DOKUMENTACJA ZBIORÓW DANYCH OSOBOWYCH

§ 1

Definicje

Ilekroć w niniejszej Dokumentacji jest mowa o:

1) Danych osobowych – rozumie się przez to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej zbierane we wszystkich zbiorach danych prowadzonych przez ITS w związku z jej działalnością. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań.
2) Zbiorze danych – rozumie się każdy zbiór danych prowadzonych przez Spółkę w związku z jej działalnością w szczególności związanych z zatrudnieniem, obsługą klientów, organizowanymi akcjami i wszelkie inne zbiory danych prowadzone przez Instytut Transportu Samochodowego
3) System – zbiór aplikacji komputerowych, wykorzystywanych przez ITS do przechowywania i przetwarzania danych osobowych.
4) Przetwarzaniu danych - rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.
5) Administratorze danych - rozumie się przez to Dyrektora ITS
6) Administratorze Zbioru – rozumie się przez to Kierownika (Menedżera, Dyrektora) Działu/Zespołu ITS (zwanego dalej ,,Działem"), który w zakresie określonym niniejszą Dokumentacją wykonuje uprawnienia i obowiązki spoczywające na Administratorze danych, w odniesieniu do Zbiorów prowadzonych przez nadzorowany przez niego Dział.
7) Ustawie - Ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity Dz. U. nr 101/2002 poz. 926 z późn. zm.)
8) Rozporządzeniu – rozumie się przez to Rozporządzenie 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. z dnia 1 maja 2004 r.)
9) Państwie trzecim – rozumie się przez to państwo nienależące do Europejskiego Obszaru Gospodarczego.

§ 2

Zasady przetwarzania danych osobowych

1. Przetwarzanie danych jest dopuszczalne tylko wtedy, gdy:
   1.1. osoba, której dane dotyczą, wyrazi na to zgodę, chyba że chodzi o usunięcie dotyczących jej danych,
   1.2. jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa,
   1.3. jest to konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą,
   1.4. jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego,
   1.5. jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez Administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą. (art. 23 Ustawy).
2. Zgoda, o której mowa w ust. 1 pkt 1.1, może obejmować również przetwarzanie danych w przyszłości, jeżeli nie zmienia się cel przetwarzania.
3. Jeżeli przetwarzanie danych jest niezbędne dla ochrony żywotnych interesów osoby, której dane dotyczą, a spełnienie warunku określonego w ust. 1 pkt 1.1 jest niemożliwe, można przetwarzać dane bez zgody tej osoby, do czasu, gdy uzyskanie zgody będzie możliwe.
4. W przypadku zbierania danych osobowych od osoby, której one dotyczą, Administrator danych jest obowiązany poinformować tę osobę o:
   - adresie swojej siedziby i pełnej nazwie,
   - celu zbierania danych, a w szczególności o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych,
   - prawie dostępu do treści swoich danych oraz ich poprawiania,
   - dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej. chyba że osoba, której dane dotyczą posiada powyższe informacje (art. 24 Ustawy).
5. W przypadku zbierania danych osobowych nie od osoby, której one dotyczą, Administrator danych jest obowiązany poinformować tę osobę, bezpośrednio po utrwaleniu zebranych danych, o:
   - adresie swojej siedziby i pełnej nazwie,
   - celu i zakresie zbierania danych, a w szczególności o odbiorcach lub kategoriach odbiorców danych,
   - źródle danych,
   - prawie dostępu do treści swoich danych oraz ich poprawiania,
   - uprawnieniach wynikających z art. 3 2 u st. 1 pkt 7 i 8 U stawy t j. wniesienia pisemnie umotywowanego żądania zaprzestania przetwarzania jej danych ze względu na jej szczególną

sytuację oraz prawie do wniesienia sprzeciwu w sytuacjach, o których mowa w pkt. 1.4 i 1.5; chyba że osoba, której dane dotyczą, posiada informacje, o których mowa powyżej, bądź zachodzą inne okoliczności określone w art. 25 ust 2 Ustawy.

6. Administrator danych przetwarzający dane powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest obowiązany zapewnić, aby dane te były:
   6.1. przetwarzane zgodnie z prawem,
   6.2. zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu niezgodnemu z tymi celami, z zastrzeżeniem pkt 7,
   6.3. merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane,
   6.4. przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania. (art. 26)
7. Zabrania się przetwarzania danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym (,,Dane wrażliwe") za wyjątkiem gdy:
   - osoba, której dane dotyczą, wyrazi na to zgodę na piśmie, chyba że chodzi o usunięcie dotyczących jej danych,
   - przetwarzanie jest niezbędne do wykonania zadań Administratora odnoszących się do zatrudnienia pracowników i innych osób, a zakres przetwarzanych danych jest określony w ustawie,
   - dane te zostały podane do publicznej wiadomości przez osobę której dotyczą, oraz w innych sytuacjach dopuszczonych przez art. 27 ust 2 Ustawy.
8. W przypadku udostępniania danych osobowych w celach innych niż włączenie do zbioru, Administrator danych udostępnia posiadane w zbiorze dane osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.
9. Dane osobowe, z wyłączeniem Danych wrażliwych, mogą być także udostępnione w celach innych niż włączenie do zbioru, innym osobom i podmiotom niż wymienione w pkt.8, jeżeli w sposób wiarygodny uzasadnią potrzebę posiadania tych danych, a ich udostępnienie nie naruszy praw i wolności osób, których dane dotyczą.
10. Dane osobowe udostępnia się na pisemny, umotywowany wniosek, chyba że przepis innej ustawy stanowi inaczej. Wniosek powinien zawierać informacje umożliwiające wyszukanie w zbiorze żądanych danych osobowych oraz wskazywać ich zakres i przeznaczenie. (art. 29 Ustawy).
11. Udostępnione dane osobowe można wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.

12. Administrator danych odmawia udostępnienia danych osobowych ze zbioru danych podmiotom i osobom innym niż wymienione w pkt 8, jeżeli spowodowałoby to istotne naruszenie dóbr osobistych osób, których dane dotyczą, lub innych osób, oraz w innych przypadkach, o których mowa w art. 30 Ustawy.
13. Administrator Zbioru zapewnia przetwarzanie danych osobowych zgodnie z postanowieniami § 2.

§ 3

Prawa osoby, której dane dotyczą

1. Każdej osobie przysługuje prawo do kontroli przetwarzania danych, które jej dotyczą, zawartych w zbiorach danych, a zwłaszcza prawo do:
   1.1. uzyskania wyczerpującej informacji, czy taki zbiór istnieje, oraz do ustalenia Administratora danych, adresu jego siedziby i pełnej nazwy,
   1.2. uzyskania informacji o celu, zakresie i sposobie przetwarzania danych zawartych w takim zbiorze,
   1.3. uzyskania informacji, od kiedy przetwarza się w zbiorze dane jej dotyczące, oraz podania w powszechnie zrozumiałej formie treści tych danych,
   1.4. uzyskania informacji o źródle, z którego pochodzą dane jej dotyczące, chyba że Administrator danych jest zobowiązany do zachowania w tym zakresie tajemnicy państwowej, służbowej lub zawodowej,
   1.5. uzyskania informacji o sposobie udostępniania danych, a w szczególności informacji o odbiorcach lub kategoriach odbiorców, którym dane te są udostępniane,
   1.6. żądania uzupełnienia, uaktualnienia, sprostowania danych osobowych, czasowego lub stałego wstrzymania ich przetwarzania lub ich usunięcia, jeżeli są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są już zbędne do realizacji celu, dla którego zostały zebrane,
   1.7. wniesienia, w przypadkach wymienionych w § 1 ust. 1 pkt 1.4 i 1.5 Ustawy, pisemnego, umotywowanego żądania zaprzestania przetwarzania jej danych ze względu na jej szczególną sytuację. W tej sytuacji Administrator danych zaprzestaje przetwarzania kwestionowanych danych osobowych albo bez zbędnej zwłoki przekazuje żądanie Generalnemu Inspektorowi, który wydaje stosowną decyzję.
   1.8. wniesienia sprzeciwu wobec przetwarzania jej danych w przypadkach, wymienionych w pkt 1.7 Ustawy, gdy administrator danych zamierza je przetwarzać w celach marketingowych lub wobec przekazywania jej danych osobowych innemu administratorowi danych, W razie wniesienia sprzeciwu, dalsze przetwarzanie kwestionowanych danych jest niedopuszczalne. Administrator danych może jednak pozostawić w zbiorze imię lub imiona i nazwisko osoby oraz numer PESEL lub adres wyłącznie w celu uniknięcia ponownego wykorzystania danych tej osoby w celach objętych sprzeciwem. (art. 32 Ustawy).

2. Osoba zainteresowana może skorzystać z prawa do informacji, o których mowa w ust. 1 pkt 1.1-1.5, nie częściej niż raz na 6 miesięcy.
3. W razie wykazania przez osobę, której dane osobowe dotyczą, że są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są zbędne do realizacji celu, dla którego zostały zebrane, Administrator danych jest obowiązany, bez zbędnej zwłoki, do uzupełnienia, uaktualnienia, sprostowania danych, czasowego lub stałego wstrzymania przetwarzania kwestionowanych danych lub ich usunięcia ze zbioru, chyba że dotyczy to danych osobowych, w odniesieniu do których tryb ich uzupełnienia, uaktualnienia lub sprostowania określają odrębne ustawy. Administrator danych jest obowiązany poinformować bez zbędnej zwłoki innych administratorów, którym udostępnił zbiór danych, o dokonanym uaktualnieniu lub sprostowaniu danych.
4. Administrator Zbioru zapewnia przetwarzanie danych osobowych zgodnie z postanowieniami § 3.

§ 4

Zabezpieczenie danych osobowych

1. Administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.
2. Administrator danych prowadzi dokumentację opisującą sposób przetwarzania danych oraz środki, o których mowa w ust. 1 . tj. Politykę Bezpieczeństwa o raz Instrukcję Zarządzania Systemem Informatycznym, stanowiące część niniejszej Dokumentacji.
3. Oryginały upoważnień i innych dokumentów sporządzonych w wykonaniu niniejszej Dokumentacji, powinny być przekazywane do działu wewnętrznej obsługi prawnej, a ich kopie przechowywane przez Administratora Zbioru.
4. Informacja o utworzeniu nowego zbioru danych osobowych lub zmianie w dotychczasowym powinna być przekazana przez Administratora Zbioru lub wskazaną przez niego osobę do menedżera działu informatycznego celem uzupełnienia danych w Załączniku nr 1 do Dokumentacji.

§ 5

Przekazywanie danych osobowych do państwa trzeciego

1. Przekazanie danych osobowych do państwa trzeciego może nastąpić, jeżeli państwo docelowe daje gwarancje ochrony danych osobowych na swoim terytorium przynajmniej takie, jakie obowiązują na terytorium Rzeczypospolitej Polskiej.
2. Administrator danych może jednak przekazać dane osobowe do państwa trzeciego, jeżeli:

- osoba, której dane dotyczą, udzieliła na to zgody na piśmie,
- przekazanie jest niezbędne do wykonania umowy pomiędzy administratorem danych a osobą, której dane dotyczą, lub jest podejmowane na jej życzenie,
- przekazanie jest niezbędne do wykonania umowy zawartej w interesie osoby, której dane dotyczą, pomiędzy administratorem danych a innym podmiotem,
- przekazanie jest niezbędne ze względu na dobro publiczne lub do wykazania zasadności roszczeń prawnych,
- przekazanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą,
- dane są ogólnie dostępne (art. 47 Ustawy).

3. W przypadkach, o których mowa w ust. 2 przekazanie danych osobowych do państwa trzeciego, które nie daje gwarancji ochrony danych osobowych przynajmniej takich, jakie obowiązują na terytorium Rzeczypospolitej Polskiej, może nastąpić po uzyskaniu zgody Generalnego Inspektora Danych Osobowych, pod warunkiem że Administrator danych zapewni odpowiednie zabezpieczenia w zakresie ochrony prywatności oraz praw i wolności osoby, której dane dotyczą. (art. 48 Ustawy).
4. Administrator Zbioru zapewnia przekazywanie danych do państwa trzeciego zgodnie z § 5.

POLITYKA BEZPIECZEŃSTWA

Ilekroć w niniejszej Polityce bezpieczeństwa jest mowa o:

1. Rozliczalności - rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
2. Integralności danych - rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;

3. Raporcie - rozumie się przez to przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych;
4. Poufności danych - rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;
5. Uwierzytelnianiu - rozumie się przez to działanie, którego celem jest weryfikacja

I. Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe.

Obszar w którym są przetwarzane dane osobowe obejmuje budynek przy ulicy Jagiellońskiej 80 w Warszawie („Budynek"). W ramach tego Budynku północne skrzydło zajmowane jest przez Instytut Transportu Samochodowego.

II. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych

Zbiorami danych są zbiory wymienione w załącznikach do niniejszej Dokumentacji, umieszczone w sieci komputerowej ITS. Programami służącymi do przetwarzania Zbiorów danych są programy wymienione w załącznikach do niniejszej Dokumentacji.

III. Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi.

Opisy struktur zbiorów danych w odniesieniu do poszczególnych zbiorów danych, oraz relacje pomiędzy poszczególnymi tablicami w Systemie określone zostały w załącznikach do niniejszej Dokumentacji.

IV. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

1. Osoby nie zatrudnione w ITS, a tym samym nie posiadające elektronicznych kart identyfikacyjnych, mogą dostać się wyłącznie na parter, na którym znajduje się recepcja. Dostęp do Budynku jest zabezpieczony poprzez całodobową ochronę. Uprawnieni do wejścia na teren biura są wyłącznie pracownicy spółek ITS („pracownicy ITS") posiadający identyfikujące karty dostępu.

2. Przebywanie osób nieuprawnionych na terenie biura przez osoby inne niż pracownicy ITS jest dopuszczalne wyłącznie w obecności pracownika ITS. Każdy pracownik ITS jest odpowiedzialny za dokładne zamykanie na klucz pomieszczeń Działu a w momencie opuszczania pomieszczenia, jako ostatni sprawdza i zamyka drzwi i okna.
3. Budynki i pomieszczenia zabezpieczane są przez pracowników ochrony, do których obowiązków należy:
   3.1. nie dopuszczanie do wchodzenia do Budynku bez ważnej karty wstępu,
   3.2. nie wpuszczanie na teren Budynku osób nie będących pracownikami ITS, domokrążców i akwizytorów, a gości na zasadach określonych w pkt.4
   3.3. ewidencjonowania w odpowiednich książkach faktu przebywania w Budynku pracowników ITS w dniach wolnych od pracy,
   3.4. systematyczne patrolowanie całego Budynku z zewnątrz i wewnątrz zarówno w dzień jak i w nocy, pod kątem zabezpieczenia obiektu i poszczególnych jego pomieszczeń,
   3.5. sprawdzanie z zewnątrz, czy wszystkie okna są zamknięte, a światła w pomieszczeniach zgaszone oraz czy zamki elektroniczne nie są uszkodzone,
   3.6. natychmiastowe reagowanie na sygnał o naruszeniu systemu przeciwpożarowego, czujek ruchu oraz przechowywanie kluczy do wyjść ewakuacyjnych.
4. Zasady przyjmowania gości.
   4.1. każda przychodząca osoba, nie będąca pracownikiem ITS jest obowiązana zgłosić się i zarejestrować w recepcji,
   4.2. recepcjonista jest obowiązany wpisać imię i nazwisko do książki wejść; w książce odnotowane są również godziny przebywania gościa w pomieszczeniach ITS,
   4.3. *Gość* otrzymuje identyfikator, który zobowiązany jest zwrócić przy wyjściu,
   4.4. *Gościem* powinna zaopiekować się osoba goszcząca, czyli pracownik ITS, do którego przyszedł *gość*. Osoba ta odpowiada za zachowanie swojego *gościa*,
   4.5. *Gość* nie może poruszać się po budynku ITS bez opieki pracownika ITS,
5. Regulacje dotyczące komputerów i systemu informatycznego, na których przetwarzane są Dane osobowe.
   5.1. Komputery przenośne wykorzystywane do przetwarzania danych osobowych są mocowane za pomocą linek zabezpieczających bądź po zamknięciu zamykane w specjalnych szafach. Osoba użytkująca komputer przenośny zawierający dane osobowe zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania, w tym stosuje środki ochrony kryptograficznej wobec przetwarzanych Danych osobowych.
   5.2. Pracownik mający dostęp do komputera zawierającego Dane osobowe nie może zezwalać na używanie komputera osobom nieupoważnionym do dostępu do Danych osobowych.
   5.3. Komputer przenośny nie może być pozostawiony w ogólne dostępnych miejscach.

5.4. Dostęp do kluczowych dla funkcjonowania firmy systemów informatycznych (serwery, systemy łączności) jest ściśle ograniczony i możliwy jedynie dla wąskiej grupy pracowników działu informatycznego.

5.5. Komputery wyposażone są w wygaszacze ekranu, które uaktywniają się automatycznie po kilku minutach bezczynności komputera, zabezpieczając tym samym przed przypadkowym dostępem do przetwarzanych danych przez osoby do tego nieupoważnione. Wyłączanie wygaszacza wymaga podania hasła znanego jedynie osobie, która rozpoczęła przetwarzanie danych.

6. Szczegółowe zasady dostępu do obszaru, w którym przetwarzane są dane osobowe.

Wszystkie dane przechowywane są w sposób, który umożliwia dostęp i przetwarzanie jedynie użytkownikom do tego upoważnionym. Funkcjonalność taką zapewniają mechanizmy autentykacji i autoryzacji wbudowane w wykorzystywane w ITS systemy operacyjne i aplikacje. Chroni to zarówno prywatność pracowników jak również blokuje próby nieautoryzowanego dostępu do danych. Szczegółowe zasady przyznawania uprawnień oraz uwierzytelniania użytkowników określa Instrukcja Zarządzania Systemem Informatycznym.

Wszyscy nowi pracownicy przechodzą cykl szkoleń obejmujących m.in. zagadnienia związane z bezpieczeństwem systemów informatycznych. Ponadto nowi pracownicy upoważnieni do przetwarzania Danych osobowych poświadczają pisemnie zapoznanie się z niniejszą Dokumentacją w tym zasadami korzystania z Systemu. Każdy z pracowników zobowiązany jest do zachowania tajemnicy Danych osobowych, z którymi zapoznał się w trakcie ich przetwarzania oraz zachowania tajemnicy służbowej, na mocy umowy o pracę, Regulaminu pracy oraz Zasad postępowania obowiązujących w firmie, co potwierdzają podpisując zobowiązania rozpoczynając pracę w ITS.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

Ilekroć w niniejszej Instrukcji jest mowa o:

1) Identyfikatorze użytkownika - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
2) Haśle - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;

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

1. Do przetwarzania danych w danym zbiorze mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez osobę Administratora Zbioru.
2. Administrator Zbioru jest obowiązany zapewnić kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane.
3. Administrator Zbioru prowadzi ewidencję osób upoważnionych do ich przetwarzania, która zawiera:
   - imię i nazwisko osoby upoważnionej,
   - datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych,
   - identyfikator.
4. Osoby, które zostały upoważnione do przetwarzania danych, są obowiązane zachować w tajemnicy te dane osobowe oraz sposoby ich zabezpieczenia.
5. W Systemie służącym do przetwarzania danych osobowych stosuje się następujące mechanizmy kontroli dostępu do tych danych:
   - w Systemie rejestrowany jest dla każdego użytkownika odrębny identyfikator, dostęp do zbioru danych odbywa się po wprowadzeniu hasła, zasady przydzielania hasła oraz zarządzania dostępem do zbioru danych określa pkt II;
   - dostęp do danych jest możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia,
6. Dla każdej osoby, której dane osobowe są przetwarzane w Systemie System ten zapewnia odnotowanie:
   - daty pierwszego wprowadzenia danych do Systemu;
   - identyfikatora użytkownika wprowadzającego dane osobowe do Systemu, chyba że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba;
   - źródła danych, w przypadku zbierania danych, nie od osoby, której one dotyczą,
   - informacji o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia, chyba że system informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych;
   - sprzeciwu, o którym mowa w art. 32 ust. 1 pkt 8 Ustawy.
7. Odnotowanie informacji, o których mowa w pkt 6 , następuje równocześnie z zatwierdzeniem przez użytkownika operacji wprowadzenia danych.
8. Dla każdej osoby, której dane osobowe są przetwarzane w Systemie, System zapewnia sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w pkt 6.

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

1. W ITS zastosowany został system informatyczny oparty o usługi katalogowe Active Direktory systemu Microsoft Windows Server. Z uwagi na różnorodność potrzeb i zastosowań w skład systemu wchodzą autorskie i komercyjne programy użytkowe, które są opisane w poszczególnych załącznikach do tej instrukcji. Zgodnie z rozporządzeniem MSWIA z dnia 29 kwietnia 2004r. w ich implementacjach zostały zastosowane adekwatne środki techniczne i organizacyjne dla zapewnienia niejawności, integralności i rozliczalności przetwarzanych danych.
2. Założenie konta i przyznanie uprawnień dostępu do Systemu i/lub danych realizowane są przez pracowników działu informatycznego na podstawie dyspozycji Administratora Zbioru bądź innych osób upoważnionych przez Administratora.
3. Rejestracja nowego użytkownika następuje za zgodą Administratora Zbioru w odniesieniu do danego zbioru, na podstawie pisemnej lub przekazanej drogą elektroniczną (e-mail) dyspozycji Administratora Zbioru lub osoby przez niego upoważnionej dotyczącej rejestracji, zmian uprawnień lub wyrejestrowania nowego użytkownika z Systemu. Dyspozycja powyższa jest realizowana przez osoby zarządzające od strony technicznej danym systemem informatycznym.
4. Odrębny identyfikator i hasło jest ustalane dla każdego użytkownika Systemu. Identyfikator użytkownika składa się z dwóch członów rozdzielanych znakiem „@”. pierwszym człon jest postaci *imie.nazwisko*, a drugi to stały tekst *its.local*. W przypadku dwóch użytkowników o tym samym nazwisko stosuje się dodatkowo pierwszą literę drugiego imienia.
5. Administrator Zbioru wpisuje identyfikator do prowadzonej ewidencji osób zatrudnionych przy ich przetwarzaniu wraz z imieniem i nazwiskiem użytkownika oraz rejestruje go w Systemie.
6. Identyfikator użytkownika nie powinien być zmieniany, a po jego wyrejestrowaniu z Systemu nie powinien być przydzielany innej osobie;
7. Raz przydzielone hasło nie może być wykorzystywane powtórnie przez użytkownika przez kolejnych 10 haseł. Zmiana hasła następuje nie rzadziej niż co 30 dni.
8. Dostęp do danych jest możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia oraz wprowadzeniu hasła.
9. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie. Identyfikator osoby, która utraciła uprawnienia do dostępu do danych osobowych, należy niezwłocznie wyrejestrować z Systemu, w którym są one przetwarzane, unieważnić jej hasło oraz podjąć inne stosowne działania w celu zapobieżenia dalszemu dostępowi tej osoby do danych.
10. Hasło użytkownika, umożliwiające dostęp do Systemu, utrzymuje się w tajemnicy, również po upływie jego ważności. Nie należy go zapisywać ani przechowywać w miejscu oraz formie dostępnej dla osób niepowołanych.

11. Pierwsze hasło jest przydzielane losowo przez System lub przydzielane przez osoby zarządzające od strony technicznej danym systemem informatycznym. Po zalogowaniu, użytkownik ma obowiązek zmiany hasła z zachowaniem zasad tworzenia haseł.
12. Zasady tworzenia haseł:
    12.1. Hasło musi składać się z co najmniej 8 znaków.
    12.2. Hasło nie może składać się tylko z liczb lub liter.
    12.3. Hasło powinno stanowić mieszankę liter, liczb i innych znaków, wykorzystywać różne wielkości znaków.
    12.4. Nie można wykorzystywać słów, które można znaleźć w słowniku, nawet jeśli pisane są odwrotnie.
    12.5. W żadnej formie nie można wykorzystywać identyfikatora jako hasła (zmieniona wielkość znaków, zapis odwrotny, podwojone litery).
    12.6. W żadnej formie nie można używać imion ani nazwisk.
    12.7. Hasła nie mogą łatwo kojarzyć się z jego właścicielem, np. imię kogoś z rodziny, zwierzaka, nazwa hobby, nr rejestracji samochodu, nr telefonu, nr ubezpieczenia, marka samochodu, nazwa ulicy zamieszkania itp.
    12.8. Nie można stosować sekwencji, które znajdują się bezpośrednio na klawiaturze np. Asdfghjki oraz powtórek złożonych z identyfikatora, tzn. Identyfikator: ann, hasło: annann.

III. Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu.

1. Uruchomienia Systemu i rozpoczęcia przetwarzania danych osobowych może dokonać jedynie osoba, której nadane zostały wymagane do tego uprawnienia.
2. Do uruchomienia komputerów jak i Systemu konieczna jest znajomość co najmniej jednego a w przypadku niektórych zbiorów danych dwóch haseł dostępu, które ustalane są z zachowaniem zasad określonych w pkt. I i II niniejszej Instrukcji.
3. Użytkownik powinien wyrejestrować się z Systemu przed wyłączeniem komputera.
4. Wszelkie uwagi dotyczące funkcjonowania Systemu a w tym i podejrzenia naruszania bezpieczeństwa czy stwierdzenia fizycznej ingerencji w przetwarzane dane, użytkowane narzędzie programowe lub sprzętowe są na bieżąco i w sposób bezpośredni komunikowane osobie zarządzającej od strony technicznej danym systemem informatycznym oraz Administratorowi Zbioru.

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

13. Dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych. Kopie są wykonywane na dysku sieciowym wydzielonego serwera, a następnie zgrywane na taśmę magnetyczną. Operacja kopiowania danych odbywa się w codziennie cyklu tygodniowym, przy czym kopie na koniec każdego tygodnia, miesiąca i roku są składowane osobno. System ten pozwala na odzyskanie danych z każdego dnia bieżącego tygodnia, końca tygodnia bieżącego miesiąca, końca każdego miesiąca do roku wstecz od aktualnej daty.
14. Kopie zapasowe:
    14.1. przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem;
    14.2. usuwa się niezwłocznie po ustaniu ich użyteczności.
15. Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:
    15.1. likwidacji - pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;
    15.2. przekazania podmiotowi nieuprawnionemu do przetwarzania danych – pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie.
    15.3. naprawy - pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.

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

Kopie zapasowe przechowywane są przez okres minimum jednego tygodnia w pomieszczeniu, do którego dostęp mają jedynie pracownicy działu informatycznego ITS.

VI. Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego.

1. System informatyczny służący do przetwarzania danych osobowych zabezpiecza się, w szczególności przed:

działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego,

utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.

2. Aby zmniejszyć ryzyko infekcji wirusami komputerowymi zabronione jest instalowanie na komputerach mających styczność z Systemem jakiegokolwiek oprogramowania nie zaaprobowanego przez dział informatyczny ITS.
3. Ochrona przed wirusami polega na stosowaniu efektywnego oprogramowania antywirusowego.
   3.1. wszystkie komputery na których przetwarzane są dane muszą być wyposażone w oprogramowanie antywirusowe;
   3.2. oprogramowanie antywirusowe jest aktualizowane na bieżąco w miarę pojawiania się nowych wersji programu lub jego uzupełnień;
   3.3. zapewniona jest możliwość codziennej aktualizacji oprogramowania za pomocą skryptów startowych, każdorazowo w trakcie logowania się do sieci komputerowej.
4. Oprogramowanie powinno być tak skonfigurowane, aby kontrola obecności wirusów odbywała się każdorazowo podczas otwierania zagrożonych plików danych.
5. Niezależnie od konfiguracji pozwalającej na stałe monitorowanie obecności wirusów każdy z komputerów wykorzystywanych do komunikacji z Systemem musi być sprawdzany przez przeglądanie wszystkich plików aktualnym programem antywirusowym, co najmniej raz w miesiącu.
6. Zewnętrzne łącza danych wykorzystywane w ITS są oddzielone od wewnętrznej sieci korporacyjnej przy pomocy urządzeń typu firewall, chroniących przed nieautoryzowanym dostępem do zasobów informatycznych firmy.
7. Wszystkie istotne elementy systemu informatycznego (serwery, urządzenia sieciowe itp.) są zasilane przy pomocy systemów UPS, zapewniających ciągłość pracy także w przypadku przerwy w dostawie energii elektrycznej.

VII. Sposób realizacji wymogu odnotowania informacji o odbiorcach którym dane osobowe zostały udostępnione.

Wraz z poszczególnymi zbiorami danych osobowych przechowywane są również informacje o osobach, którym dane zostały udostępnione, łącznie z informacją o dacie i zakresie udostępnienia.

VIII. Ochrona przed zagrożeniami sieciowymi

1. Ochrona przed atakami sieciowymi

W celu zmniejszenia podatności na atak DDoS, ataki spoza wewnętrznej sieci ITS oraz zminimalizowanie skutków tych ataków wdrożone zostały następujące metody przeciwdziałania:

- analiza i segregacja ruchu sieciowego pod kątem blokowania lub odrzucania niepożądanego ruchu w oparciu o zadane reguły
- zastosowanie list kontroli dostępu (ACL) na urządzeniach sieciowych, blokujących niepożądanych dostęp na poziomie warstwy 2 i 3
- dynamiczne blokowanie dostępu do usług serwerowych w reakcji na nieautoryzowane próby dostępu na poziomie warstwy 7
- monitoring ruchu z urządzeń sieciowych na dedykowanym urządzeniu, umożliwiającym podgląd obciążenia sieci lokalnej, informowanie o anomaliach i wskazywanie elementów generujących największe obciążenie

2. Przegląd urządzeń

Okresowo, nie rzadziej niż co 30 dni dokonywany jest przegląd kluczowych urządzeń sieciowych, w szczególności przełączników, routerów i serwerów świadczących usługi sieciowe. Podczas przeglądu dokonuje się czynności mające na celu:

- sprawdzenie poprawności działania
- aktualizację zasad zmniejszających podatności na ataki
- weryfikację konfiguracji pod kątem wydajności i bezpieczeństwa
- zlokalizowanie elementów ograniczających transmisję
- weryfikację reguł kontroli ruchu

3. Eliminacja ruchu anonimizowanego

Eliminacja ruchu anonimizowanego do stron WWW opiera się na blokowaniu wejść z adresów IP, oznaczonych jako bramki wyjściowe TOR. Ruch jest kierowany na statyczną stronę informującą o blokadzie ruchu TOR. Lista adresów bramek jest aktualizowana co 10 minut.

4. Aktualizacje

Aktualizacja oprogramowania antywirusowego na stacjach roboczych jest dokonywana manualnie przez administratora poprzez udostępnienie nowszej wersji oprogramowania i zdalne zainicjowanie upgrade'u stacji roboczych z poziomu konsoli zarządzającej systemu antywirusowego. Aktualizacja definicji jest dokonywana na bieżąco przez wszystkie stacje robocze. Definicje sygnatur wirusów są pobierane na bieżąco przez serwer systemu antywirusowy i udostępniane w postaci paczki, pobieranej automatycznie przez oprogramowanie klienckie na stacjach roboczych.

Aktualizacja systemów operacyjnych stacji klienckich odbywa się w trybie automatycznym poprzez usługę Microsoft Update.
Aktualizacja systemów operacyjnych serwerów jest dokonywana podczas miesięcznych przeglądów, z wyłączeniem sytuacji po opublikowaniu krytycznych poprawek bezpieczeństwa, instalowanych bezzwłocznie po otrzymaniu informacji o publikacji.
Aktualizacja oprogramowania firmware przełączników sieciowych odbywa się podczas okresowych przeglądów.

IX. Incydenty

Incydentem jest każde zdarzenie mające wpływ istotny na działanie infrastruktury, urządzeń oraz sieci informatycznej Instytutu. Skutkiem incydentu może być:

- ograniczenie w znacznym zakresie możliwości funkcjonowania Instytutu
- utrata dostępu lub zagrożenie spójności danych
- utrata w znacznym zakresie ciągłości działania infrastruktury informatycznej

X. Procedura reagowania na incydenty

1. Powiadomienie

Każdorazowo o wystąpieniu incydentu powiadamiany jest przełożony SI. Przy zaistnieniu incydentów o stopniu wysokim lub krytycznym i pochodzących spoza Instytutu, oraz przy braku możliwości usunięcia zewnętrznych przyczyn lub niemożności zlokalizowania źródła zagrożenia powiadamiany jest zespół CERT. Powiadomienie wysyła osoba wyznaczona do kontaktów z CERT.

2. Podjęcie działań

W przypadku wystąpienia incydentu podejmowane są następujące działania:

1. likwidacja aktywnej przyczyny incydentu, jeżeli jest możliwa
2. powiadomienie przełożonego SI o wystąpieniu incydentu
3. przywrócenie poprawnego działania elementów infrastruktury objętych skutkami incydentu
4. zapis w dzienniku incydentów
5. powiadomienie zespołu CERT w przypadku incydentu o stopniu wysokim lub krytycznym oraz źródle zlokalizowanym poza Instytutem

Zmiana stron WWW na skutek ataku na serwer jest odnotowywana w dzienniku incydentów ze obligatoryjnym wysokim stopniem zagrożenia. Natychmiastowo po wystąpieniu incydentu podejmowane są następujące działania:

1. zmiana haseł dostępowych do zasobów dyskowych i baz danych
2. zmiana strony na statyczną informację o przerwie w działaniu

3. analiza incydentu i zabezpieczenie przed powtórnym atakiem, jeżeli jest możliwe
4. odtworzenie zmienionych lub zniszczonych skryptów stron WWW z kopii zapasowej
5. odtworzenie z kopii zapasowej zmienionych lub zniszczonych baz danych zasilających systemy CMS oraz udostępniających dane użytkownikom
6. przełączenie z powrotem na dynamiczną zawartość strony

3. Dziennik incydentów

Każdy incydent wymagający podjęcia działań zapisywany jest w dzienniku incydentów. Wpis zawiera:

- datę i godzinę wystąpienia incydentu
- stopień zagrożenia: niski, wysoki, krytyczny
- urządzenia i zasoby których dotyczył incydent
- opis podjętych działań w celu wyeliminowania zagrożenia i przywrócenia poprawnego działania infrastruktury oraz ruchu sieciowego
- oszacowanie skutków incydentu

Opracował *(imię i nazwisko, podpis, data)*	**Sprawdził** *(imię i nazwisko, podpis, data)*	**Zatwierdził** *(imię i nazwisko, podpis, data)*
15-04-2015 r. *Michał Kułach*	*15-04-2015 r.* *mgr inż. Tomasz Maślanka*	*15-04-2015 r.* *dr hab. inż. Marcin Ślęzak*
	Kierownik SI	Dyrektor ITS