PROCEDURA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM PRZETWARZAJĄCYM DANE OSOBOWE

Podpis zatwierdzającego	*02.11.2023* */Data zatwierdzenia/*	**Obowiązuje od:** **06.11.2023**

SPIS TREŚCI

1. CEL PROCEDURY.

Niniejsza procedura opisuje sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych. Dokument ten określa procedury dotyczące korzystania z systemów informatycznych, nadawania uprawnień czy też sposobu ewidencji użytkowników systemów informatycznych.

2. SŁOWNIK POJĘĆ.

Administrator danych osobowych (Administrator) – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych;

Administrator Systemów Informatycznych (ASI) – Prezes Zarządu lub wyznaczony pracownik/osoba współpracująca zajmująca się zarządzaniem całością systemu informatycznego, odpowiadająca za jego sprawne działanie. Do zadań Administratora Systemów Informatycznych należy nadzorowanie pracy serwerów, dodawanie i usuwanie kont, nadawanie uprawnień użytkownikom, konfiguracja komputerów, instalowanie oprogramowania, dbanie o bezpieczeństwo systemu, nadzorowanie, eliminowanie nieprawidłowości,

Inspektora Ochrony Danych (IOD) - wyznaczona przez Administratora, zgodnie z Polityką Bezpieczeństwa przetwarzania danych osobowych, osoba fizyczna odpowiedzialna za bezpieczeństwo danych osobowych przetwarzanych w systemie informatycznym, a w szczególności za przeciwdziałanie dostępowi osób niepowołanych do systemu informatycznego, podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń oraz nadzór nad mechanizmem uwierzytelniania użytkowników. Zakres odpowiedzialności Inspektora Ochrony Danych wyznaczają przepisy o ochronie danych osobowych, Polityka Bezpieczeństwa, Instrukcja oraz odpowiednie zarządzenia wewnętrzne Administratora,

informatyczne nośniki danych - urządzenia, dyski lub inne informatyczne nośniki, które służą do przetwarzania i gromadzenia danych osobowych,

informatyczne szyfrowany nośniki danych - urządzenia, dyski lub inne informatyczne nośniki, które służą do przetwarzania i gromadzenia danych osobowych, posiadające wbudowany mechanizm szyfrowania i uwierzytelniania.

mechanizm uwierzytelniania użytkownika - rozumie się przez działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu poprzez indywidualnie ustalane hasło i identyfikator pozwalające na dostęp do określonych zasobów informacyjnych w systemie informatycznym,

obszar przetwarzania danych osobowych - budynki, pomieszczenia, części pomieszczeń, w których przetwarzane są dane osobowe z użyciem stacjonarnego sprzętu komputerowego, określony w Polityce Bezpieczeństwa,

przetwarzanie danych osobowych - jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemie informatycznym,

użytkownik - osoba o ściśle określonym zakresie uprawnień i obowiązków, która posiada indywidualny identyfikator oraz hasło pozwalające na korzystanie z systemu informatycznego

3. ZASADY NADAWANIA UPRAWNIEŃ.

3.1 Przydzielanie uprawnień do systemu informatycznego realizowane jest w oparciu o następujące zasady:

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.

3.2 Dostęp do systemu informatycznego mogą posiadać, w zależności od wykonywanych czynności służbowych lub umownych:

3.3 Dostęp do systemu informatycznego mogą posiadać, w zależności od wykonywanych czynności służbowych lub umownych:

- pracownicy Administratora w zakresie niezbędnym do właściwego wykonywania obowiązków służbowych;
- osoby, przy pomocy których Administrator 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;
  c) stażyści, na podstawie umowy z Urzędem Pracy;
  d) praktykanci, na podstawie umowy ze szkołą wyższą;
  e) wolontariusze, na podstawie umowy o wolontariat.

3.4 Użytkownik systemu informatycznego jest jednoznacznie identyfikowany poprzez nadany mu indywidualny identyfikator użytkownika.

3.5 Niedopuszczalne jest korzystanie z tego samego identyfikatora przez więcej niż jednego użytkownika.

3.6 Raz użyty identyfikator nie może być przydzielony innemu użytkownikowi.

3.7 Uprawnienia dostępu są nadawane wyłącznie w zakresie wynikającym z zajmowanego stanowiska i potrzeby wykonywania obowiązków służbowych na danym stanowisku pracy. Bezzasadne nadawanie uprawnień (przywilejów) będzie kwalifikowane jako incydent związany z bezpieczeństwem informacji.

3.8 Użytkownikowi systemu informatycznego zostaje nadany dostęp po:

1) zapoznaniu z przepisami, w tym niniejszą dokumentacją przetwarzania danych osobowych, dotyczącymi ochrony danych osobowych;
2) podpisaniu oświadczenia o zachowaniu informacji (w tym danych osobowych), do których użytkownik będzie miał dostęp podczas wykonywania obowiązków służbowych lub zobowiązań umownych oraz środków ich zabezpieczania w tajemnicy (również po ustaniu łączącej strony umowy), w tym powstrzymanie się od wykorzystywania ich w celach pozasłużbowych;
3) otrzymaniu upoważnienia do przetwarzania danych osobowych.

3.9 Rejestr użytkowników wraz z uprawnieniami do systemu lub aplikacji prowadzi ASI.

3.10 Rejestr, o którym mowa powyżej prowadzony jest w postaci elektronicznej lub papierowej.

3.11 Weryfikację aktualności rejestru, o którym mowa powyżej prowadzi ASI we współdziałaniu ze osobami odpowiedzialnymi za wnioskowanie o nadanie/modyfikację/odebranie uprawnień do systemu informatycznego.

3.12 ASI nie rzadziej, jak raz na kwartał dokonuje przeglądu stanu aktywności kont użytkowników.

4. NADAWANIE, MODYFIKACJA UPRAWNIEŃ.

4.1 Nadawanie uprawnień użytkownikowi, następuje na podstawie wniosku złożonego przez jego przełożonego lub Administratora w formie papierowej lub elektronicznej. Wniosek powinien zawierać informację o profilu uprawnień zgodnym z obowiązującym katalogiem oraz przyjętym zakresem obowiązków na danym stanowisku lub wynikającym z umowy. Wypełniony wniosek należy przekazać ASI.

4.2 W przypadku konieczności Administrator lub bezpośredni przełożony użytkownika zgłasza do ASI wniosek o zmianę uprawnień do zasobu systemu informatycznego zgodnie ze wzorem „Wniosek o nadanie, modyfikację, odebranie uprawnień do systemu informatycznego".

4.3 ASI realizuje otrzymany wniosek lub odmawia nadania/modyfikacji uprawnień do systemu informatycznego w przypadku uchybienia wymogom określonym w niniejszym dokumencie lub powzięciu podejrzeń co do przekroczenia uprawnień wymaganych na danym stanowisku. Każdą odmowę nadania należy potraktować jako incydent.

4.4 W przypadku nadania/modyfikacji uprawnień wymagających logowania, ASI przekazuje użytkownikowi informację zawierającą wymienione z nazwy systemy informatyczne, do których użytkownik otrzymał dostęp oraz login i hasło na potrzeby pierwszego logowania.

4.5 Wzór wniosku o nadanie/modyfikację uprawnień stanowi załącznik „Wniosek o nadanie, modyfikację, odebranie uprawnień do systemu informatycznego".

5. ODEBRANIE/BLOKOWANIE UPRAWNIEŃ.

5.1 ASI jest uprawniony do odebrania/blokowania uprawnień dostępu do systemów informatycznych w momencie:

a) otrzymania od Administratora, upoważnionego przez niego pracownika lub przełożonego pracownika informacji (w dowolnej formie) o utracie lub zmianie uprawnień użytkownika odnośnie dostępu do zasobów informatycznych,

b) powzięciu podejrzeń co do przekroczenia uprawnień przez użytkownika systemów. Każde odebranie/blokowanie uprawnień zgodnie z pkt 5.1b należy potraktować jako incydent.

5.2 Odbieranie/blokowanie uprawnień użytkownikowi, następuje na podstawie wniosku złożonego przez jego przełożonego lub Administratora w formie papierowej lub elektronicznej. Wypełniony wniosek należy przekazać ASI.

5.3 Terminami obowiązującymi przy składaniu wniosku są w szczególności:

1) w przypadku zakończenia współpracy/ustania stosunku pracy – wniosek odbierający wszystkie uprawnienia – natychmiast, najpóźniej ostatniego dnia pracy;

2) długotrwałe zwolnienie lekarskie – wniosek odbierający wszystkie uprawnienia – natychmiast po upływie 30 (trzydziestu) dni kalendarzowych zwolnienia lekarskiego;

3) zmiana zakresu obowiązków – wniosek modyfikujący uprawnienia – natychmiast, najpóźniej ostatniego dnia przed zmianą zakresu obowiązków.

5.4 ASI przyjmuje, weryfikuje i bezzwłocznie realizuje wniosek o odebranie uprawnień do systemu informatycznego spełniający wymogi określone niniejszą instrukcją.

5.5 Wzór wniosku o odebranie uprawnień stanowi załącznik „Wniosek o nadanie, modyfikację, odebranie uprawnień do systemu informatycznego".

6. ZARZĄDZANIE UPRZYWILEJOWANYMI KONTAMI.

6.1 Uprzywilejowane konto w systemie na wniosek Administratora zakłada ASI.

6.2 Uprzywilejowane konto nie może służyć do realizacji przez użytkownika rutynowych zadań.

6.3 Przywileje podlegają cofnięciu niezwłocznie po ustaniu potrzeby uzasadniającej ich nadanie.

6.4 Nadawane przywileje podlegają regularnym przeglądom i kontroli.

6.5 W stosunku do haseł użytkowników uprzywilejowanych stosuje się zaostrzone standardy bezpieczeństwa.

6.6 Standardy, o których mowa powyżej stosuje się również do haseł:

1) elementów aktywnych sieci teleinformatycznych;
2) konfiguracji komputerów, w tym hasła do BIOS.
3) predefiniowanych lub utworzonych kont stosowanych do administrowania systemami informatycznymi oraz kont do administrowania serwerami, na których te systemy działają.

6.7 Hasła, o których mowa w w/w pkt 6.6 przechowuje się w postaci zaszyfrowanej.

6.8 Do przechowywania haseł zapisanych na papierze stosuje się wyłącznie koperty, które uniemożliwiają otwarcie bez uszkodzenia ich struktury (tzw. „koperty bezpieczne”).

6.9 Koperty z hasłami przechowuje się w sejfie, w miejscu zapewniającym dostęp tylko osobom upoważnionym.

6.10 Dane umieszczone na bezpiecznej kopercie zawierają:

4) numer koperty adekwatny do numeru ewidencyjnego podanego w ewidencji haseł;
5) datę jej złożenia i podpis osoby składającej kopertę;

6.11 Koperty z hasłami do kont o których mowa w w/w pkt 6.6 podlegają ścisłej ewidencji prowadzonej przez ASI.

6.12 Ewidencja haseł do kont o których mowa w w/w pkt 6.6 przechowywana jest w miejscu zabezpieczonym przed dostępem osób niepowołanych.

6.13 Za aktualność przechowywanych haseł do kont o których mowa w w/w pkt 6.6 odpowiedzialny jest ASI.

6.14 Awaryjne otwarcie bezpiecznej koperty oraz pobranie kopii hasła znajdującego się w kopercie wymaga uprzedniej pisemnej akceptacji Administratora lub osoby przez niego upoważnionej i jest udokumentowane w ewidencji kopert.

6.15 Po użyciu, hasło ulega zniszczeniu, a w to miejsce jest generowane nowe hasło, którego kopia jest przechowywana na identycznych zasadach jak w przypadku zniszczonego hasła.

7. STOSOWANE METODY I ŚRODKI UWIERZYTELNIENIA.

7.1 Każdy użytkownik systemu informatycznego musi posiadać unikalny identyfikator i wprowadzone przez siebie hasło autoryzujące jego osobę w systemie informatycznym.

7.2 Użytkownik ponosi pełną odpowiedzialność za utworzenie hasła (prócz pierwszego hasła do systemu nadawanego przez administratora systemu informatycznego) i jego przechowywanie.

7.3 Osoba pełniąca funkcję ASI powinna posiadać dodatkowo odrębne konto służące tylko i wyłącznie do administracji danym systemem informatycznym, o ile dany system udostępnia taką funkcjonalność.

7.4 Każdy użytkownik posiadający dostęp do systemu informatycznego jest obowiązany do:

1) zachowania w poufności wszystkich swoich haseł lub innych danych uwierzytelniających wykorzystanych do pracy w systemie informatycznym;
2) niezwłocznej zmiany haseł w przypadkach zaistnienia podejrzenia lub rzeczywistego ujawnienia;
3) niezwłocznej zmiany hasła tymczasowego, przekazanego przez ASI;
4) poinformowania ASI oraz IOD o podejrzeniu lub rzeczywistym ujawnieniu hasła;
5) Zmiany wykorzystywanych haseł nie rzadziej niż raz na 90 dni.

7.5 Zabronione jest:

1) zapisywanie haseł w sposób jawny i umieszczania ich w miejscach dostępnych dla innych osób;
2) stosowanie haseł opartych na skojarzeniach, łatwych do odgadnięcia lub wywnioskowania z informacji dotyczących danej osoby, np. imiona, numery telefonów, daty urodzenia itp.;
3) używanie tych samych haseł w różnych systemach operacyjnych i aplikacjach;
4) udostępnianie haseł innym użytkownikom;
5) przeprowadzanie prób łamania haseł;
6) wpisywanie haseł „na stałe” (np. w skryptach logowania) oraz wykorzystywania opcji auto-zapamiętywania haseł (np. w przeglądarkach internetowych).

7.6 ASI obowiązany jest do skonfigurowania systemu, aby próby dostępu do tego systemu były limitowane zarówno w ujęciu ilościowym, jak i czasowym jeżeli system umożliwia wymienioną konfigurację.

7.7 W przypadku, gdy system umożliwia limitowanie wprowadzenia błędnego hasła, należy przyjąć próg ilości wprowadzonych błędnych haseł na 5, po czym ustanowić blokadę konta.

7.8 ASI ograniczył możliwość wielokrotnego logowania, gdzie użytkownik loguje się na kilku komputerach równocześnie wykorzystując ten sam identyfikator.

7.9 ASI odblokowuje/zresetuje hasło do danego systemu informatycznego w przypadku przekroczenia przez użytkownika ustalonej ilości prób logowania po weryfikacji przyczyny blokady z właścicielem konta lub jego przełożonym. Po odblokowaniu dostępu do konta/zresetowaniu hasła ASI przekazuje stosowną informację użytkownikowi.

8. ZABEZPIECZENIA KRYPTOGRAFICZNE, ZARZĄDZANIE KLUCZAMI.

8.1 Technologia kryptograficzna używana jest w następujących przypadkach:

1) zabezpieczenie danych znajdujących się na komputerach przenośnych, autoryzacja z wykorzystaniem użytkownika i hasła lub klucza kryptograficznego
2) zabezpieczenie połączeń zdalnych do infrastruktury Administratora z wykorzystaniem kanałów VPN,
3) bezpieczne logowanie poprzez sieć Internet do usług administrowanych przez firmy trzecie – dostęp https i protokół SSL, poczta elektroniczna,
4) przesyłania danych pocztą elektroniczną z użyciem protokołów szyfrowania połączenia (TLS lub SSL),
5) szyfrowania plików będących załącznikami do wiadomości e-mail.

8.2 Klucze kryptograficzne zmienia się w momencie:

1) zauważenia incydentu związanego z naruszeniem bezpieczeństwa stosowania urządzeń kryptograficznych,
2) gdy zachodzi podejrzenie, że mogły się dostać/pozostać w rękach osób nieupoważnionych (np. zagubienia sprzętu, w przypadku wygaśnięcia stosunku pracy, zakończenia umowy o współpracy z firmami mającymi do nich dostęp).

9. PROCEDURY ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY.

9.1 Rozpoczęcie pracy w systemie informatycznym następuje po wprowadzeniu unikalnego identyfikatora i hasła.

9.2 Zawieszenie pracy w systemie informatycznym, tj. brak wykonywania jakichkolwiek czynności przez okres 5 minut w systemie informatycznym, powoduje automatycznie uruchomienie systemowego wygaszacza ekranu blokowanego hasłem. Zastosowanie powyższego mechanizmu nie zwalnia użytkownika z obowiązku każdorazowego blokowania ekranu wygaszaczem chronionym hasłem po odejściu od stanowiska.

9.3 Przed zakończeniem pracy użytkownik ma obowiązek upewnić się, czy dane zostały zapisane, aby uniknąć utraty danych.

9.4 Po zakończeniu pracy, użytkownik obowiązany jest wylogować się z systemu informatycznego przetwarzającego dane osobowe i z systemu operacyjnego, zabezpieczyć nośniki informacji (elektroniczne i papierowe) oraz wyłączyć komputer.

9.5 W sytuacji, gdy wgląd w wyświetlane na monitorze dane może mieć nieuprawniona osoba, trzeba tymczasowo zmienić widok wyświetlany na monitorze lub obrócić monitor (przymknąć ekran laptopa) w sposób uniemożliwiający wgląd w wyświetlaną treść.

9.6 Użytkownik systemu informatycznego przetwarzającego dane osobowe niezwłocznie powiadamia ASI lub IOD w przypadku, gdy:

1) wygląd systemu, sposób jego działania, zakres danych lub sposób ich przedstawienia przez system informatyczny odbiega od standardowego stanu uznawanego za typowy dla danego systemu informatycznego;

2) niektóre opcje, dostępne użytkownikowi w normalnej sytuacji, przestały być dostępne lub też opcje niedostępne użytkownikowi w normalnej sytuacji, stały się dostępne.

10. ZASADY KORZYSTANIA ZE SŁUŻBOWEJ POCZTY ELEKTRONICZNEJ.

10.1 W przypadku możliwości ASI nadaje użytkownikowi dedykowany adres skrzynki poczty elektronicznej działający w domenie Administratora.

10.2 Korespondencja elektroniczna związana z działalnością Administratora powinna być prowadzona przez służbową skrzynkę poczty elektronicznej użytkownika z użyciem protokołów szyfrowania połączenia (TLS lub SSL).

10.3 Załączniki do korespondencji, przesyłane w postaci plików, które zawierają dane osobowe lub niejawne powinny być szyfrowane. Hasło do pliku należy przekazać adresatowi podczas rozmowy telefonicznej lub przesłać inna drogą elektroniczną (np. SMS).

10.4 Informacja o służbowym adresie skrzynki pocztowej jest jawna i dostępna powszechnie, w tym może być dostępna na łamach witryny internetowej Administratora w postaci książki adresowej.

10.5 Nadany użytkownikowi adres skrzynki poczty elektronicznej służy wyłącznie do realizacji celów służbowych lub umownych. Korespondencja realizowana drogą elektroniczną z wykorzystaniem systemów informatycznych Administratora podlega rejestrowaniu i może być monitorowana. Informacje przesyłane za pośrednictwem sieci Administratora (w tym do i z Internetu) nie stanowią własności prywatnej użytkownika.

10.6 Wszelka korespondencja elektroniczna niezwiązana z działalnością Administratora powinna być prowadzona przez prywatną skrzynkę poczty elektronicznej użytkownika. Korzystanie z systemu poczty elektronicznej dla celów prywatnych nie może wpływać na wydajność systemu poczty elektronicznej.

10.7 Użytkownicy dokonujący wysyłki korespondencji masowej poza organizację, obowiązani są do ukrywania odbiorów w kopii (pole BCC lub UDW).

10.8 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;
3) odbieranie przesyłek z nieznanych źródeł;
4) otwieranie załączników z plikami samorozpakowującymi się bądź wykonalnymi typu exe, com, itp.;
5) przesyłanie pocztą elektroniczną plików wykonywalnych typu: bat, com, exe. Zabronione jest również przesyłanie plików multimedialnych i plików graficznych niezwiązanych z działalnością Administratora;
6) ukrywanie lub dokonywanie zmian tożsamości nadawcy;
7) czytanie, usuwanie, kopiowanie lub zmiana zawartości skrzynek pocztowych innego użytkownika;
8) odpowiadanie na niezamówione wiadomości reklamowe lub wysyłane łańcuszki oraz na inne formy wymiany danych określanych spamem; w przypadku otrzymania takiej wiadomości należy przesłać ją administratorowi systemu informatycznego;
9) posługiwanie się adresem służbowym e-mail w celu rejestrowania się na stronach handlowych, informacyjnych, chat'ach lub forach dyskusyjnych, które nie dotyczą zakresu wykonywanej pracy lub obowiązków umownych;
10) wykorzystywanie poczty elektronicznej do reklamy prywatnych towarów lub usług, działalności handlowo-usługowej innej niż wynikającej z potrzeb Administratora lub do poszukiwania dodatkowego zatrudnienia.

11. ZASADY KORZYSTANIA Z SIECI PUBLICZNEJ (INTERNET).

11.1 Sieć, w której pracują urządzenia komputerowe Administratora musi być odseparowana od sieci publicznej zaporą oraz systemem wykrywania włamań (IPS).

11.2 Zdalne korzystanie z systemów informatycznych poprzez sieć publiczną może mieć miejsce po zastosowaniu systemu uwierzytelniania użytkownika i szyfrowanego kanału transmisji.

11.3 Zdalny dostęp do serwerów w celach administracyjnych może mieć miejsce po zastosowaniu systemu umożliwiających uwierzytelnianie użytkownika, szyfrowanie kanału transmisji i rejestracji dostępu.

11.4 Systemy informatyczne powinny korzystać z szyfrowanych protokołów wymiany danych, w szczególności połączeń sftp i https.

11.5 Dostęp użytkowników do sieci publiczne (Internet) jest ograniczony do niezbędnego minimum na danym stanowisku pracy.

11.6 Dostęp do przeglądania stron internetowych możliwy jest po nadaniu odpowiednich uprawnień (USER, VIP, GUEST).

11.7 Wprowadza się całkowite ograniczenia w dostępie do treści uznanych za pornograficzne, rasistowskie, traktujące o przemocy, przestępstwach, jak również do protokołów umożliwiających wymianę plików w sieciach z naruszeniem przepisów prawa.

11.8 Dostęp do protokołu wymiany plików możliwy jest w uzasadnionych przypadkach, po nadaniu odpowiednich uprawnień.

11.9 Dalsze ograniczenia dostępu do sieci Internet mogą być rekomendowane przez administratora bezpieczeństwa informacji.

12. ZASADY KORZYSTANIA Z SIECI LOKALNEJ.

12.1 Sieć lokalna służy do przechowywania danych biznesowych współdzielonych pomiędzy pracownikami, w ramach poszczególnych działów.

12.2 ASI jest odpowiedzialny za nadawanie uprawnień do poszczególnych katalogów sieciowych na podstawie zaakceptowanego przez Administratora i właściciela katalogu sieciowego wniosku o nadanie uprawnień od przełożonego danego działu.

12.3 Użytkownik nie może przechowywać w sieci lokalnej plików osobistych takich jak zdjęcia, pliki multimedialne i innych danych objętych prawami autorskimi.

12.4 Uprawnienia do katalogów są przydzielane poprzez dodanie użytkownika do jednej z poniższych grup:

1) Grupa ADM – przeznaczona dla administratorów, mających uprawnienia „full access”,
2) Grupa READ – przeznaczona dla użytkowników mających mieć dostęp „tylko do odczytu”
3) Grupa CHANGE – przeznaczona dla użytkowników mających mieć dostęp „read and write”
4) Grupa LIST – zapewniająca wejście do katalogu i wylistowanie jego zawartości.

12.5 Użytkownik nie może podłączać do sieci lokalnej żadnych urządzeń zewnętrznych, które nie zostały zatwierdzone przez ASI lub w szczególnych jednostkowych przypadkach przez bezpośredniego przełożonego.

12.6 Pracownik ponosi pełną odpowiedzialność za pliki umieszczane w sieci lokalnej. Przesyłanie danych (kopiowanie, przenoszenie) w sieci lokalnej może być monitorowane.

12.7 ASI jest zobowiązany do prowadzenia pełnej dokumentacji związanej z danym zasobem sieciowym lub konfiguracją. Dokumentacja powinna być prowadzona w sposób ułatwiający przeprowadzenie cyklicznego audytu wewnętrznego danego zasobu.

13. ZASADY POSTĘPOWANIA Z URZĄDZENIAMI PRZENOŚNYMI.

Każdy użytkownik elektronicznych urządzeń przenośnych (np. laptop, tablet, smartphone) i nośników wymiennych (np. dyski zewnętrzne, pendrive) jest obowiązany do stosowania się do poniższych zasad:

1) blokada ekranu (pin/hasło/symbol graficzny), szyfrowanie pamięci/karty pamięci, program antywirusowy, wyłączanie nieużywanych usług (wi-fi, gprs/lte, bluetooth, nfc), instalowanie oprogramowania z zaufanego źródła (np. iStore, Google Play), używanie szyfrowania, np.: poczty lub VPN podczas korzystania z publicznych hotspot–ów;
2) urządzeń przenośnych i nośników wymiennych zawierających ważne, wrażliwe lub krytyczne informacje biznesowe, nie należy pozostawiać bez nadzoru, zwłaszcza gdy są pozostawiane np. w samochodach i innych środkach transportu, pokojach hotelowych, centrach konferencyjnych i salach spotkań i tam gdzie jest to możliwe, zaleca się ich fizyczne zamykanie lub odpowiednie zabezpieczenie za pomocą specjalnych zamków zabezpieczających przed kradzieżą,
3) użytkownik wykonując czynności zawodowe lub umowne w domu, powinien zadbać o należyte zabezpieczenie powierzonego sprzętu oraz dostępu do informacji przed nieautoryzowanym dostępem osób trzecich;
4) zabrania się spożywania posiłków i picia podczas pracy z powierzonym sprzętem;
5) zabrania się udostępniania osobom trzecim nośników elektronicznych informacji oraz powierzonego sprzętu będącego własnością Administratora;
6) w przypadku utraty nośnika elektronicznego lub sprzętu komputerowego należy ten fakt bezzwłocznie zgłosić do bezpośredniego przełożonego, IOD lub ASI. Bezpośredni przełożony lub ASI bezzwłocznie zgłaszają taki fakt do IOD, ponieważ zagubienie nośnika przetwarzającego dane może wiązać się z utratą poufności informacji chronionych przez Administratora.

14. TWORZENIE KOPII ZAPASOWYCH.

14.1 Postanowienia ogólne:

1) za tworzenie kopii zapasowych i archiwalnych odpowiedzialny jest ASI;
2) tworzenie kopii odbywa się zgodnie z procedurą tworzenia i odtwarzania kopii zapasowych i podlega rejestracji. Wzór rejestru określa załącznik „Rejestr tworzenia kopii.doc" do dokumentacji przetwarzania danych osobowych. Rejestr prowadzony jest w postaci papierowej lub elektronicznej;
3) po utworzeniu kopii automatycznie (jeżeli jest technicznie realizowalne) jest generowany raport o przebiegu wykonania kopii. Raport podlega weryfikacji przez ASI;
4) miejsce przechowywania kopii jest zabezpieczone przed nieuprawnionym dostępem oraz skutkami zdarzeń takich, jak pożar, zalanie, oddziaływanie silnego pola elektromagnetycznego, promieniowanie, zanieczyszczenie środowiska na takim poziomie, jak jest zabezpieczony system, z którego kopia zapasowa została wykonana;
5) kopie są przechowywane w bezpiecznej odległości (co najmniej w innej strefie pożarowej) od miejsca, w którym jest prowadzona eksploatacja systemów;
6) regularnie, co najmniej raz na kwartał, ASI przeprowadza testowe sprawdzenie odtworzenia systemu, aplikacji, bazy danych lub dokumentów z kopii dla aktualnych systemów produkcyjnych. Testowe odtworzenie podlega udokumentowaniu w dzienniku pracy systemu, jeżeli jest prowadzony;
7) w przypadku, gdy okres trwałości zapisu na nośniku elektronicznym lub magnetycznym jest krótszy od wymaganego okresu przechowywania wynikającego z uwarunkowań prawnych lub biznesowych, dane z nośników są przenoszone na inny nośnik;
8) nośnik, z którego przeniesiono zapis, jest niszczony zgodnie z zasadami obowiązującymi u Administratora;
9) po zakończeniu eksploatacji nośników informacji dane na nich przechowywane powinny zostać z nich usunięte w sposób trwały lub same nośniki powinny zostać zniszczone w sposób trwały. Jest dopuszczalne zlecenia czynności niszczenia nieaktualnych danych oraz wycofanych z eksploatacji nośników informacji wyspecjalizowanym firmom zewnętrznym

14.2 Zasady tworzenia kopii bezpieczeństwa i kopii archiwalnych:

1) zbiory danych, oprogramowanie oraz konfiguracja systemów operacyjnych serwerów Administratora powinny być zabezpieczone w postaci cyklicznie wykonywanych kopii bezpieczeństwa lub archiwalnych.
2) kopie bezpieczeństwa są wykonywane:
   a) przed dokonaniem zmian w konfiguracji systemów operacyjnych lub oprogramowania;
   b) przed dokonaniem zmian w programach (np. zmiana wersji);
   c) przed i/lub po każdej istotnej zmianie danych w bazie danych;
3) oprócz kopii, o których mowa w pkt. 2., są wykonywane kopie archiwalne:
   a) dobowe – raz na dobę
   b) tygodniowe – na koniec danego tygodnia;
   c) miesięczne – na koniec danego miesiąca;
4) pliki użytkowników systemu informatycznego istotne dla działalności firmy są przechowywane na indywidualnie udostępnionych dyskach serwerów.
5) dyski serwerów, o których mowa w pkt. 4 zabezpiecza się przed utratą danych w postaci kopii bezpieczeństwa i/lub archiwalnych.

6) kopie bezpieczeństwa są:
   d) wykonywane w co najmniej jednym egzemplarzu;
   e) przechowywane w innym miejscu niż te, w którym zbiory eksploatowane są na bieżąco (co najmniej w innej strefie pożarowej).
7) kopie archiwalne są:
   f) wykonywane w co najmniej jednym egzemplarzu;
   g) przechowywane w innym miejscu niż te, w którym zbiory eksploatowane są na bieżąco (co najmniej w innej strefie pożarowej).
   h) w trakcie transportu zabezpieczane przed osobami nieupoważnionymi i niekorzystnymi zjawiskami fizycznymi mogącymi doprowadzić do ich zniszczenia bądź uszkodzenia;
8) kopie bezpieczeństwa są przechowywane do momentu wykonania następnej kopii bezpieczeństwa.
9) kopie archiwalne dobowe przechowywane są przez okres 14 dni, tygodniowe są przechowywane przez okres 1 miesiąca, a kopie miesięczne przez okres 13 miesięcy.

15. KORZYSTANIE Z URZĄDZEŃ KOMUNIKACJI. ZARZĄDZANIE WYDRUKAMI.

15.1 Każdy użytkownik zobowiązany jest do przestrzegania zakazu prowadzenia rozmów, podczas których może dochodzić do wymiany informacji danych osobowych lub informacji poufnych Administratora, jeśli rozmowy te odbywają się w miejscach publicznych, otwartych pomieszczeniach biurowych lub takich, które nie gwarantują zachowania poufności rozmów.

15.2 Odczytanie wiadomości z faksów, automatycznych sekretarek lub systemów poczty głosowej powinno być możliwe wyłącznie po wprowadzeniu indywidualnego hasła. W przypadku braku takiej możliwości urządzenia należy zabezpieczyć przed dostępem osób nieuprawnionych.

15.3 Zabronione jest wykorzystywanie domyślnych („fabrycznych") haseł dla ww. urządzeń.

15.4 Przekazywanie za pomocą urządzeń faksowych dokumentów zawierających dane osobowe wrażliwe lub informacje poufne u Administratora jest zabronione.

15.5 Drukarki nie mogą być pozostawione bez kontroli, jeśli są wykorzystywane (lub wkrótce będą) do drukowania dokumentów zawierających dane osobowe.

15.6 Wydruki zawierające dane przechowywane są wyłącznie w odrębnych wyznaczonych szafach,

15.7 Osoba zatrudniona przy przetwarzaniu danych, sporządzająca wydruk zawierający dane ma obowiązek na bieżąco sprawdzać przydatność wydruku w wykonywanej pracy, a w przypadku jego nieprzydatności wydruk zniszczyć,

15.8 Likwidacji wydruków dokonuje się przy użyciu przeznaczonych do tego celu urządzeń (niszczarek) o odpowiedniej klasie DIN, adekwatnej do klasyfikacji niszczonych dokumentów.

16. ZABEZPIECZENIE SYSTEMU - AWARIĄ ZASILANIA.

16.1 Wszystkie krytyczne systemy informatyczne powinny być zasilane z zabezpieczonej, wydzielonej sieci lub zabezpieczone indywidualnie przy pomocy zasilaczy awaryjnych (UPS).

16.2 Minimalny czas podtrzymywania zasilania za pomocą zasilaczy awaryjnych nie może być krótszy niż:

1) 15 minut dla stacji roboczych, przetwarzających dane istotne dla działalności firmy.
2) 45 minut dla serwerów.
3) Dopuszcza się krótsze okresy niż określone w ust. 3., jeśli źródła określone w pkt. 2. posiadają funkcje automatycznego uruchomienia.

17. OCHRONA PRZED SZKODLIWYM OPROGRAMOWANIEM.

17.1 Zidentyfikowanymi obszarami systemu informatycznego Administratora narażonymi na ingerencję wirusów oraz innego szkodliwego oprogramowania są dyski twarde lub karty pamięci urządzeń, pamięć RAM oraz elektroniczne nośniki informacji.

17.2 Drogą przedostania się wirusów lub szkodliwego oprogramowania może być sieć publiczna, wewnętrzna sieć teleinformatyczna lub elektroniczne nośniki informacji.

17.3 Stacje robocze, komputery przenośne oraz serwery są objęte ochroną w czasie rzeczywistym za pomocą oprogramowania antywirusowego oraz zapory (firewall), zapewniających integralność zasobów przechowywanych i przetwarzanych w systemie informatycznym Administratora.

17.4 Za wybór i prawidłowe funkcjonowanie oprogramowania antywirusowego odpowiada ASI.

17.5 Oprogramowanie antywirusowe uruchamiane jest przy starcie systemu, a użytkownik nie posiada uprawnień do jego wyłączenia.

17.6 Konfiguracja programu antywirusowego zapewnia ciągłe monitorowanie otrzymywanych i wysyłanych, a także uruchamianych plików i poczty e-mail pod kątem występowania złośliwego oprogramowania.

17.7 Stacje robocze i komputery przenośne przynajmniej raz w miesiącu skanowane są pod kątem występowania na nich złośliwego oprogramowania.

17.8 Serwery plikowe podlegają skanowaniu pod kątem występowania na nich oprogramowania złośliwego przynajmniej raz w tygodniu.

17.9 Użytkownicy systemu mają obowiązek skanowania każdego zewnętrznego elektronicznego nośnika informacji, z którego chcą skorzystać – umieścić w złączu komputera..

17.10 W przypadku stwierdzenia pojawienia się wirusa i braku możliwości usunięcia go przez program antywirusowy, użytkownik ma obowiązek skontaktować się z ASI.

17.11 W przypadku wystąpienia infekcji i braku możliwości automatycznego usunięcia wirusów przez system antywirusowy, ASI podejmuje działania zmierzające do usunięcia zagrożenia. W szczególności działania te mogą obejmować:

1) usunięcie zainfekowanych plików, o ile jest to akceptowalne ze względu na prawidłowe funkcjonowanie systemu informatycznego;
2) odtworzenie plików z kopii zapasowych, po uprzednim sprawdzeniu, czy dane zapisane na kopiach zapasowych nie są zainfekowane;
3) samodzielną ingerencję w zawartość pliku – w zależności od posiadanych kwalifikacji lub skonsultowanie się z odpowiednim serwisem.
4) odłączenie urządzenia od sieci LAN.

18. ZASADY EKSPLOATACJI, PRZEGLĄDÓW I KONSERWACJI SYSTEMU.

18.1 ASI odpowiada za poprawne działanie sprzętu komputerowego. Czynność tą może wykonywać poprzez pracowników lub współpracowników lub poprzez podmioty zewnętrzne.

18.2 Administrator systemu informatycznego jest zobowiązany do:

1) instalowania wyłącznie licencjonowanego oprogramowanie lub oprogramowania, które nie wymaga opłaty licencyjnej, zgodnie z warunkami licencji
2) prowadzenia spisu posiadanego pod opieką sprzętu komputerowego oraz oprogramowania wraz z dostarczoną dokumentacją,
3) przechowywania kart gwarancyjnych, kluczy i licencji do oprogramowania,
4) prowadzi rejestr wydanego sprzętu komputerowego wraz z wyszczególnieniem użytkownika,
5) udziela pomocy użytkownikowi w obsłudze sprzętu i oprogramowania,

18.3 ASI jest odpowiedzialny za przygotowania sprzętu komputerowego do prawidłowej i zgodnej z przeznaczeniem pracy, oraz przekazania go za potwierdzeniem użytkownikowi, który:

1) jest zobowiązany do dbałości o sprzęt oraz oprogramowanie, a także odpowiedzialny za zabezpieczenie go przed używaniem przez osoby nieuprawnione oraz do ochrony przed kradzieżą lub zagubieniem.

2) nie może samodzielnie zmieniać konfiguracji przekazanego sprzętu komputerowego oraz instalować lub usuwać oprogramowania, w tym nie może używać na przekazanym sprzęcie prywatnego oprogramowania.

18.4 Sprzęt podlega konserwacji według ustalonego planu, wynikającego z zaleceń producentów. Konserwacja sprzętu komputerowego, systemów informatycznych oraz nośników informacji ma na celu zapewnienie nieprzerwanej i bezpiecznej pracy tych systemów, zapobieganie utraty, uszkodzenia lub naruszenia bezpieczeństwa.

18.5 Wszelkie naprawy oraz konserwacje urządzeń komputerowych oraz zmiany w systemie informatycznym przeprowadzane są – o ile to możliwe – przez upoważnionych pracowników Administratora.

18.6 Naprawy, konserwacje i zmiany w systemie informatycznym przeprowadzane przez serwisanta zewnętrznego prowadzone są pod nadzorem ASI w siedzibie Administratora (jeśli to możliwe) lub poza siedzibą Administratora, po uprzednim usunięciu elementów zawierających dane osobowe, o ile nie wiąże się to z nadmiernymi utrudnieniami.

18.7 Wszelkie prace, o których mowa powyżej, wykonywane przez podmiot zewnętrzny, powinny odbywać się na zasadach określonych w szczegółowej umowie pomiędzy Administratorem a tymże podmiotem, z uwzględnieniem klauzuli powierzenia przetwarzania danych lub klauzuli dotyczącej zachowania w poufności przez wykonawcę wszelkich informacji, do których ma dostęp w czasie wykonywania usługi.

18.8 W przypadku zdalnej obsługi serwisowej systemów informatycznych Administratora, porty komunikacyjne mogą być włączane jedynie na wyraźne żądanie dostawcy takich usług, za zgodą ASI i muszą być ponownie odłączone tuż po zakończeniu prac serwisowych co należy odnotować w rejestrze.

18.9 Jeśli nośnik danych (dysk, płyta lub inne) zostanie uszkodzony i nie można go odczytać ani usunąć z niego danych, należy go zniszczyć mechanicznie w niszczarce spełniającej wymagania normy DIN 66399 na poziomie bezpieczeństwa nie niższym niż 3.

19. POSTANOWIENIA KOŃCOWE.

19.1 Każdy użytkownik systemu informatycznego ma obowiązek zapoznania się z treścią niniejszej Procedury,

19.2 Fakt zapoznania się z treścią Procedury oraz zaznajomienia z powszechnie obowiązującymi przepisami o ochronie danych osobowych użytkownik potwierdza stosownym oświadczeniem. Oświadczenie przechowywane jest w aktach osobowych pracownika,

19.3 Naruszenie przez użytkownika niniejszej Procedury może zostać potraktowane przez Administratora, jako naruszenie obowiązków pracowniczych i powodować określoną przepisami Kodeksu pracy odpowiedzialność pracownika,

19.4 W sprawach które nie zostały określone w niniejszym dokumencie lub innych dokumentach czy instrukcjach obowiązuje zasada: wszystko jest zabronione, dopóki nie jest wyraźnie dozwolone,

19.5 Treść niniejszej Procedury ma charakter poufny, chroniony tajemnicą pracodawcy na zasadzie art. 100 § 2 pkt 4 Kodeksu pracy.