Załącznik nr 1

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w „LekSeek Polska Spółka z ograniczoną odpowiedzialnością" Spółce komandytowej

Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w „LekSeek Polska Spółka z ograniczoną odpowiedzialnością" Spółce komandytowej (LekSeek), zwaną dalej „Instrukcją Zarządzania" wprowadza się w oparciu o wymogi bezpieczeństwa informacji określone w Rozporządzeniu 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 (Dz. U. Nr 100, poz. 1024), jak również w każdym innym akcie prawa powszechnie obowiązującego, który wyżej powołane Rozporządzenie zastąpi lub zmieni.

System, na którym pracują użytkownicy, jest zbiorem samodzielnych lub połączonych zależnościami podsystemów informatycznych w których ma miejsce przetwarzanie danych osobowych.

Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności

§ 1

1. Użytkownikowi zostaje przyznany unikalny w konkretnym podsystemie identyfikator wraz z poufnym hasłem, który proponuje Inspektor Ochrony Danych (Dalej: IOD) występując z wnioskiem o przyznanie użytkownikowi uprawnień do przetwarzania danych w podsystemie.
2. O przyznaniu identyfikatora decyduje Administrator Danych Osobowych (ADO/LekSeek), co jest tożsame z przyznaniem użytkownikowi prawa do przetwarzania danych osobowych w systemie informatycznym .
3. Identyfikator wraz z prawidłowym hasłem umożliwia użytkownikowi dostęp do podsystemu przetwarzania danych osobowych.
4. Każdy z użytkowników przed dopuszczeniem do podsystemu składa oświadczenie o zachowaniu poufności,i zapoznaje się z Instrukcją Zarządzania oraz Polityką Bezpieczeństwa oraz zostaje pouczony o wdrożonych procedurach bezpieczeństwa.
5. IOD przysługuje prawo do zablokowania konta użytkownika w każdym czasie.
6. Po zakończeniu operacji w systemie informatycznym, użytkownik zobowiązany jest wylogować się z podsystemu.
7. W przypadku awarii, zagubienia hasła lub innych nieprzewidzianych sytuacji zagrażających bezpieczeństwu danych – każdy użytkownik zobowiązany jest do niezwłocznego powiadomienia ADO lub IOD.
8. Użytkownikom przyznaje się równe uprawnienia w dostępie do podsystemu (poziom podstawowy) chyba, że specyfika systemu wymaga innego podejścia.
9. IOD przysługuje prawo dostępu do podsystemu na poziomie wyższym (ADO).

Stosowane metody i środki uwierzytelnienia
oraz procedury związane z ich zarządzaniem i użytkowaniem

§ 2

1. Użytkownicy którym przyznano dostęp do podsystemu przetwarzania danych osobowych (w tym identyfikator dostępu do systemu) ustalają hasło dostępu z IOD.
2. Hasło jest informacją o poufnym charakterze i należy zachować je w tajemnicy.
3. Obowiązuje ścisły zakaz ujawniania hasła osobom trzecim, w tym innym użytkownikom.
4. Hasła do wszystkich podsystemów użytkowanych w Zakładzie/Dziale należy przechowywać w zamykanym pomieszczeniu, w miejscu niedostępnym dla osób trzecich, w szafce zamykanej na klucz lub zabezpieczonej szyfrem.
5. Osobą odpowiedzialną za bezpieczne przechowywanie listy identyfikatorów wraz z hasłami wymienionymi w pkt. 4 jest IOD.
6. Dostęp do listy identyfikatorów i haseł użytkowników wszystkich podsystemów użytkowanych w Zakładzie/Dziale posiadają ADO oraz IOD. Użytkownik, który utracił hasło, zobowiązany jest zgłosić ten fakt bezzwłocznie IOD, który ustali nowe hasło.

§ 3

1. Hasło składa się z ciągu co najmniej 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne.
2. Hasła są różne dla każdego z użytkowników.
3. Hasła są przechowywane w podsystemie w postaci zaszyfrowanej.
4. Para „identyfikator i hasło” przyznane jednemu użytkownikowi nie może zostać powtórnie wykorzystane.
5. Hasła są zmieniane nie rzadziej niż co 30 dni.
6. System wymusza zmianę hasła.
7. Użytkownik zobowiązany jest zapamiętać hasło, o którym mowa wyżej.
8. Jeżeli system informatyczny środkami technicznymi nie wymusza podjęcia czynności określonych w pkt 1-6, użytkownik zobowiązany jest do przestrzegania powyższych zasad, a tym samym do okresowej zmiany hasła i ustanowieniu nowego, spełniającego wymogi określone w niniejszym paragrafie.

§ 4

Osobą odpowiedzialną za ustalanie poprawności haseł jest IOD. Jeśli użytkownik podsystemu odpowiedzialny za zmianę hasła nie jest pewien jego poprawności, zobowiązany jest do konsultacji z osobą odpowiedzialną za ustalanie poprawności bezpiecznych haseł.

Procedury rozpoczęcia, zawieszenia i zakończenia pracy
przeznaczone dla użytkowników systemu

§ 5

1. W celu uruchomienia podsystemu informatycznego użytkownik powinien:
    1) uruchomić komputer,
    2) wybrać odpowiednią opcję umożliwiającą logowanie do podsystemu,
    3) zalogować się do podsystemu poprzez wskazanie loginu oraz poufnego i aktualnego hasła.
2. Użytkownik podczas logowania do podsystemu nie może ujawniać hasła osobom trzecim oraz pozostawiać zapisanego hasła w pobliżu stanowiska pracy i innych pracowników.
3. Użytkownik zobligowany jest do skutecznego wylogowania się z podsystemu za każdym razem, gdy zamierza opuścić stanowisko pracy, niezależnie od tego na jak długo ma zamiar odejść od komputera.
4. Wylogowanie następuje poprzez wybranie w systemie opcji „wyloguj" lub zablokowanie ekranu w sposób, który uniemożliwia odblokowanie bez znajomości hasła, dzięki zastosowaniu funkcji wygaszacza ekranu.
5. Ekrany komputerów, na których przetwarzane są dane osobowe, należy chronić wygaszaczami zabezpieczonymi hasłem. Monitory należy ustawić tak, aby ograniczyć dostęp do danych osobom nieupoważnionym do przetwarzania danych.
6. W przypadku stwierdzenia fizycznej ingerencji w systemie lub innych podejrzeń dotyczących możliwości naruszenia bezpieczeństwa systemu, użytkownik niezwłocznie zawiadamia o zaistniałym fakcie ADO lub IOD.

Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania

§ 6

1. Kopie zapasowe zbiorów danych osobowych tworzone są codziennie po zakończonym dniu pracy ze zbiorem, chyba że danego dnia nie dokonano żadnych zmian w zbiorze.
2. Za tworzenie kopii zapasowych odpowiedzialny jest Opiekun Zbioru. Opiekuna Zbioru wyznacza IOD.
3. Opiekun Zbioru dokonuje zapisu kopii zbiorów danych osobowych na nośnikach CD, DVD, Pendrive lub innych nośnikach informacji przynajmniej co 14 dni lub częściej jeśli zmian na zbiorze jest dostatecznie wiele lub gdy uważa to za stosowne.
4. Opiekun Zbioru oznacza i przechowuje kopie zbiorów danych w zamykanym pomieszczeniu, w miejscu niedostępnym dla osób trzecich, w szafce zamykanej na klucz lub zabezpieczonej szyfrem.
5. Poprawność procesu tworzenia i przechowywania kopii zapasowych – nadzoruje IOD.

Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych

§ 7

1. Elektroniczne nośniki informacji zawierające dane osobowe są przechowywane w zamkniętych szafkach z zabezpieczeniem dostępu osób trzecich.
2. Kopie bezpieczeństwa są niezwłocznie niszczone lub zawarte w nich dane usuwane po ustaniu użyteczności danych osobowych tam zawartych.
3. Zniszczenia kopii/ usunięcia danych dokonuje się w sposób uniemożliwiający późniejsze odtworzenie danych, poprzez fizyczne zniszczenie nośników danych lub jeśli to niemożliwe, poprzez trwałe usunięcie danych przy pomocy specjalistycznego oprogramowania służącego do tego celu. W przypadku wątpliwości, należy zwrócić się do IOD.
4. Fakt zniszczenia kopii zapasowych/ usunięcia danych wymaga sporządzenia na tę okoliczność protokółu opatrzonego podpisem IOD i osoby sporządzającej ten dokument. Wzór protokołu stanowi **Załącznik 1** do Instrukcji Zarządzania.
5. Kopie zapasowe przechowuje się przez okres 2 lat o ile przepisy lub zawarte umowy nie stanowią inaczej, lub gdy użyteczność danych osobowych ustała przed upływem 2 lat licząc od dnia utworzenia kopii zapasowej, na której te dane są utrwalone.

Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, o którym mowa w pkt III ppkt 1 załącznika do rozporządzenia 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 (Dz. U. Nr 100, poz. 1024)

§ 8

1. System informatyczny LekSeek jest zabezpieczony przed atakami z zewnątrz sieci za pomocą oprogramowania typu firewall. Dodatkowo na serwerze pocztowym program antywirusowy chroni system przed przedostaniem się do wewnątrz sieci złośliwego oprogramowania.
2. Komponenty serwerowe chronione są przed zakłóceniami w sieci zasilającej przy pomocy urządzeń typu UPS, podtrzymujących zasilanie.
3. Każdy podsystem w którym ma miejsce przetwarzanie danych osobowych, podlega ochronie przed działaniem wirusów komputerowych aktualnym oprogramowaniem antywirusowym aktualizowanym na bieżąco.
4. W celu przeciwdziałania atakom zainfekowanych plików, podsystem musi być skanowany przynajmniej raz dziennie pod kątem obecności w systemie wirusów i innych zagrożeń. Za proces ten odpowiedzialny jest Opiekun Zbioru.
5. W przypadku wykrycia jakiegokolwiek zagrożenia użytkownik niezwłocznie zawiadamia IOD.
6. Wszystkie komputery, na których uruchomione są podsystemy przetwarzające dane osobowe muszą być zaopatrzone w urządzenia typu UPS, podtrzymujące zasilanie, a tym samym zabezpieczające podsystem przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.
7. W przypadku stwierdzenia braku zasilania należy dokonać natychmiastowego zapisu danych osobowych oraz przeprowadzić procedurę opuszczenia podsystemu.

Sposób realizacji wymogów, o których mowa w § 7 ust. 1 pkt 4 rozporządzenia 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 (Dz. U. Nr 100, poz. 1024)

§ 9

1. Podsystemy informatyczne nie służące do przetwarzania danych osobowych, a ograniczone wyłącznie do edycji tekstu w celu udostępnienia go na piśmie, zapewniają odnotowanie:
    1) informacji o odbiorcach, którym dane osobowe zostały udostępnione,
    2) dacie i zakresie tego udostępnienia.
2. Odnotowanie następuje przez automatyczny zapisek okoliczności w podsystemie.

Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych

§ 10

1. Przeglądów oraz konserwacji systemu dokonuje osoba wskazana przez IOD.
2. W przypadku przekazania innym podmiotom elementów systemu w celu naprawy, wszelkie dane osobowe muszą zostać z nich usunięte. Proces ten nadzoruje IOD.
3. Dane osobowe muszą być zabezpieczone przed dostępem osób trzecich zanim nośnik lub element systemu zostanie przekazany podmiotowi innemu niż IOD lub osoba przez niego wskazana.

Uwagi końcowe

§ 11

1. Dopuszcza się możliwość wprowadzania w Instrukcji Zarządzania procedur uzupełniających, jeśli wymagać będzie tego specyfika komórki organizacyjnej.
2. Stworzone procedury w szczególności powinny uściślać postanowienia określone w § 2, § 3, § 5, § 6, § 9 niniejszej Instrukcji Zarządzania.

Zmiany i udostępnienie tekstu Instrukcji Zarządzania

§ 12

1. Dopuszcza się możliwość dokonywania zmian w Instrukcji Zarządzania.
2. Tekst Instrukcji Zarządzania jest udostępniany użytkownikom w taki sposób, aby mogli się z nim zapoznać i wdrożyć w życie jej postanowienia.

25.05.2018 roku
data

……
Administrator Danych Osobowych

PROTOKÓŁ
zniszczenia kopii zapasowej zbioru danych osobowych/ usunięcia danych z nośnika informacji zawierającego kopię zapasową

Dnia ……. roku, w siedzibie „LekSeek Polska Spółka z ograniczoną odpowiedzialnością" Spółki komandytowej w Warszawie przy ul. Puławskiej 465 dokonano zniszczenia/ usunięcia danych z kopii zapasowej zbioru danych osobowych przechowywanych

na: ……

(należy wymienić nośnik informacji: CD, pendrive etc)

Kopia zapasowa została zniszczona przez*:

……..

Dane zapisane jako kopia zapasowa zostały trwale usunięte przez*:

……..

W wykonaniu czynności stwierdzonych niniejszym protokołem wzięli udział:

……

……

* niepotrzebne skreślić