INSTRUKCJA
ZARZĄDZANIA SYSTEMAMI INFORMATYCZNYMI SŁUŻĄCYMI DO PRZETWARZANIA DANYCH OSOBOWYCH W PODHALAŃSKIEJ LOKALNEJ GRUPIE DZIAŁANIA

Opracowana zgodnie z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE

Zatwierdzono, Biały Dunajec dnia 04.10.2018 r.

DEFINICJE

Określenia i skróty użyte w niniejszej Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w PODHALAŃSKA LGD oznaczają:

Instrukcja Zarządzania:	niniejsza Instrukcja zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych
Polityka Bezpieczeństwa:	Polityka bezpieczeństwa przetwarzania danych osobowych przyjęta w PODHALAŃSKIEJ LGD dnia 04.10.2018
RODO:	Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)
GIODO:	Generalny Inspektor Ochrony Danych Osobowych
ADO / Administrator:	Administrator Danych Osobowych, tj. PODHALAŃSKA LOKALNA GRUPA DZIAŁANIA z siedzibą w PORONINIE (biuro Biały Dunajec, ul. Jana Pawła II 310)
ASI:	Administrator Systemów Informatycznych, który może być wyznaczony przez Administratora celem nadzorowania bezpieczeństwa przetwarzania danych osobowych w systemach informatycznych, zgodnie z Polityką Bezpieczeństwa
Użytkownik:	Osoba upoważniona lub użytkownik systemu posiadająca upoważnienie wydane przez Administratora lub osobę wyznaczoną przez niego i uprawniona do przetwarzania danych osobowych, w zakresie wskazanym w upoważnieniu, w sposób określony w Polityce Bezpieczeństwa
Pracownik:	osoba zatrudniona u Administratora na podstawie umowy o pracę jak również pełniąca u Administratora funkcje lub świadcząca na rzecz Administratora usługi na podstawie umowy cywilno-prawnej innej niż umowa o pracę
System:	system informatyczny w rozumieniu art. 7 pkt 2a UODO
Informatyk:	osoba zatrudniona na jakiejkolwiek podstawie prawnej przez Administratora Ochrony Danych Osobowych do wykonywania celów i zadań określonych w niniejszej Instrukcji
IOD:	inspektor ochrony danych - osoba powoływana w celu zapewnienia stosowania przepisów Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) przez przedsiębiorstwo. Pełni rolę doradczą a jego stanowisko musi być niezależne.

1. INFORMACJE OGÓLNE

1. Niniejsza Instrukcja Zarządzania określa ogólne zasady zarządzania każdym Systemem służącym do przetwarzania danych osobowych u Administratora, w sposób zapewniający

realizację zadań bezpieczeństwa zbiorów danych przetwarzanych przy pomocy tych Systemów.

2. W przypadku gdy okoliczności będą tego wymagać, dopuszcza się opracowanie na podstawie niniejszej Instrukcji Zarządzania szczegółowych Instrukcji Zarządzania poszczególnymi Systemami służącymi do przetwarzania danych osobowych u Administratora.
3. Instrukcja Zarządzania adresowana jest do wszystkich osób odpowiedzialnych u Administratora za realizację stosownie do przydzielonych uprawnień, zakresu obowiązków i odpowiedzialności w przetwarzaniu danych osobowych.
4. Instrukcja Zarządzania, w punktach w niej wskazanych, wykonywana jest przez informatyka zatrudnionego przez Administratora. Jeżeli Administrator tak postanowi informatyk może pełnić rolę ASI.
5. Jeżeli Administrator nie wyznaczy ASI, wszyscy pracownicy w wykonywaniu niniejszej Instrukcji Zarządzania podlegają bezpośrednio nadzorowi ze strony administratora w zakresie przestrzegania przepisów niniejszej instrukcji.
6. Instrukcja Zarządzania określa procedury i obowiązki Użytkowników w związku z dostępem do sieci informatycznej i Systemów, przy czym zasady te, nawet jeśli nie zostało to wyraźnie określone w Instrukcji Zarządzania, a wynika to z ich właściwości, mają zastosowanie do wszystkich Pracowników Administratora, z zastrzeżeniem ich uprawnień i obowiązków w zakresie przetwarzania danych osobowych.

2. PROCEDURY NADAWANIA, ZMIANY UPRAWNIEŃ DO PRZETWARZANIA DANYCH I REJESTROWANIA TYCH UPRAWNIEŃ W SYSTEMACH INFORMATYCZNYCH, OSOBY ODPOWIEDZIALNE

1. Każdy Użytkownik sieci informatycznej i Systemów zapoznaje się przed przystąpieniem do pracy z Instrukcją Zarządzania oraz z innymi procedurami obowiązującymi Pracowników Administratora.
2. Administrator stosuje schemat uprawnień dostępu do sieci informatycznej oraz Systemów, według założeń, iż Użytkownicy uzyskują dostęp do sieci informatycznej i poszczególnych Systemów na z góry zdefiniowanym poziomie użytkownika w zależności od zakresu obowiązków i powierzonych zadań do wykonania na danym stanowisku.
3. Nadawanie i usuwanie uprawnień do sieci informatycznej należy do Administratora danych lub osoby przez niego wyznaczonej (informatyka/ASI).
4. Dostęp do Systemów w sposób umożliwiający przetwarzanie danych osobowych uzyskują, w sposób określony w pkt. 3 powyżej, Użytkownicy, tj. osoby posiadające upoważnienie do przetwarzania danych osobowych, o którym mowa w Polityce Bezpieczeństwa.
5. Każdy Pracownik - użytkownik sieci informatycznej Administratora posiada konto w systemie umożliwiające mu dostęp do określonego zakresu danych zgromadzonych na serwerach, realizację wydruków na drukarkach sieciowych oraz uruchamianie określonych aplikacji sieciowych. Korzystanie z poczty elektronicznej jest możliwe za pomocą odrębnego konta utworzonego w systemie pocztowym.

6. Konta Użytkownika są zakładane i usuwane wyłącznie na wniosek pracownika lub według decyzji Administratora.
7. Upoważnienie do przetwarzania danych osobowych w Systemie, nadawane jest Użytkownikom, zgodnie z procedurą określoną **w Polityce Bezpieczeństwa poprzez pisemne upoważnienie/ umowę.**
8. Informatyk wykonuje prace związane usuwaniem awarii, rekonfiguracją oprogramowania, pomocą Użytkownikom w obsłudze programów użytkowych i innych. Użytkownicy zainteresowani wykonaniem jakichkolwiek prac przez informatyka, zgłaszają je pisemnie lub mailowo do akceptacji Administratora, celem wykonania prac. W przypadkach awaryjnych dopuszcza się ustne lub telefoniczne zgłoszenie wykonania prac.

3. STOSOWANE METODY I ŚRODKI UWIERZYTELNIENIA ORAZ PROCEDURY ZWIĄZANE Z ICH ZARZĄDZANIEM I UŻYTKOWANIEM

1. Ochrona informacji przed nieuprawnionym dostępem jest naczelną zasadą bezpieczeństwa sieci informatycznej i Systemów u Administratora.
2. Stosowanie zasad uwierzytelniania Użytkowników sieci informatycznej czy Systemów ma bezpośredni wpływ na zachowanie poufności, rozliczalności oraz integralności danych.
3. W związku z powyższą zasadą Administrator stosuje dwustopniowy system uwierzytelniania poszczególnych Użytkowników tj. (A) na poziomie sieci informatycznej, (B) na poziomie poszczególnych Systemów.
4. Do uwierzytelnienia Użytkownika w sieci informatycznej / Systemie stosuje się unikalne identyfikatory i hasła.
5. Unikalność identyfikatora Użytkownika polega w szczególności na tym, że nazwa identyfikatora nie może pokrywać się z nazwą identyfikatora innych użytkowników i jest nazwą niepowtarzalną, tj. nie może być nadana w późniejszym czasie innemu użytkownikowi. Użytkownik nie może korzystać z takich funkcyjnych identyfikatorów jak np. administrator, jak również nie może korzystać z identyfikatorów innych użytkowników.
6. U Administratora zastosowanie ma poziom bezpieczeństwa przetwarzania danych adekwatnie do klasyfikacji tych danych w Systemach. U administratora zaklasyfikowano poziom bezpieczeństwa przetwarzania danych jako:

   poziom podstawowy - dla Systemów, w których nie są przetwarzane dane osobowe sensytywne oraz żadne urządzenie systemu informatycznego służące do przetwarzania danych osobowych nie jest połączone z siecią publiczną. Wówczas hasło na poziomie dostępu do Systemu musi się składać z co najmniej 6-ciu znaków,

7. Hasło dostępu do sieci informatycznej nie może mieć mniej niż 8 znaków.
8. Hasło nie może być łatwe do odgadnięcia, tj. w szczególności stanowić powszechnie używane słowo, prostą sekwencję cyfr lub liter, bądź nie może kojarzyć się z użytkownikiem lub jego funkcją.

9. Hasło dostępu do sieci informatycznej / Systemu dla nowego użytkownika nadaje Informatyk. Informatyk resetuje stare hasło i nadaje nowe hasło dostępu dla użytkownika, który zapomniał swojego hasła.
10. Po nadaniu przez Zespół Informatyki hasła Użytkownikowi, o którym mowa w ust. 1, Użytkownik niezwłocznie zmienia to hasło, na tylko jemu znane hasło które zachowuje w tajemnicy jedynie do swojej wiadomości. W późniejszym czasie użytkownik w dowolnym momencie może zmienić swoje hasło.
11. Zaleca się dokonywanie zmiany hasła minimum co 30 dni. W zależności od fabrycznych ustawień Systemu zmiana hasła może być wymuszana automatycznie.
12. Każdy Użytkownik ma zakaz ujawniania innym użytkownikom swojego hasła, jak również zakaz używania haseł innych użytkowników. Hasło musi być zmienione przez Użytkownika niezwłocznie w przypadku podejrzenia lub stwierdzenia jego ujawnienia. Hasło nie może być nigdzie zapisywane.
13. Każdy Użytkownik powinien opuścić system oraz wylogować się, jeśli przerwa w pracy będzie dłuższa lub opuszcza stanowisko pracy. Zaleca się wylogowywać użytkowników, którzy zapomnieli tego uczynić.
14. Hasła nie są archiwizowane.
15. Hasła administratora posiada Informatyk lub ASI.

4. ZARZĄDZANE UPRAWNIENIAMI UŻYTKOWNIKÓW

1. Przyznanie, zmiana lub usunięcie uprawnień użytkownika do przetwarzania danych osobowych w systemie informatycznym lub w zbiorze papierowym realizowane jest przez ASI.
2. W przypadku zlecenia nadania bądź zmiany uprawnień (np. z powodu zatrudnienia osoby lub zmiany stanowiska pracy), administrator danych jest zobowiązany do sprawdzenia, czy użytkownik:
    a. Zapoznał się z obowiązującą Polityka bezpieczeństwa i oświadczył jej stosowanie
    b. Podpisał oświadczenie o zachowaniu poufności,
    c. Będzie przetwarzał dane osobowe w zakresie i celu określonym w polityce bezpieczeństwa i instrukcji zarządzania.
3. Administrator nadaje identyfikator oraz uprawnienia użytkownikowi w systemie informatycznym.
4. Usunięcie uprawnień użytkownikowi polega na wyrejestrowaniu go z systemu.
5. Identyfikator użytkownika po wyrejestrowaniu z systemu informatycznego nie może być przydzielony innej osobie.
6. Administrator odpowiada za przechowywanie i aktualizację wszystkich Upoważnień.

5. PROCEDURY ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY PRZEZNACZONE DLA UŻYTKOWNIKÓW SYSTEMU

1. Każdy Użytkownik powinien uruchomić komputer i zalogować się podając własny identyfikator i hasło dostępu.

2. Podanie przy logowaniu 3 krotnie błędnego identyfikatora lub hasła powinno powodować blokowanie się komputera Użytkownika.
3. Użytkownik przy uruchomieniu poszczególnych Systemów powinien zalogować się podając własny identyfikator i hasło dostępu.
4. Po zalogowaniu się Użytkownik winien ocenić pracę Systemu, wygląd aplikacji, dostępności opcji i stanu zbioru danych.
5. Przy każdorazowym opuszczeniu stanowiska komputerowego, należy dopilnować, aby na ekranie nie były wyświetlane informacje lub dane, poprzez zablokowanie komputera. Każdy Użytkownik ma obowiązek stosowania wygaszacza ekranu zabezpieczonego hasłem lub wylogowania się z systemu.
6. W przypadku dłuższych przerw w pracy zaleca wylogowanie się z Systemu, względnie komputera.
7. Po zakończeniu pracy Użytkownik zobowiązany jest wylogować się z Systemu, zamknąć aplikacje, następnie wylogować się z systemu operacyjnego komputera.
8. Po zakończeniu pracy Użytkownik jest zobowiązany również zweryfikować, czy nie zostały pozostawione bez nadzoru inne elektroniczne nośniki informacji zawierające dane osobowe (np. pendrive).
9. Użytkownik w pełnym zakresie odpowiada za powierzony mu sprzęt komputerowy i wykonywane czynności aż do momentu rozliczenia ze sprzętu komputerowego.
10. W przypadku podejrzenia naruszenia bezpieczeństwa Systemu (np. brak możliwości logowania się, stwierdzenia fizycznej ingerencji w przetwarzane dane, zainfekowanie komputera wirusami itd.) Użytkownik niezwłocznie informuje Informatyka.

6. ZABEZPIECZENIA INFRASTRUKTURY INFORMATYCZNEJ I TELEKOMUNIKACYJNEJ

1. W celu zabezpieczenia komputerów przed skutkami awarii zasilania - Zastosowano listwy przeciwprzepięciowe.
2. Komputery służące do przetwarzania danych osobowych są połączone z siecią lokalną
3. W przypadku, gdy zbiór danych osobowych przetwarzany jest przy użyciu komputera przenośnego, wymagane zabezpieczenia, to: szyfrowanie dysku twardego, szyfrowanie BIOS.
4. Programy zainstalowane na komputerach obsługujących przetwarzanie danych osobowych są użytkowane z zachowaniem praw autorskich i posiadają licencje.
5. Zastosowano sprzętowe i programowych środków ochrony przed nieuprawnionym dostępem do danych osobowych, w tym środki zapewniające rozliczalność wykonywanych operacji:
   - Lokalizacja urządzeń komputerowych uniemożliwia osobom niepowołanym dostęp do nich.

- Dostęp do zbioru danych osobowych, który przetwarzany jest na wydzielonej stacji komputerowej / komputerze przenośnym zabezpieczony został przed nieautoryzowanym uruchomieniem za pomocą hasła BIOS.
- Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.

6. Zastosowano sprzętowe i programowe środki ochrony poufności danych przesyłanych drogą elektroniczną (środków ochrony transmisji),
   - Zastosowano środki kryptograficznej ochrony danych dla danych osobowych przekazywanych drogą teletransmisji.
   - Dostęp do środków teletransmisji zabezpieczono za pomocą mechanizmów uwierzytelnienia.
7. Zastosowano sprzętowe i programowe środki ochrony przed szkodliwym oprogramowaniem i nieuprawnionym dostępem do przetwarzanych danych
   - Zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity, inne.
   - Użyto zapory sieciowej do ochrony dostępu do sieci komputerowej.

7. ZABEZPIECZENIA BAZ DANYCH I OPROGRAMOWANIA PRZETWARZAJĄCEGO DANE OSOBOWE

1. Dostęp do zbioru danych osobowych (do bazy danych i do programów) wymaga uwierzytelnienia z wykorzystaniem identyfikatora oraz hasła.
2. Zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do zbioru danych osobowych.
3. Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe.
4. Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.
5. Zastosowano system antywirusowy na stanowiskach, na których przetwarzane są dane osobowe.
6. Kopie zapasowe danych tworzone są automatycznie z wykorzystaniem skryptów oraz oprogramowania do zarządzania kopiami bezpieczeństwa.

8. PROCEDURA 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 do celów prywatnych wyłącznie okazjonalnie i powinno być ono ograniczone do niezbędnego minimum.
4. Korzystanie z Internetu do 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. Nie należy w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł.
7. Należy korzystać wyłącznie z przeglądarek posiadających odpowiednie opcje zabezpieczeń.
8. W przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, należy zwracać uwagę na pojawienie się odpowiedniej ikonki (kłódka, protokół https).

9. PROCEDURA 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 do celów prywatnych wyłącznie okazjonalnie i powinno być to ograniczone do niezbędnego minimum.
4. Korzystanie z Systemu Poczty Elektronicznej do 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 świadomy 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 silnym hasłem (duże i małe litery i cyfry lub znaki specjalne). Hasło należy przesłać odrębnym e-mailem.
14. Cała korespondencja wpływająca na służbową skrzynkę jest korespondencją służbową. Użytkownicy nie powinni rozsyłać, wiadomości zawierających załączniki o dużym rozmiarze dla większej liczby adresatów - określenie krytycznych rozmiarów przesyłek i krytycznej liczby adresatów jest uzależnione od wydajności systemu poczty elektronicznej
15. Użytkownicy powinni okresowo kasować niepotrzebne wiadomości pocztowe.

10. PROCEDURA ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY

Celem procedury jest zabezpieczenie danych osobowych przed nieuprawnionym dostępem i utratą poufności w sytuacji, gdy użytkownik rozpoczyna, przerywa lub kończy pracę w systemie informatycznym przetwarzającym dane osobowe.

1. Użytkownik rozpoczyna pracę z systemem informatycznym przetwarzającym dane osobowe z użyciem identyfikatora i hasła.
2. Użytkownik jest zobowiązany do powiadomienia Inspektora ochrony danych osobowych oraz o próbach logowania się do systemu osoby nieupoważnionej, jeśli system to sygnalizuje.
3. W przypadku, gdy użytkownik podczas próby zalogowania się zablokuje system, zobowiązany jest powiadomić o tym administratora danych, który odpowiada za odblokowanie systemu użytkownikowi.
4. Użytkownik jest zobowiązany do uniemożliwienia osobom niepowołanym (np. klientom, pracownikom innych działów) wgląd do danych wyświetlanych na monitorach komputerowych – **tzw. Polityka czystego ekranu.**

5. Przed czasowym opuszczeniem stanowiska pracy, użytkownik zobowiązany jest wywołać blokowany hasłem wygaszacz ekranu lub wylogować się z systemu. Jeżeli tego nie uczyni – po upływie 20 minut system automatycznie aktywuje wygaszacz.
6. Po zakończeniu pracy, użytkownik zobowiązany jest:
   11. wylogować się z systemu informatycznego.
   12. zabezpieczyć stanowisko pracy, w szczególności wszelką dokumentację oraz nośniki magnetyczne i optyczne, na których znajdują się dane osobowe.

11. ZABEZPIECZENIE ELEKTRONICZNYCH NOŚNIKÓW INFORMACJI – TWARDE DYSKI, PŁYTY CD/DVD, PENDRIVE, TELEFONY KOMÓRKOWE ITP.

1. Nośniki danych są przechowywane w sposób uniemożliwiający dostęp do nich osób nieupoważnionych, jak również zabezpieczający je przed zagrożeniami środowiskowymi (zalanie, pożar, wpływ pól elektromagnetycznych)
2. Nośniki danych domyślnie zablokowane są przez program antywirusowy
3. Nośniki danych są ewidencjonowane w załączniku nr 6 - rejestr nośników komputerowych.
4. Zabrania się wynoszenia poza obszar organizacji wymiennych nośników informacji a w szczególności twardych dysków z zapisanymi danymi osobowymi bez zgody ADO.
5. W sytuacji przekazywania nośników z danymi osobowymi poza obszar organizacji należy stosować następujące zasady bezpieczeństwa:
   a. adresat powinien zostać powiadomiony o przesyłce,
   b. nadawca powinien sporządzić kopię przesyłanych danych,
   c. dane przed wysłaniem powinny zostać zaszyfrowane, a hasło podane adresatowi inną drogą,
   d. stosować bezpieczne koperty depozytowe,
   e. przesyłkę należy przesyłać przez kuriera,
   f. adresat powinien powiadomić nadawcę o otrzymaniu przesyłki.
6. Użytkownicy są zobowiązani do niezwłocznego i trwałego usuwania/kasowania danych osobowych z nośników informacji po ustaniu powodu ich przechowywania (chyba, że z powodu odrębnych przepisów należy je zachować na dłużej).
7. Podlegające likwidacji uszkodzone lub przestarzałe nośniki, a w szczególności twarde dyski z danymi osobowymi są komisyjnie niszczone w sposób fizyczny w/g Załącznika nr 4.
8. Nośniki informacji zamontowane w sprzęcie IT, a w szczególności twarde dyski z danymi osobowymi powinny być wymontowane lub wyczyszczone specjalistycznym oprogramowaniem, zanim zostaną przekazane poza obszar organizacji (np. sprzedaż lub darowizna komputerów stacjonarnych / laptopów).

12. ZABEZPIECZENIA SYSTEMU INFORMATYCZNEGO, W TYM PRZED WIRUSAMI KOMPUTEROWYMI

Celem administratora jest zabezpieczenie systemów informatycznych przed szkodliwym oprogramowaniem (np. typu robaki, wirusy, konie trojańskie, rootkity) oraz nieautoryzowanym dostępem do systemów przetwarzających dane osobowe

1. System jest zabezpieczony przez program antywirusowy.
2. System antywirusowy zapewnia: ochronę przed szkodliwym oprogramowaniem dla stacji roboczych i serwerów plików, funkcje kontroli urządzeń oraz sieci, kontrole aplikacji, zarządzanie systemami, ochronę przed Ransomware, ochronę poczty email, ochronę bankowości i zakupów online, ochronę przed spamem
3. Użytkownicy zobowiązani są do skanowania plików przychodzących programem antywirusowym, chyba że program antywirusowy robi to automatycznie.
4. Aktualizacja definicji wirusów odbywa się automatycznie przez system.
5. W przypadku stwierdzenia pojawienia się wirusa, każdy użytkownik winien powiadomić Administratora danych.

13. OCHRONA PRZED NIEAUTORYZOWANYM DOSTĘPEM DO SIECI LOKALNEJ

Stosowane zabezpieczenia mają na celu zabezpieczenie systemów informatycznych przed nieautoryzowanym dostępem do sieci lokalnej np. przez programy szpiegujące, hackerów.

7. Stosowana jest Zapora i ochrona sieci
8. Zastosowano mechanizmy kontroli dostępu do sieci przez osoby nieupoważnione.

14. ZASADY I SPOSÓB ODNOTOWYWANIA W SYSTEMIE INFORMACJI O UDOSTĘPNIENIU DANYCH OSOBOWYCH

1. Odbiorcą danych jest każdy, komu udostępnia się dane osobowe, z wyłączeniem:
    a. osoby, której dane dotyczą,
    b. osoby, upoważnionej do przetwarzania danych,
    c. administratora mającego siedzibę w państwie trzecim,
    d. podmiotu, któremu powierzono przetwarzanie danych,
    e. organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.
2. System przetwarzający dane osobowe udostępniane odbiorcom musi umożliwiać rejestrację:
    a. nazwy jednostki organizacyjnej lub imienia i nazwiska osoby, której udostępniono dane,
    b. zakresu udostępnianych danych,
    c. daty udostępnienia.
3. Dane osobowe udostępnia się:

   a. osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa,
   b. pozostałym osobom lub podmiotom, jeżeli w sposób wiarygodny uzasadnią potrzebę posiadania tych danych, a ich udostępnienie nie naruszy praw i wolności osób, których dane dotyczą.
4. Dane osobowe udostępnia się na pisemny, umotywowany wniosek, chyba że przepis innej ustawy stanowi inaczej.
5. Na żądanie osoby, której dane zostały udostępnione, informacje o udostępnieniu danych są zamieszczane w raporcie z systemu informatycznego lub wyciągu z rejestru papierowego, a raport przekazywany jest tej osobie.
6. Odnotowanie informacji o udostępnieniu danych (komu, zakresie, dacie) powinno nastąpić niezwłocznie po udostępnieniu danych:
   a. w systemie informatycznym, jeśli przetwarza udostępnione dane osobowe,
   b. w postaci ewidencji udostępniania danych. (patrz Załącznik nr 5)

15. BEZPIECZEŃSTWO DANYCH OSOBOWYCH KLIENTÓW WE WSPÓŁPRACY Z PODMIOTAMI PRZETWARZANIA DANYCH.

1. Administrator może powierzyć przetwarzanie danych osobowych Podmiotowi zewnętrznemu – tzw. Podmiotowi przetwarzania.
2. Obowiązki podmiotu przetwarzającego względem administratora muszą być określone w umowie lub innym akcie prawnym. Umowa musi wskazywać, co się stanie z danymi osobowymi po rozwiązaniu umowy.
3. Podmiot przetwarzający dane może zlecić innemu podmiotowi przetwarzającemu podwykonawstwo części swoich obowiązków albo wyznaczyć podmiot współprzetwarzający dane wyłącznie po otrzymaniu uprzedniej pisemnej zgody administratora danych.
4. Po stronie Podmiotu przetwarzania zapewniony jest Rozszerzony obowiązek informacyjny, poprzez zawarcie szczegółowych informacji w umowie dla klienta, w jakim celu, w jaki sposób, jak długo i komu powierzane są jego dane i kto jest Inspektorem Ochrony Danych Podmiotu.
5. W przypadku wycieku danych należy jak najszybciej poinformować o tym Podmiot przetwarzania, który przetwarza powierzone mu dane administratora.

16. PRZEGLĄDY I KONSERWACJE SYSTEMU INFORMATYCZNEGO I APLIKACJI

1. Administrator danych odpowiada za bezawaryjną pracę systemu IT, w szczególności: stacji roboczych, aplikacji serwerowych, baz danych, poczty email.
2. Przegląd i konserwacja systemu informatycznego powinny być wykonywane w terminach określonych przez producentów systemu.
3. Za terminowość przeprowadzenia przeglądów i konserwacji oraz ich prawidłowy przebieg odpowiada administrator danych.

4. Administrator danych odpowiada za sprawdzanie poprawności działania systemu IT, w szczególności: stacji roboczych, serwerów, drukarek, baz danych, poczty email.
5. Administrator danych odpowiada za identyfikację i przyjmowanie zgłoszeń o nieprawidłowościach w działaniu systemu informatycznego oraz oprogramowania celem ich niezwłocznego usunięcia.
6. Wszelkie prace konserwacyjne i naprawcze sprzętu komputerowego oraz uaktualnienia systemu informatycznego, wykonywane przez podmiot zewnętrzny, powinny odbywać się na zasadach określonych w szczegółowej umowie z uwzględnieniem klauzuli dotyczącej ochrony danych.
7. Czynności konserwacyjne i naprawcze wykonywane doraźnie przez osoby nie posiadające upoważnień do przetwarzania danych (np. specjalistów z firm zewnętrznych), muszą być wykonywane pod nadzorem osób upoważnionych.
8. Przed przekazaniem uszkodzonego sprzętu komputerowego z danymi osobowymi do naprawy poza teren organizacji, należy:
    a. wymontować nośniki z danymi osobowymi,
    b. trwale usunąć dane osobowe z użyciem specjalistycznego oprogramowania,
    c. nadzorować proces naprawy przez osobę upoważnioną przez administratora danych, gdy nie ma możliwości usunięcia danych z nośnika.

17. AKTUALIZACJE OPROGRAMOWANIA

1. IOD/ ADO odpowiada za aktualizację oprogramowania zgodnie z zaleceniami producentów co do bezpieczeństwa i stabilności nowych wersji (np. aktualizacje, service pack-i, łatki).
2. IOD/ ADO odpowiada za zapewnienie licencjonowanego oprogramowania do przetwarzania danych osobowych.

18. POSTANOWIENIA KOŃCOWE

1. Instrukcja zarządzania została zatwierdzona przez Administratora i podana do wiadomości u Administratora osobom odpowiedzialnym za realizację zadań związanych z ochroną danych osobowych w dniu 04.10.2018 r. i weszła w życie z dniem podjęcia uchwały Zarządu zatwierdzającej ją.
2. Instrukcja Zarządzania zastępuje poprzednio obowiązujące u Administratora regulacje dotyczące ochrony danych osobowych przetwarzanych w systemach informatycznych
3. Instrukcja Zarządzania winna być na bieżąco weryfikowana i dostosowywana do aktualnego stanu faktycznego i prawnego związanego z ochroną przetwarzania danych osobowych u Administratora.