POLITYKA
OCHRONY DANYCH OSOBOWYCH
W SYSTEMACH INFORMATYCZNYCH
SŁUŻĄCYCH DO PRZETWARZANIA
DANYCH OSOBOWYCH W ITONA
SP. Z O.O. Z SIEDZIBĄ W LUBLINIE

SPIS TREŚCI

WSTĘP

Wdrożenie niniejszej „Polityki ochrony danych osobowych w systemach informatycznych służących do przetwarzania danych osobowych w ITONA sp. z o.o. w Lublinie", zwanej dalej Polityką, ma na celu zabezpieczenie danych osobowych przetwarzanych w systemach informatycznych.

Polityka jest dokumentem eksploatacyjnym, regulującym zasady oraz procedury zarządzania i administrowania systemami informatycznymi służącymi do przetwarzania danych osobowych w ITONA sp. z o.o. w Lublinie. Pozostałe dokumenty dotyczące ochrony danych osobowych obowiązujące w ITONA sp. z o.o. w Lublinie oraz instrukcje zarządzania systemami informatycznymi powinny być zgodne z niniejszym dokumentem.

ROZDZIAŁ I. POSTANOWIENIA OGÓLNE.

1. Cel wydania dokumentu.
   1) Celem wydania dokumentu jest realizacja postanowień art. 24 ust. 1 i ust. 2 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) (Dz. Urz. UE L 119 z 04.05.2016 r., str. 47), zwanego dalej Rozporządzeniem;
   2) opracowanie i wdrożenie niniejszego dokumentu ma na celu podniesienie standardów przetwarzania danych osobowych w systemach informatycznych w ITONA sp. z o.o. w Lublinie.
2. Streszczenie dokumentu.

   Niniejsza Polityka określa:
   1) procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień oraz wskazanie osoby odpowiedzialnej za te czynności;
   2) stosowane metody i środki uwierzytelnienia w systemie oraz procedury związane z ich zarządzaniem i użytkowaniem;
   3) procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemie przeznaczone dla użytkowników systemu;
   4) procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania;
   5) sposób, miejsce i okres przechowywania:
      a) elektronicznych nośników informacji zawierających dane osobowe,
      b) kopii zapasowych;
   6) sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu;

7) procedury wykonywania przeglądów i konserwacji systemów oraz elektronicznych nośników informacji służących do przetwarzania danych osobowych.

3. Zakres stosowania dokumentu.
   1) Niniejszy dokument dotyczy danych osobowych przetwarzanych w systemach informatycznych;
   2) wszyscy pracownicy ITONA sp. z o.o. w Lublinie przetwarzający dane osobowe w systemach informatycznych powinni stosownie do swoich obowiązków służbowych zapoznać się z Polityką i przestrzegać regulacji oraz zasad określonych w niniejszym dokumencie. Powyższemu obowiązkowi podlegają również stażyści, aplikanci, praktykanci przetwarzający dane osobowe w systemach informatycznych.
4. Definicje pojęć.

   W niniejszej Polityce stosuje się terminologię opisaną w „Słowniku pojęć z zakresu ochrony danych osobowych" stanowiącym załącznik nr 1 do „Polityki Ochrony Danych Osobowych w ITONA sp. z o.o. w Lublinie".
5. Przeglądy „Polityki ochrony danych osobowych w systemach informatycznych służących do przetwarzania danych osobowych w ITONA sp. z o.o. w Lublinie".

   Wszelkie propozycje zmian Polityki należy zgłaszać Inspektorowi Ochrony Danych (IOD). IOD w porozumieniu z Osobą zarządzająca sprzętem komputerowym i oprogramowaniem raz w roku dokonuje przeglądu i aktualizacji Polityki (lub każdorazowo w przypadku konieczności dokonania istotnych zmian).

ROZDZIAŁ II. PROCEDURY NADAWANIA, MODYFIKACJI I REJESTROWANIA UPRAWNIEŃ W SYSTEMIE INFORMATYCZNYM.

1. W systemach informatycznych służących do przetwarzania danych osobowych stosuje się mechanizmy kontroli dostępu do tych danych w celu zabezpieczenia przed nieuprawnionym dostępem do zasobów systemowych. Wspomniana kontrola realizowana jest m.in. poprzez zarządzanie uprawnieniami dostępu do systemu oraz wprowadzenie procedury rejestracji użytkownika w systemie.
2. Każda osoba przed przystąpieniem do przetwarzania danych osobowych w systemie informatycznym zobligowana jest do zapoznania się z:
   1) Rozporządzeniem;
   2) „Polityką Ochrony Danych Osobowych w ITONA sp. z o.o. w Lublinie";
   3) „Polityką Ochrony Danych Osobowych w sytuacji naruszenia bezpieczeństwa przetwarzania danych osobowych w ITONA sp. z o.o. w Lublinie";
   4) niniejszą Polityką.
3. Dostęp do systemów informatycznych służących do przetwarzania danych osobowych

może uzyskać wyłącznie osoba uprawniona, która posiada imienne upoważnienie do przetwarzania danych osobowych.

4. Nadanie i jakiekolwiek zmiany uprawnień do użytkowania systemu informatycznego, w którym przetwarzane są dane osobowe następują wyłącznie na wniosek bezpośredniego przełożonego użytkownika (zgodnie z załącznikiem nr 1 do niniejszej Polityki).
5. Wniosek dotyczący systemu, w którym przetwarza się dane osobowe wymaga akceptacji IOD.
6. Osoba zarządzająca sprzętem komputerowym i oprogramowaniem występuje z wnioskiem o nadanie/modyfikację/odbiór uprawnień dla pracownika w następujących sytuacjach:
   1) pracownik nowoprzyjęty (w tym stażyści i praktykanci),
   2) pracownik zmieniający stanowisko pracy lub miejsce zatrudnienia w ramach ITONA sp. z o.o. w Lublinie,
   3) pracownik, dla którego w ramach jego obowiązków służbowych zaistniała konieczność modyfikacji nadanych wcześniej uprawnień,
   4) pracownik, dla którego w ramach jego obowiązków służbowych zaistniała konieczność nadania uprawnień.
7. Wszystkie wnioski rejestrowane są w Rejestrze wniosków o nadanie/modyfikację/odbiór uprawnień do użytkowania systemu informatycznego (zgodnie z załącznikiem nr 2 do niniejszej Polityki; wypełniony Rejestr znajduje się w dokumentacji prowadzonej przez Osobę zarządzającą sprzętem komputerowym i oprogramowaniem).

ROZDZIAŁ III. STOSOWANE METODY I ŚRODKI UWIERZYTELNIENIA W SYSTEMIE ORAZ PROCEDURY ZWIĄZANE Z ICH ZARZĄDZANIEM I UŻYTKOWANIEM.

1. Identyfikacja i uwierzytelnienie użytkownika.
   1) W systemach informatycznych służących do przetwarzania danych osobowych stosuje się mechanizmy kontroli dostępu do tych danych;
   2) stosowanie mechanizmów uwierzytelniania oraz zarządzanie hasłami użytkownika w systemach informatycznych ma na celu ochronę przed nieuprawnionym dostępem, utratą i modyfikacją danych osobowych. Ponadto realizacja zasad uwierzytelniania użytkownika w systemie pozwala na zapewnienie dostępności, autentyczności, rozliczalności, integralności i poufności danych;
   3) użytkownik uzyskuje dostęp do systemu, w którym przetwarzane są dane osobowe wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia przy pomocy hasła;

4) jeżeli dostęp do danych osobowych przetwarzanych w systemie informatycznym posiada więcej niż jedna osoba, wówczas zapewnia się, aby w takim systemie dla każdego użytkownika rejestrowany był odrębny identyfikator;
5) identyfikacja użytkownika odbywa się na podstawie unikatowego/indywidualnego identyfikatora (loginu) skojarzonego z hasłem. Identyfikator wiąże się z prawami dostępu określającymi uprawnienia nadane użytkownikowi. Identyfikator użytkownika nie zmienia się w ciągu całego okresu pracy (stażu, praktyki) w ITONA sp. z o.o. w Lublinie;
6) identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych w systemie informatycznym, nie może być przydzielony innej osobie.

2. Zarządzanie i zasady posługiwania się hasłami.
1) Hasło wydawane jest użytkownikowi po pozytywnym zakończeniu procedury nadania uprawnień do użytkowania systemu informatycznego, w którym przetwarzane są dane osobowe (zgodnie z załącznikiem nr 1 niniejszej Polityki);
2) hasła generuje i w ustalonej formie wydaje użytkownikom Osoba zarządzająca sprzętem komputerowym i oprogramowaniem. Hasła powinny być przekazywane w sposób zapewniający ich poufność i bezpieczeństwo w celu ograniczenia ryzyka przechwycenia haseł (zalecanym sposobem jest osobiste przekazywanie hasła);
3) użytkownik systemu służącego do przetwarzania danych odpowiada za niezwłoczną zmianę hasła tymczasowego przydzielonego przez Osobę zarządzająca oprogramowaniem. Użytkownik odpowiada za zachowanie poufności nowego, wybranego przez siebie hasła;
4) użytkownik jest odpowiedzialny za wszystkie operacje dokonane przy użyciu jego identyfikatora oraz za zachowanie poufności swojego hasła. Hasło należy utrzymywać w tajemnicy również po upływie jego ważności;
5) oprogramowanie systemowe nie może pozwalać na wyświetlanie hasła jawnym tekstem na monitorze komputera, jak również na przechowywanie i zapisywanie hasła w postaci jawnego tekstu;
6) użytkownikowi zabrania się przekazywania hasła innym osobom oraz zapisywania i umieszczania haseł w miejscach, w których mogłyby zostać ujawnione;
7) hasła dostępu do profili z uprawnieniami administratora powinny być przechowywane w bezpiecznym miejscu, w sposób zapewniający utrzymanie ich w tajemnicy;
8) wymagania dotyczące haseł:
a) musi składać się co najmniej z 8 znaków, zawierać małe i wielkie litery

oraz cyfry lub znaki specjalne,

b) musi być zmieniane nie rzadziej niż co 30 dni,

c) nie może być tożsame z nazwą konta lub jego częścią,

d) musi być inne niż 5 ostatnio używanych haseł.

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

1. Procedura rozpoczęcia pracy:
   1) przed rozpoczęciem pracy, użytkownik powinien sprawdzić, czy na stacji roboczej lub innym sprzęcie informatycznym nie znajdują się ślady uszkodzeń lub ingerencji osób (w sytuacji podejrzenia naruszenia zabezpieczeń systemu informatycznego służącego do przetwarzania danych osobowych należy niezwłocznie poinformować Osobę zarządzającą sprzętem komputerowym i oprogramowaniem oraz IOD.);
   2) należy uruchomić komputer oraz zalogować się do systemu wprowadzając identyfikator użytkownika i hasło (hasło należy wprowadzać w sposób zapewniający jego poufność – tj. uniemożliwiający podejrzenie itp.);
   3) monitory urządzeń komputerowych muszą być ustawione w sposób uniemożliwiający osobie nieuprawnionej wgląd w wyświetlane na monitorze dane osobowe.
2. Procedura zawieszenia pracy w systemie:
   1) użytkownik systemu powinien przestrzegać zasady czystego ekranu, która polega na zabezpieczeniu komputera pozostawionego bez nadzoru przed jego nieuprawnionym użyciem. Użytkownik przy każdorazowym opuszczaniu stanowiska komputerowego powinien zadbać, aby na ekranie nie były wyświetlane dane osobowe. W sytuacji pozostawiania bez nadzoru komputera lub innego sprzętu zabezpieczanego hasłem oraz w momencie opuszczania pomieszczania biurowego, w którym to urządzenie się znajduje, użytkownik zobowiązany jest do zablokowania urządzenia (blokowania komputera stacjonarnego z zainstalowanym systemem operacyjnym Microsoft Windows dokonuje się poprzez naciśnięcie klawiszy „Windows + L” albo „CTRL + ALT + Delete”, a następnie ENTER);
   2) na stacjach roboczych wymaga się stosowania wygaszacza ekranu chronionego hasłem w przypadku braku aktywności użytkownika w systemie.
3. Procedura zakończenia pracy w systemie:
   1) zamknąć uruchomiony program/aplikację służącą do przetwarzania danych osobowych;

2) wylogować się z systemu;

3) wyłączyć urządzenie komputerowe (niedopuszczalne jest wyłączanie komputera przed zamknięciem oprogramowania oraz zakończeniem pracy w sieci).

ROZDZIAŁ V. PROCEDURY TWORZENIA KOPII ZAPASOWYCH ZBIORÓW DANYCH ORAZ PROGRAMÓW I NARZĘDZI PROGRAMOWYCH SŁUŻĄCYCH DO ICH PRZETWARZANIA.

1. W ITONA sp. z o.o. w Lublinie dane osobowe przetwarzane w systemie informatycznym zabezpiecza się poprzez wykonywanie kopii zapasowych zbiorów danych i programów służących do przetwarzania danych. Kopie zapasowe tworzy się w celu zapewnienia optymalnego poziomu ochrony danych osobowych przetwarzanych ITONA sp. z o.o. w Lublinie.
2. Za wskazanie zbiorów do zabezpieczenia kopią zapasową odpowiada Zarząd.
3. Osoba zarządzająca sprzętem komputerowym i oprogramowaniem w ITONA sp. z o.o. w Lublinie prowadzi wykaz systemów informatycznych (według wzoru stanowiącego załącznik nr 4 do niniejszej Polityki - Lista systemów informatycznych).
4. Osoba zarządzająca sprzętem komputerowym i oprogramowaniem w ITONA sp. z o.o. w Lublinie przygotowuje plan wykonywania kopii zapasowych (stanowiący załącznik nr 3 do niniejszej Polityki) i odpowiada za jego realizację.
5. Osoba zarządzająca sprzętem komputerowym i oprogramowaniem w ITONA sp. z o.o. w Lublinie wykonująca kopie zapasowe jest zobowiązana do każdorazowego weryfikowania poprawności wykonania kopii zapasowych.
6. Osoba zarządzająca sprzętem komputerowym i oprogramowaniem ma obowiązek okresowo przeprowadzać operację testowego odzyskiwania danych z wykonanych kopii zapasowych w celu weryfikacji procesu odtworzenia kopii. Odtworzenie może być sprawdzane wyłącznie w środowisku testowym.
7. Użytkownik ma następujące możliwości zabezpieczenia danych (plików):

1) sporządzenie kopii zapasowych na wymiennym nośniku;

2) przechowywanie danych (plików) zapisanych na nośnikach informacji (np.: serwer, itp.),

3) dane zostają automatycznie zapisywane w związku z działalnością prowadzoną przez podmiot współpracujący z ITONA sp. z o.o. z siedzibą w Lublinie w chmurze obliczeniowej.

ROZDZIAŁ VI. SPOSÓB, MIEJSCE I OKRES PRZECHOWYWANIA ELEKTRONICZNYCH NOŚNIKÓW INFORMACJI ZAWIERAJĄCYCH DANE OSOBOWE ORAZ KOPII ZAPASOWYCH.

1. W ITONA sp. z o.o. w Lublinie istnieje obowiązek przechowywania wydruków,

elektronicznych nośników informacji zawierających dane osobowe, kopii zapasowych w miejscach zabezpieczających dane przed nieuprawnionym dostępem, przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem.

2. Wydruki oraz nośniki informacji zawierające dane osobowe (w tym kopie zapasowe zbiorów danych osobowych i programów) przechowywane są w zabezpieczonych pomieszczeniach stanowiących obszar przetwarzania danych osobowych określony w załączniku nr 6 do „Polityki Ochrony Danych Osobowych w ITONA sp. z o.o. w Lublinie".
3. Nośniki informacji zawierające dane osobowe należy przechowywać w zabezpieczonych pomieszczeniach w szafach/sejfach/kasetkach zamykanych na klucz.
4. Pracownik ponosi odpowiedzialność za zabezpieczenie kluczy do szaf i szuflad, w których przechowywane są dane osobowe.
5. Nośniki zawierające kopie zapasowe nie mogą być przechowywane w miejscu przetwarzania danych, dla których utworzono kopie zapasowe.
6. Kopie zapasowe danych osobowych usuwa się niezwłocznie po ustaniu ich użyteczności.
7. Wydruki zawierające dane osobowe, należy zniszczyć w niszczarce niezwłocznie po ich wykorzystaniu, chyba, że z odrębnych przepisów wynika obowiązek ich przechowywania.

ROZDZIAŁ VII. ZABEZPIECZENIE I OCHRONA SYSTEMU.

1. Za integralność i utrzymanie prawidłowego działania systemów informatycznych służących do przetwarzania danych osobowych odpowiada Osoba zarządzająca sprzętem komputerowym i oprogramowaniem.
2. Osoba zarządzająca sprzętem komputerowym i oprogramowaniem odpowiada za specyfikację zamówienia w odniesieniu do wymogów sprzętowych składników systemu teleinformatycznego.
3. Nabywane dla potrzeb użytkowania w ITONA sp. z o.o. w Lublinie urządzenia i systemy informatyczne służące do przetwarzania danych osobowych powinny spełniać wymogi oraz zasady określone w przepisach dotyczących ochrony danych osobowych. Za realizację powyższego obowiązku odpowiada Osoba zarządzająca sprzętem komputerowym i oprogramowaniem.
4. Podczas wyboru i pozyskiwania systemów informatycznych służących do przetwarzania danych osobowych należy zadbać, aby dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, system ten zapewniał odnotowywanie informacji o odbiorcach, którym dane osobowe zostały udostępnione oraz dacie i zakresie tego udostępnienia (chyba, że system informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych).
5. Bezpieczeństwo funkcjonowania sieci komputerowej zapewnia się poprzez

zabezpieczenia sprzętowe, oprogramowanie i procedury, jak również zawarcie niezbędnych umów serwisowych.

6. System informatyczny służący do przetwarzania danych osobowych zabezpiecza się przed:
   1) utratą danych spowodowaną awarią lub zakłóceniami zasilania;
   2) zagrożeniami pochodzącymi z sieci publicznej poprzez stosowanie fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem do danych;
   3) działaniem szkodliwego oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu.
7. Połączenie wewnętrznej sieci z Internetem jest realizowane za pośrednictwem urządzeń zapewniających ochronę zasobów komputerowych znajdujących się w sieci wewnętrznej (firewall, UTM).
8. Dostęp do sieci Internet związany jest m.in. z następującymi zagrożeniami: utrata kontroli nad zasobami systemu informatycznego; przechwycenie informacji na temat zasobów sieci wewnętrznej; atak na zasoby sieci; dostęp do zasobów systemu, w którym przetwarzane są dane osobowe.
9. Ochrona przed wyżej wymienionymi zagrożeniami odbywa się poprzez wprowadzenie i przestrzeganie określonych procedur, instrukcji, zasad i mechanizmów technicznych na etapie wdrożeń oraz eksploatacji systemu teleinformatycznego polegających w szczególności na:
   1) stosowaniu sprzętowych i programowych zabezpieczeń na styku z siecią Internet;
   2) zarządzaniu dostępem do sieci Internet;
   3) stosowaniu ograniczeń w dostępie do usług internetowych;
   4) ciągłym monitoringu oraz kontroli ruchu i dostępu do sieci Internet;
   5) rejestrowaniu incydentów oraz innych określonych zdarzeń zaistniałych na styku sieci Internet i sieci wewnętrznej;
   6) stosowaniu odpowiednich zabezpieczeń stanowisk komputerowych mających dostęp do sieci Internet;
   7) kontrolowaniu dostępu użytkowników do usług i zasobów sieci Internet zgodnie z przyznanymi uprawnieniami;
   8) konieczności użytkowania bezpiecznych, ogólnie znanych stron WWW;
   9) blokowaniu niektórych wybranych stron internetowych.
10. Szkodliwym oprogramowaniem, którego celem jest uzyskanie nieuprawnionego dostępu do systemu i zniszczenia w systemie są:
   1) wirusy, kody trojańskie, robaki internetowe;
   2) programy mające na celu nieautoryzowane zdobycie, modyfikację lub destrukcję

danych;

3) programy umożliwiające zdobycie lub podniesienie uprawnień w systemach informatycznych służących do przetwarzania danych osobowych;
4) programy, które mogą wpłynąć niekorzystnie na pracę systemów informatycznych poprzez utrudnienie lub sparaliżowanie ich pracy;
5) inne, które mogą spowodować destabilizację działania i fałszowanie danych.

11. W przypadku wystąpienia naruszeń ochrony danych osobowych w systemie teleinformatycznym należy podjąć działania zgodnie z „Polityką Ochrony Danych Osobowych w sytuacji naruszenia bezpieczeństwa przetwarzania danych osobowych w ITONA sp. z o.o. w Lublinie”.
12. W ITONA sp. z o.o. w Lublinie każdy komputer jest objęty ochroną w czasie rzeczywistym za pomocą oprogramowania antywirusowego.
13. Za instalację i właściwe skonfigurowanie oprogramowania antywirusowego na stacjach roboczych i komputerach przenośnych odpowiada Osoba zarządzająca sprzętem komputerowym i oprogramowaniem.
14. Aktualizacja baz wirusów odbywa się automatycznie. Po każdej naprawie i konserwacji urządzenia, a przed ponownym włączeniem do systemu informatycznego zawartość stałych nośników komputerowych jest sprawdzana za pomocą aktualnego oprogramowania.
15. W przypadku transportowania komputerów przenośnych, na których znajdują się dane osobowe, poza obszar ich przetwarzania, obowiązkowo stosuje się środki ochrony kryptograficznej tych danych.

ROZDZIAŁ VIII. ZASADY DLA UŻYTKOWNIKÓW SYSTEMU TELEINFORMATYCZNEGO.

1. Użytkownik systemu teleinformatycznego jest zobowiązany do:
   1) przestrzegania prawa oraz wewnętrznych regulacji w zakresie prawidłowego i bezpiecznego przetwarzania danych osobowych w systemach informatycznych;
   2) prawidłowego korzystania z urządzeń i systemów informatycznych zgodnie z powierzonymi obowiązkami służbowymi;
   3) ochrony powierzonego sprzętu komputerowego oraz wszystkich zasobów systemu teleinformatycznego, z których korzysta podczas przetwarzania danych osobowych w ramach wykonywania swoich obowiązków służbowych;
   4) ochrony danych osobowych przed ich udostępnieniem osobom nieupoważnionym, nieuprawnioną zmianą, utratą, uszkodzeniem lub zniszczeniem stosując dostępne środki techniczne oraz zasady opisane w niniejszej Polityce oraz „Polityce Ochrony Danych Osobowych w ITONA sp. z o.o. w Lublinie”.
   5) zachowania szczególnej staranności przy przetwarzaniu danych, a zwłaszcza

do zapewnienia, aby dane były:

a) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość”),

b) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 Rozporządzenia za niezgodne z pierwotnymi celami („ograniczenie celu”),

c) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych”),

d) prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane („prawidłowość”),

e) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1 Rozporządzenia, z zastrzeżeniem, że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy Rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą („ograniczenie przechowywania”),

f) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność”).

2. Użytkownikom nie wolno:

1) wykorzystywać identyfikatorów innych użytkowników i uruchamiać aplikacji deszyfrujących (łamiących) hasła;

2) ujawniać innym osobom przetwarzanych danych osobowych oraz informacji o sposobach zabezpieczenia danych osobowych w systemach informatycznych.

3) używania modemów GSM będących na wyposażeniu sprzętu przenośnego podczas korzystania z sieci LAN. Urządzenia te powinny być wtedy wyłączone lub zablokowane,

4) przechowywania na dostępnych zasobach informatycznych, tj. komputer, nośniki wymienne, dyski sieciowe itp., wszelkiego rodzaju utworów np. muzyka, filmy, programy naruszające prawo do własności intelektualnej zgodnie z ustawą o prawie autorskim i prawach pokrewnych,
5) korzystania z oprogramowania innego niż zakupione na podstawie odpowiednich umów zawartych przez ITONA sp. z o.o. w Lublinie lub stworzone samodzielnie, zatwierdzone i udostępnione do użytku przez Osobę zarządzająca sprzętem komputerowym i oprogramowaniem,
6) samodzielnej instalacji lub deinstalacji jakiegokolwiek oprogramowania,
7) samodzielnej instalacji, wymiany i usuwania jakichkolwiek komponentów oraz wyposażenia urządzenia komputerowego (napędy i nagrywarki CD i DVD, FDD, dodatkowe dyski twarde, rozszerzenia pamięci operacyjnej, itp.) bez zgody Osoby zarządzającej sprzętem komputerowym i oprogramowaniem w ITONA sp. z o.o. w Lublinie,
8) samodzielnego uruchamiania urządzenia komputerowego z nośników zewnętrznych (FDD, CD-ROM, DVD-ROM, itp.),
9) wynoszenia komputerów stacjonarnych lub jakichkolwiek elementów komputerów z siedziby ITONA sp. z o.o. w Lublinie,
10) przechowywania danych służbowych na prywatnych komputerach lub prywatnych przenośnych nośnikach informacji,
11) wykonywania kopii i dystrybucji oprogramowania i jego dokumentacji, których właścicielem jest ITONA sp. z o.o. w Lublinie,
12) modyfikowania logów i plików systemowych,
13) dokonywania prób obejścia zabezpieczeń narzucanych przez systemy informatyczne.

ROZDZIAŁ IX. ZAŁĄCZNIKI.

1. Załącznik nr 1 – Wniosek o nadanie/modyfikację/odbiór uprawnień do użytkowania systemu informatycznego.
2. Załącznik nr 2 – Rejestr wniosków o nadanie/modyfikację/odbiór uprawnień do użytkowania systemu informatycznego.
3. Załącznik nr 3 – Plan wykonywania kopii zapasowych.
4. Załącznik nr 4 – Lista systemów informatycznych.
5. Załącznik nr 5 – Arkusz aktualizacji.