgadnięcia, a przy ich tworzeniu – spełnić co najmniej jeden z niżej wymienionych warunków:
1) połączyć kilka słów razem;
2) zastąpić w określonym słowie kilka małych liter dużymi;
3) zastąpić poszczególne znaki w haśle wcześniejszymi lub dalszymi znakami w alfabecie lub na klawiaturze;
4) zastąpić w określonym słowie litery numerami odzwierciedlającymi ich pozycję w alfabecie;
5) celowo zastosować słowo z błędem (jednak niepopełnianym często lub nietypowym).

VII. ZASADY ROZPOCZĘCIA, ZAWIESZENIA, PROWADZENIA I ZAKOŃCZENIA PRACY W SYSTEMIE TELEINFORMATYCZNYM

1. Przed przystąpieniem do pracy w systemie informatycznym Użytkownik zobowiązany jest dokonać sprawdzenia stanu sprzętu informatycznego oraz oględzin swojego miejsca pracy, co obejmuje weryfikację podłączonych urządzeń nieznanego pochodzenia.
2. W przypadku stwierdzenia podłączenia urządzeń niewiadomego pochodzenia zabrania się uruchamiania systemu informatycznego do momentu ich usunięcia.
3. Rozpoczęcie pracy w systemie informatycznym następuje po wprowadzeniu unikalnego identyfikatora i hasła.
4. Zawieszenie pracy tj. brak wykonywania jakichkolwiek czynności przez 5–10 minut, powoduje automatycznie uruchomienie systemowego wygaszacza ekranu, blokowanego hasłem.
5. Zastosowanie mechanizmu, o którym mowa w ust. 11, nie zwalnia Użytkownika z obowiązku każdorazowego blokowania ekranu przed odejściem od stanowiska (Ctrl + Alt + Del i wybranie „zablokuj komputer" lub skrótem klawiszowym: Win + L).
6. Przed zakończeniem pracy Użytkownik ma obowiązek upewnić się, czy dane zostały zapisane, aby uniknąć ich utraty.
7. Po zakończeniu pracy Użytkownik jest obowiązany wylogować się z systemów informatycznych przetwarzających dane osobowe, zabezpieczyć nośniki informacji (elektroniczne i papierowe) oraz każdorazowo wyłączyć komputer, chyba że Użytkownik otrzymał informację od Administratora Systemu Informatycznego o planowanych pracach serwisowych.
8. W celu zabezpieczenia elektronicznych nośników danych na czas nieobecności Osoby Upoważnionej, Użytkownik jest obowiązany umieścić je w miejscu chronionym, zamknąć na klucz, a przedmiotowy klucz przechowywać w miejscu uniemożliwiającym dostęp osobom nieupoważnionym.

9. W sytuacji gdy wgląd w treści wyświetlane na monitorze może mieć osoba nieuprawniona, Użytkownik jest zobowiązany tymczasowo zmienić widok wyświetlany na monitorze lub obrócić monitor (przymknąć ekran laptopa) w sposób uniemożliwiający wgląd w wyświetlaną treść.
10. Jeżeli pomieszczenie nie pozwala na ustawienie ekranu monitora w sposób uniemożliwiający wgląd w wyświetlane treści osobom nieupoważnionym, Administrator Systemu Informatycznego powinien zapewnić filtr ograniczający kąt widzenia ekranu.
11. Użytkownik systemu informatycznego przetwarzającego dane osobowe natychmiast powiadamia Administratora Systemu Informatycznego, gdy:
    1) zweryfikowano podłączone do sprzętu komputerowego urządzenia niewiadomego pochodzenia;
    2) wygląd systemu, sposób jego działania, zakres danych lub sposób ich przedstawienia przez system informatyczny odbiegają od standardowego stanu uznawanego za typowy dla danego systemu informatycznego;
    3) niektóre opcje dostępne Użytkownikowi w normalnej sytuacji przestały być dostępne lub też opcje niedostępne Użytkownikowi w normalnej sytuacji stały się dostępne;
    4) stwierdzono bądź podejrzewa się, że miało lub mogło mieć miejsce jakiekolwiek inne naruszenie ochrony danych osobowych, tj. przypadkowe lub niezgodne z prawem zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
12. W przypadku stwierdzenia bądź podejrzenia, że w organizacji miało lub mogło mieć miejsce naruszenie ochrony danych osobowych, Użytkownik zobowiązany jest do niezwłocznego podjęcia postępowania zgodnie z procedurą: Polityka zarządzania naruszeniami ochrony danych osobowych, zawartą w § 23 Polityki ochrony danych osobowych, stanowiącej część Dokumentacji ochrony danych osobowych.

VIII. INSTRUKCJA WYMIANY I PRZECHOWYWANIA DANYCH

1. Wszelkiego rodzaju pliki zawierające dane osobowe lub inne informacje poufne nie powinny być:
    1) przechowywane na dyskach komputerów służbowych lub w pamięci innych służbowych urządzeń mobilnych, tj. tablet, telefon (na w/w urządzeniach powinna znajdować się minimalna ilość danych roboczych lub jednorazowych),
    2) przechowywane na prywatnych dyskach zewnętrznych,
    3) przesyłane:
        a) w korespondencji e-mail w sposób nieszyfrowany,
        b) za pośrednictwem jakichkolwiek komunikatorów poza środowiskiem Office (np. WhatsApp, Messenger, itp.),
        c) przy wykorzystaniu narzędzi Google.
2. W przypadku konieczności przesłania pliku z danymi osobowymi lub innymi informacjami poufnymi w korespondencji e-mail, plik taki należy zaszyfrować/spakować (np. programem 7 zip, winzipem, winrarem) i zahasłować; hasło powinno być przesłane do odbiorcy innym kanałem komunikacji, np. w wiadomości SMS.
3. Pliki bieżące i operacyjne, w tym zawierające dane osobowe lub inne informacje poufne, użytkownik powinien:
    1) przechowywać na dedykowanych zasobach sieciowych (w folderze utworzonym przez Administratora Systemów Informatycznych na wniosek użytkownika) lub umieszczać w obszarze chmurowym danego użytkownika, utworzonym w aplikacji Microsoft Office 365 – OneDrive,
    2) w uzasadnionych przypadkach kopie danych osobowych lub innych informacji poufnych mogą być przechowywane na służbowych, zaszyfrowanych dyskach zewnętrznych, przechowywanych w zamykanym, ognioodpornym sejfie, znajdującym się w biurze Administratora,

3) udostępniać wybranym użytkownikom lub innym uprawnionym osobom, w szczególności przedstawicielom klientów, dostawców Administratora, za pomocą opcji „udostępnienie elementu" lub „zarządzaj dostępem", zapewniając w ten sposób pełną kontrolę nad plikiem (blokowanie edycji, kopiowania, zakończenie udostępniania),
4) udostępniać uprawnionym członkom personelu Administratora za pomocą usługi Microsoft OneDrive, a w przypadku braku dostępu do tej usługi albo chęci prowadzenia wspólnej pracy kilku osób nad danym plikiem – korzystać z platformy Microsoft SharePoint; aby móc korzystać z w/w platformy, użytkownik zobowiązany jest zwrócić się do Administratora Systemu Informatycznego z prośbą o utworzenie dedykowanej witryny SharePoint i nadanie uprawnień wskazanym przez Administratora członkom personelu,
5) usuwać z dysku sieciowego po upływie okresu uprawniającego do legalnego przechowywania tych danych; w przypadku wątpliwości odnośnie do długości okresu legalnego przetwarzania określonych danych osobowych, użytkownik powinien skonsultować się z Inspektorem Ochrony Danych Osobowych lub Radcą Prawnym,
6) usuwać w określonym zakresie i czasie z dysku sieciowego, na każde wezwanie Administratora.

4. Pliki współdzielone, znajdujące się na dysku sieciowym (na serwerze Organizacji), podlegają przeglądowi i usuwaniu przez Administrator– - w przypadku upływu okresu legalnego przetwarzania zawartych w nich danych osobowych.

IX. UŻYTKOWANIE SPRZĘTU KOMPUTEROWEGO

1. Do sprzętu komputerowego zalicza się między innymi:
   1) komputery stacjonarne;
   2) komputery przenośne;
   3) wymienne nośniki informacji;
   4) tablety;
   5) smartfony;
   6) drukarki;
   7) modemy;
   8) monitory;
   9) routery;
   10) osprzęt dostarczony razem z wyżej wymienionym sprzętem lub zakupiony oddzielnie, a w szczególności zasilacze, klawiatury, myszki komputerowe itp.
2. Administrator Systemu Informatycznego przekazuje pracownikowi służbowy sprzęt komputerowy.
3. Przekazanie sprzętu to czynność polegająca na dostarczeniu sprzętu komputerowego wraz z odpowiednio skonfigurowanym oprogramowaniem.
4. Za poprawne działanie oraz skonfigurowanie sprzętu komputerowego odpowiada Administrator Systemu Informatycznego.
5. Użytkownicy nie mogą samodzielnie dokonywać jakichkolwiek zmian konfiguracji zasobów teleinformatycznych.
6. Wszelkie zapotrzebowanie na dodatkowe podzespoły jest zgłaszane do Administratora Systemu Informatycznego lub Osobie Upoważnionej przez Administratora Danych Osobowych.
7. Użytkownik nie może samodzielnie instalować lub usuwać oprogramowania, w tym nie może używać prywatnego oprogramowania na przekazanym sprzęcie czy podłączać własnych urządzeń.
8. Administrator Systemu Informatycznego udziela pomocy Użytkownikowi w obsłudze sprzętu i oprogramowania.
9. Użytkownik może korzystać ze stacji roboczych (komputerów PC i laptopów) wyłącznie na przydzielonym mu stanowisku. Korzystanie z innego sprzętu komputerowego jest dopuszczalne jedynie za zgodą i na polecenie bezpośredniego przełożonego lub za wiedzą i zgodą Administratora Systemu Informatycznego.

10. W przypadku korzystania ze stacji roboczej przez kilku Użytkowników bezpośredni przełożony lub Administrator Systemu Informatycznego wyznacza osobę odpowiedzialną za sprzęt, określając uprawnienia i obowiązki wszystkich współużytkowników tego sprzętu.
11. Użytkownik jest zobowiązany do dbałości o powierzony mu sprzęt komputerowy i oprogramowanie oraz do ochrony tego sprzętu przed kradzieżą lub zagubieniem, a także odpowiedzialny za zabezpieczenie go przed używaniem przez osoby nieuprawnione.
12. Użytkownik korzystający ze sprzętu komputerowego będącego własnością Administratora Danych Osobowych jest obowiązany do stosowania poniższych zasad:
    1) komputery przenośne należy przewozić jako bagaż podręczny oraz w miarę możliwości w opakowaniach niesugerujących ich zawartości;
    2) zabrania się pozostawiania bez opieki w miejscach publicznych sprzętu komputerowego przetwarzającego informacje Administratora Danych Osobowych;
    3) Użytkownik, wykonując czynności zawodowe lub umowne poza obszarem przetwarzania danych Administratora Danych Osobowych, powinien zadbać o należyte zabezpieczenie miejsca przechowywania powierzonego mu sprzętu komputerowego oraz należyte zabezpieczenie dostępu do informacji Administratora Danych Osobowych przed nieautoryzowanym dostępem osób trzecich;
    4) zabrania się spożywania posiłków i napojów podczas pracy z powierzonym sprzętem komputerowym;
    5) Użytkownik jest zobowiązany chronić powierzony mu sprzęt komputerowy przed zagrożeniami z otoczenia (np. kurz, ogień, zalanie);
    6) problemy wynikające z nieprawidłowego funkcjonowania sprzętu komputerowego należy zgłaszać Administratorowi Systemu Informatycznego;
    7) zabrania się udostępniania osobom trzecim powierzonego sprzętu komputerowego będącego własnością Administratora Danych Osobowych;
    8) w przypadku utraty sprzętu komputerowego będącego własnością Administratora Danych Osobowych należy ten fakt bezzwłocznie zgłosić do Administratora Systemu Informatycznego oraz postępować zgodnie z procedurą: Polityka zarządzania naruszeniami ochrony danych osobowych, zawartą w § 23 Polityki ochrony danych osobowych, stanowiącej część Dokumentacji ochrony danych osobowych, ponieważ utrata nośnika przetwarzającego dane może wiązać się z utratą poufności informacji chronionych przez Administratora Danych Osobowych.
13. Każdy Użytkownik sprzętu komputerowego ponosi całkowitą odpowiedzialność za sprzęt powierzony do użytkowania, a w przypadku, gdy jego utrata, uszkodzenie lub zniszczenie były wynikiem zamierzonego działania lub rażącego zaniedbania, może zostać on obciążony kosztami.
14. Uszkodzony, wycofywany z eksploatacji lub przeznaczony do ponownego użycia sprzęt komputerowy należy przekazać Administratorowi Systemu Informatycznego.
15. W przypadku ustania stosunku pracy pracownika, rozwiązania lub wygaśnięcia umowy cywilnoprawnej albo potrzeby przekazania sprzętu w użytkowanie innej osobie, Użytkownik jest zobowiązany do zwrotu używanego sprzętu komputerowego Administratorowi Systemu Informatycznego wraz z protokołem przekazania i odebrania mienia, zgodnie z ust. 1 pkt 4 rozdziału: Zasady korzystania z systemów teleinformatycznych, będącego częścią niniejszego dokumentu.
16. Jeżeli zestaw jest kompletny i nie ma uszkodzeń, Administrator Systemu Informatycznego podpisuje protokół przekazania i odebrania mienia, o którym mowa powyżej.
17. Drukarki nie mogą być pozostawione bez kontroli, jeśli są wykorzystywane do drukowania dokumentów zawierających dane osobowe.
18. Zabronione jest pozostawianie wydrukowanych dokumentów zawierających dane osobowe lub inne poufne informacje na urządzeniach drukujących.

X. WYMAGANIA DOTYCZĄCE URZĄDZEŃ MOBILNYCH

1. Skonfigurowanie smartfona lub tabletu odbywa się przed przekazaniem Użytkownikowi sprzętu.
2. Za odpowiednie skonfigurowanie urządzenia mobilnego odpowiedzialny jest Administrator Systemu Informatycznego lub Administrator Biznesowy Systemu lub Dział Administracji.
3. Wobec urządzeń mobilnych należy stosować m.in.:
   1) blokadę urządzenia (PIN/hasło/symbol graficzny);
   2) szyfrowanie nośników pamięci, w tym kart pamięci;
   3) zaporę ogniową w postaci firewall;
   4) oprogramowanie antywirusowe.
4. Zabronione jest pobieranie aplikacji na smartfony i tablety z nieoficjalnych źródeł.
5. Wszystkie aplikacje wykorzystywane do zastosowań biznesowych muszą być zatwierdzone przez Administratora Systemu Informatycznego.
6. W zastosowaniach biznesowych nie mogą być stosowane aplikacje, których warunki licencji tego zabraniają.
7. Aplikacje do zastosowań biznesowych powinny być instalowane pod nadzorem Administratora Systemu Informatycznego lub Administratora Biznesowego Systemu.
8. Zalecane jest pobieranie aplikacji jedynie ze znanych i wiarygodnych źródeł (np. Apple App Store, Google Play Store) oraz oficjalnych stron dostawców aplikacji biznesowych.
9. Przed zainstalowaniem aplikacji na smartfonie lub tablecie należy zawsze uważnie przeglądać uprawnienia, o które prosi aplikacja.
10. W razie wątpliwości w zakresie wymaganych uprawnień, o których mowa w ust. 9, należy natychmiast przerwać instalację.
11. Użytkownik urządzenia mobilnego jest zobowiązany do wyłączania nieużywanych usług (Wi-Fi, GPRS, Bluetooth, NFC).
12. Jeżeli Użytkownik utraci urządzenie mobilne, w szczególności na skutek kradzieży lub zgubienia urządzenia, jest obowiązany bezzwłocznie powiadomić Administratora Systemu Informatycznego o tym fakcie oraz postępować zgodnie z procedurą: Polityka zarządzania naruszeniami ochrony danych osobowych, zawartą w § 23 Polityki ochrony danych osobowych, stanowiącej część Dokumentacji ochrony danych osobowych.

XI. ZASADY KORZYSTANIA Z INTERNETU

1. Dostęp Użytkowników do Internetu powinien odbywać się wyłącznie za pośrednictwem środków i rozwiązań dostarczonych przez Organizację.
2. Zabronione jest zestawianie indywidualnych połączeń z Internetem przez poszczególnych Użytkowników przy otwartych sieci WiFi
3. Użytkownikom zakazuje się podłączania do sieci komputerowej własnych urządzeń bez uprzedniej zgody Administratora Systemu Informatycznego.
4. W godzinach pracy Użytkownicy mogą korzystać z Internetu wyłącznie do celów służbowych.
5. Zabrania się przetwarzania za pomocą służbowego sprzętu komputerowego treści niezgodnych z polskim prawem, w szczególności uznanych za pornograficzne, rasistowskie, traktujących o przemocy czy przestępstwach, jak również korzystania z protokołów umożliwiających wymianę plików w sieciach z naruszeniem przepisów prawa.
6. Użytkownikom nie wolno pobierać, udostępniać, a tym bardziej instalować oprogramowania pochodzącego z sieci publicznej bez każdorazowej zgody Administratora Systemu Informatycznego.
7. Zabrania się wykorzystywania niezautoryzowanych usług internetowych umożliwiających przetwarzanie informacji.
8. Do usług, o których mowa w ust. 7, zalicza się w szczególności usługi służące do przechowywania, udostępniania dokumentów lub prowadzenia rozmów przez Internet.

9. Zabrania się uruchamiania aplikacji deszyfrujących hasła oraz prowadzenia działań mających na celu podsłuchiwanie lub przechwytywanie informacji przepływającej w sieci bez uprzedniej zgody Administratora Danych Osobowych.
10. Zabrania się uruchamiania aplikacji, które mogą zakłócić i destabilizować pracę systemu informatycznego lub sieci komputerowej bądź naruszyć prywatność zasobów systemowych, bez uprzedniej zgody Administratora Danych Osobowych.

XII. ZASADY KORZYSTANIA Z POCZTY ELEKTRONICZNEJ

1. Użytkownikowi zostaje nadany dedykowany adres skrzynki poczty elektronicznej, działający w domenie Administratora Danych Osobowych.
2. Niezależnie od sytuacji indywidualne hasło Użytkownika do poczty elektronicznej powinno być znane wyłącznie jemu. W związku z tym Użytkownik jest odpowiedzialny za wszelkie działania podjęte przy wykorzystaniu jego hasła.
3. Użytkownikowi nie wolno nikomu udostępniać swojego profilu poczty elektronicznej. Dotyczy to zarówno osób trzecich, jak i innych pracowników.
4. Nadany Użytkownikowi adres skrzynki poczty elektronicznej służy wyłącznie do realizacji celów służbowych lub umownych.
5. Informacja o służbowym adresie skrzynki pocztowej jest jawna i dostępna powszechnie, w tym może być dostępna na łamach witryny internetowej Administratora Danych Osobowych w postaci książki adresowej.
6. Korespondencja realizowana drogą elektroniczną z wykorzystaniem systemów informatycznych Administratora Danych Osobowych podlega rejestrowaniu i może być monitorowana, jeżeli jest to niezbędne do zapewnienia Organizacji pełnego wykorzystania czasu pracy oraz właściwego użytkowania narzędzi pracy udostępnionych Użytkownikowi.
7. Informacje przesyłane za pośrednictwem sieci Administratora Danych Osobowych (w tym do i z Internetu) nie stanowią własności prywatnej Użytkownika.
8. Użytkownikowi nie wolno używać do wypełniania obowiązków służbowych poczty elektronicznej innej niż należąca do Organizacji.
9. Użytkownik dokonujący wysyłki korespondencji z załącznikiem zawierającym w swojej treści dane osobowe, poufne informacje lub informacje mogące stanowić tajemnicę przedsiębiorstwa jest obowiązany do opatrzenia takiego dokumentu hasłem autoryzacyjnym.
10. Hasło do pliku, o którym mowa w ust. 9, powinno zostać przesłane za pomocą innej formy komunikacji, np. wiadomości SMS.
11. Wiadomości wychodzące i przychodzące są skanowane pod kątem obecności wirusów.
12. Użytkownicy muszą odbierać pocztę elektroniczną co najmniej raz dziennie. W przypadku nieobecności w pracy Użytkownicy są zobowiązani włączyć w systemie pocztowym automatyczne zawiadomienie o ich nieobecności.
13. Użytkownicy są obowiązani do okresowego porządkowania i usuwania zbędnych wiadomości z folderów osobistych programu pocztowego, aby nie dopuścić do jego zablokowania z powodu przekroczenia dopuszczalnej pojemności skrzynki pocztowej. Przeglądy nie mogą być wykonywane rzadziej niż raz na pół roku.
14. Wszelka korespondencja elektroniczna niezwiązana z działalnością Administratora Danych Osobowych powinna być prowadzona przez prywatną skrzynkę poczty elektronicznej Użytkownika.
15. Wykorzystywanie systemów informatycznych, w tym służbowej poczty elektronicznej, do działań niezgodnych z prawem lub takich, które mogą zostać uznane za skutkujące szkodą dla Administratora Danych Osobowych, może stanowić podstawę do podjęcia działań dyscyplinarnych.
16. Użytkownicy dokonujący wysyłki korespondencji masowej poza Organizację są obowiązani do ukrywania odbiorów w kopii (pole BCC lub UDW).

17. Zabronione jest:
    1) wysyłanie materiałów służbowych na konta prywatne (np. celem pracy nad dokumentami w domu);
    2) wykorzystywanie systemu poczty elektronicznej do działań mogących zaszkodzić wizerunkowi Administratora Danych Osobowych;
    3) otwieranie załączników od nieznanych nadawców, w szczególności z plikami samorozpakowującymi się bądź wykonalnymi, typu .exe, .com itp.;
    4) przesyłanie pocztą elektroniczną plików wykonywalnych, typu .bat, .com, .exe, plików multimedialnych oraz plików graficznych (do wymiany tego typu dokumentów służą zasoby sieciowe udostępnione przez dział IT);
    5) ukrywanie lub dokonywanie zmian tożsamości nadawcy;
    6) czytanie, usuwanie, kopiowanie lub zmienianie zawartości skrzynek pocztowych innego Użytkownika;
    7) posługiwanie się adresem służbowym e-mail w celu rejestrowania się na stronach handlowych, informacyjnych, chatach lub forach dyskusyjnych, które nie dotyczą zakresu wykonywanej pracy lub obowiązków umownych;
    8) wykorzystywanie poczty elektronicznej do reklamy prywatnych towarów lub usług oraz działalności handlowo-usługowej innej niż wynikająca z potrzeb Administratora Danych Osobowych.

XIII. ZASADY BEZPIECZEŃSTWA FIZYCZNEGO

1. Dostęp do pomieszczeń archiwów dokumentów oraz tych, w których znajdują się systemy informatyczne wysokiej istotności, jak również systemy wspomagające, takie jak UPS-y, generatory prądu i inne, mogą posiadać wyłącznie Osoby Upoważnione.
2. W pomieszczeniach, w których są ulokowane systemy informatyczne wysokiej istotności i systemy wspomagające, nie wolno wykonywać zdjęć oraz rejestrować dźwięku i obrazu w postaci nagrań wideo bez odpowiedniego zezwolenia.
3. Zezwolenie, o którym mowa w ust. 2, może być udzielane przez Administratora Danych Osobowych lub Osobę Upoważnioną.
4. Palenie, jedzenie oraz picie w pomieszczeniach, w których znajdują się środki przetwarzania danych osobowych (np. pomieszczenia serwerowni i węzłów teletechnicznych), jest zabronione.
5. Dostęp do pomieszczeń, w których przetwarza się dane osobowe, należy ograniczyć do:
    1) Osób Upoważnionych do przetwarzania danych osobowych, którym przydzielono odpowiedni dostęp;
    2) personelu technicznego i sprzątającego – o ile jego dostęp następuje tylko i wyłącznie pod nadzorem Osób Upoważnionych, zgodnie z pkt 1 powyżej, lub jest w inny sposób monitorowany, a przetwarzane w pomieszczeniach dane osobowe są odpowiednio zabezpieczone;
    3) gości Organizacji – o ile ich tożsamość jest weryfikowana, daty i godziny wejść i wyjść są rejestrowane, a dostęp do obszaru przetwarzania danych osobowych i przebywanie w nim następuje tylko pod nadzorem Osób Upoważnionych do przetwarzania danych osobowych.
6. W Organizacji obowiązuje zakaz pozostawiania niezabezpieczonych pomieszczeń, w których zachodzi proces przetwarzania danych osobowych, bez nadzoru Osoby Upoważnionej.
7. Pomieszczenia, w których zachodzi proces przetwarzania danych osobowych, należy zabezpieczać przed nieuprawnionym dostępem, np. za pomocą klucza mechanicznego lub z wykorzystaniem systemu kontroli dostępu.
8. W pomieszczeniach, w których zachodzi proces przetwarzania danych osobowych, obowiązuje zakaz pozostawiania niezabezpieczonych okien.

9. Każdy pracownik jest zobowiązany do przestrzegania zakazu prowadzenia rozmów, podczas których może dochodzić do wymiany informacji, w tym danych osobowych lub innych informacji poufnych będących własnością Administratora Danych Osobowych, jeśli rozmowy te odbywają się w miejscach publicznych, otwartych pomieszczeniach biurowych lub takich, które nie gwarantują zachowania poufności rozmów.

XIV. KLASYFIKACJA INCYDENTÓW I NARUSZEŃ BEZPIECZEŃSTWA DANYCH OSOBOWYCH ORAZ PROCEDURA ICH ZGŁASZANIA

1. Za naruszenie ochrony danych osobowych uważa się w szczególności:
   1) przypadkowe lub niezgodne z prawem zniszczenie, w tym usunięcie lub utratę danych osobowych;
   2) nieuprawnioną modyfikację danych osobowych;
   3) nieuprawnione ujawnienie danych osobowych;
   4) nieuprawnione kopiowanie danych osobowych;
   5) nieuprawniony dostęp do danych osobowych.
2. Do naruszenia ochrony danych osobowych mogą doprowadzić naruszenia bezpieczeństwa, w szczególności:
   1) niezablokowanie dostępu do systemu przed odejściem od stanowiska pracy;
   2) ujawnienie indywidualnych haseł dostępu do wykorzystywanych systemów informatycznych;
   3) wykonywanie nieuprawnionych kopii danych osobowych;
   4) kradzież nośników papierowych lub sprzętu komputerowe służącego do przetwarzania danych osobowych;
   5) wszelkie działania Użytkownika związane z samodzielnym naprawianiem, potwierdzaniem lub testowaniem potencjalnych słabości systemu;
   6) niewłaściwe niszczenie nośników z danymi osobowymi, pozwalające na ich nieuprawniony odczyt;
   7) niepodjęcie działań zmierzających do eliminacji wirusów komputerowych lub innych programów zagrażających integralności systemu teleinformatycznego;
   8) brak nadzoru nad serwisantami i innymi osobami nieuprawnionymi, przebywającymi w pomieszczeniach, gdzie przetwarza się dane osobowe;
   9) dopuszczenie do przetwarzania danych osobowych pracowników bez odpowiednich upoważnień;
   10) naruszenie zasad zawartych w niniejszym Regulaminie oraz inne sytuacje wskazujące na naruszenie bezpieczeństwa danych osobowych lub je potwierdzające.
3. W przypadku zauważenia zdarzenia mogącego świadczyć lub świadczącego o naruszeniu bezpieczeństwa, którego skutkiem może być lub jest naruszenie zasad ochrony danych osobowych, pracownik jest zobowiązany do zgłoszenia tego faktu Inspektorowi Ochrony Danych (w sposób zgodny z **Instrukcją postępowania w przypadku naruszenia ochrony danych osobowych wraz z przykładami naruszeń**), który następnie jest zobowiązany do postępowania zgodnie z procedurą: **Polityka zarządzania naruszeniami ochrony danych osobowych**, zawartą w § 23 Polityki ochrony danych osobowych, stanowiącej część Dokumentacji ochrony danych osobowych.

XV. SZKOLENIA DLA UŻYTKOWNIKÓW

1. Szkolenia Użytkowników mają na celu uzyskanie przez nich optymalnego poziomu wiedzy i umiejętności, które pozwolą właściwie użytkować i chronić zasoby teleinformatyczne.
2. Okresowo szkolenia są powtarzane, ze szczególnym uwzględnieniem:

1) zmian dokonywanych w zasobach teleinformatycznych, mających wpływ na sposób korzystania z nich przez Użytkowników;
2) zmian przepisów prawa;
3) zmian wewnętrznych uregulowań;
4) wystąpienia przypadków naruszenia bezpieczeństwa.

3. Zakres szkoleń obejmuje zagadnienia ujęte w niniejszym Regulaminie, w szczególności:
   1) zapoznanie z obowiązującymi regulacjami prawnymi dotyczącymi ochrony danych osobowych;
   2) zapoznanie z obowiązującą Dokumentacją ochrony danych osobowych;
   3) przygotowanie Użytkowników do właściwego korzystania z powierzonych zasobów;
   4) sposób postępowania w przypadku zdarzenia związanego z naruszeniem bezpieczeństwa danych osobowych;
   5) sposób postępowania w sytuacjach awaryjnych i kryzysowych.
4. Po zakończeniu szkolenia każdy Użytkownik podpisuje oświadczenie potwierdzające uczestnictwo w szkoleniu, znajomość, zrozumienie oraz przyjęcie do stosowania zasad zawartych w dokumentach będących przedmiotem szkolenia.

XVI. POSTĘPOWANIE DYSCYPLINARNE W PRZYPADKU NARUSZENIA BEZPIECZEŃSTWA

1. Nieprzestrzeganie zasad ujętych w niniejszym Regulaminie stanowi ciężkie naruszenie obowiązków pracowniczych i może być przyczyną odpowiedzialności dyscyplinarnej, określonej w art. 108 i art. 52 Kodeksu pracy, lub stanowi rażące naruszenie staranności w wykonaniu zobowiązania w przypadku stosunku prawnego innego niż stosunek pracy.
2. Każdy przypadek wskazany w ust. 1 jest analizowany przez Administratora Danych Osobowych, który w porozumieniu z Administratorem Systemu Informatycznego, Inspektorem Ochrony Danych oraz bezpośrednim przełożonym pracownika dokonuje kwalifikacji naruszenia. W szczególności umyślne działanie może zostać zakwalifikowane jako ciężkie naruszenie zasad przyjętych w Organizacji.