INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

w

ELPIANO MAŁGORZATA JUREWICZ

Pasaż Ursynowski 3 lok. 6

02-784 Warszawa

NIP: 5213118194

REGON: 141787918

Dokument przygotowany przez:

Clauzula.pl

Relexus Sp. z o.o.
ul. Zielona 8/18
61-851 Poznań

NIP 7831698739
REGON 302403780
KRS 0000458750

Clauzula.pl

I – Część ogólna

§ 1 Podstawa Prawna

Zgodnie z art. 39a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2002 r. Nr 101, poz. 926 z późn. zm.) oraz z § 3 ust. 1 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. z 2004 r. Nr 100, poz. 1024 z późn. zm.), ustanawia się „Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych".

ELPIANO MAŁGORZATA JUREWICZ, Pasaż Ursynowski 3 lok. 6, 02-784 Warszawa, NIP: 5213118194, REGON: 141787918

§ 2 Pojęcia

1. Ilekroć w niniejszym dokumencie jest mowa o:
   a) **ustawie** – należy przez to rozumieć ustawę, o której mowa w § 1 części ogólnej niniejszej instrukcji zarządzania systemem informatycznym
   b) **rozporządzeniu** – należy przez to rozumieć rozporządzenie, o którym mowa w § 1 części ogólnej niniejszej instrukcji zarządzania systemem informatycznym
   c) **jednostce organizacyjnej** – należy przez to rozumieć ELPIANO MAŁGORZATA JUREWICZ, Pasaż Ursynowski 3 lok. 6, 02-784 Warszawa, NIP: 5213118194, REGON: 141787918.
   d) **ADO** – należy przez to rozumieć Administratora Danych Osobowych w rozumieniu ustawy
   e) **ABSI** – należy przez to rozumieć Administratora Bezpieczeństwa Informacji w rozumieniu ustawy
   f) **ASI** – należy przez to rozumieć Administratora Systemu Informatycznego w rozumieniu § 3 części ogólnej niniejszej instrukcji zarządzania systemem informatycznym
   g) **Instrukcji** – należy przez to rozumieć niniejszy dokument
   h) **Polityce Bezpieczeństwa** – należy przez to rozumieć przyjęty do stosowania w jednostce organizacyjnej dokument zatytułowany: „Polityka Bezpieczeństwa" ELPIANO MAŁGORZATA JUREWICZ, Pasaż Ursynowski 3 lok. 6, 02-784 Warszawa, NIP: 5213118194, REGON: 141787918.
   i) **Użytkowniku** – należy przez to rozumieć osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym w drodze upoważnienia, o jakim mowa w Polityce Bezpieczeństwa. Postanowienia dotyczące użytkowników należy stosować odpowiednio do ADO oraz ABSI.
   j) **systemie informatycznym** – należy przez to rozumieć system informatyczny, w którym przetwarzane są dane osobowe w jednostce organizacyjnej
   m) **kopii pełnej** – należy przez to rozumieć kopię zapasową całości danych osobowych przetwarzanych w systemie informatycznym

Relexus Sp. z o.o.
ul. Zielona 8/18
61-851 Poznań
NIP 7831698739
REGON 302403780
KRS 0000458750
Clauzula.pl

n) **kopii przyrostowej** – należy przez to rozumieć kopię zapasową tej części danych osobowych przetwarzanych w systemie informatycznym, która została dodana do systemu informatycznego w określonym czasie

o) **osobie wyznaczonej przez ASI w sytuacji wyjątkowej** – należy przez to rozumieć osobę, która podpisała oświadczenie stanowiące załącznik nr 2 do Polityki Bezpieczeństwa, otrzymała upoważnienie stanowiące załącznik nr 1 do Polityki Bezpieczeństwa, oraz została ustnie upoważniona przez ASI do dokonania określonych działań wchodzących w zakres jego obowiązków.

§ 3 ASI, ABSI oraz ADO

1. ASI wyznaczany jest przez ABSI lub ADO drogą pisemnego upoważnienia. W przypadku nie wyznaczenia ASI, jego funkcję pełni ABSI lub osoba pełniąca funkcję ABSI. Wzór upoważnienia ASI stanowi załącznik nr 1 do niniejszego dokumentu.
2. ASI jest również zobowiązany do podpisania oświadczenia, stanowiącego załącznik nr 2 do Polityki Bezpieczeństwa.

§ 4 Obowiązki ASI

1. ASI jest odpowiedzialny za przestrzeganie zasad bezpieczeństwa przetwarzania danych osobowych w zakresie systemu informatycznego służącego do tego celu.
2. Do obowiązków ASI należy także kontrola przepływu informacji pomiędzy systemem informatycznym a siecią publiczną oraz kontrola działań inicjowanych z sieci publicznej i systemu informatycznego.
3. Obowiązkiem ASI jest zabezpieczenie sprzętu komputerowego przed nieuprawnionym dostępem oraz przeprowadzanie analizy ryzyka uwzględniającej realne zagrożenia dla systemu informatycznego.

§ 5 Poziom Bezpieczeństwa

Zgodnie z rozporządzeniem, uwzględniając fakt, że użytkowany w jednostce organizacyjnej system informatyczny służący do przetwarzania danych osobowych jest połączony z siecią Internet, wprowadza się wysoki poziom bezpieczeństwa.

II – Część szczegółowa

§ 1 Uprawnienia

1. Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym określa się w sposób następujący:
   a) użytkownik zamierzający przetwarzać dane osobowe, po uzyskaniu upoważnienia stanowiącego załącznik nr 1 do Polityki

Relexus Sp. z o.o.
ul. Zielona 8/18
61-851 Poznań

NIP 7831698739
REGON 302403780
KRS 0000458750

Clauzula.pl

Bezpieczeństwa, oraz podpisaniu oświadczenia stanowiącego załącznik nr 2 do Polityki Bezpieczeństwa, składa ustnie wniosek do ASI o nadanie identyfikatora i hasła w celu umożliwienia wykonywania przetwarzania danych osobowych w systemie informatycznym, ASI zobowiązany jest niezwłocznie przydzielić użytkownikowi identyfikator i hasło. Podanie użytkownikowi hasła nie może nastąpić w sposób umożliwiający zapoznanie się z nim osobom trzecim.

b) w przypadku wygaśnięcia przesłanek uprawniających użytkownika do przetwarzania danych osobowych, w szczególności cofnięcia upoważnienia, stanowiącego załącznik nr 1 do Polityki Bezpieczeństwa, ASI zobowiązany jest do dopełnienia czynności uniemożliwiających ponowne wykorzystanie identyfikatora użytkownika, którego uprawnienia wygasły.

§ 2 Metody i środki uwierzytelniania; procedury związane z zarządzaniem i użytkowaniem

1. Stosuje się następujące metody oraz środki uwierzytelniania, a także procedury związane z ich zarządzaniem i użytkowaniem:

a) hasła powinny składać się z kombinacji co najmniej ośmiu (8) znaków alfanumerycznych. Jeżeli jest to możliwe, w haśle powinny znaleźć się znaki pisane wielką i małą literą, znaki numeryczne i specjalne

b) osobą odpowiedzialną za przydział identyfikatora i pierwszego hasła jest ASI

c) użytkownik, po pierwszym zalogowaniu się do systemu jest zobowiązany do zmiany hasła

d) hasło nie może być takie samo jak profil użytkownika;

e) użytkownik jest zobowiązany do zabezpieczenia swojego hasła przed nieuprawnionym dostępem osób trzecich

f) hasło nie powinno być wyświetlane na monitorze w formie tekstowej

g) systemy muszą umożliwiać użytkownikom zmianę haseł

h) przy zmianie hasła użytkownik powinien wprowadzić stare hasło a następnie wprowadzić dwukrotnie nowe hasło

i) w przypadku stwierdzenia bądź podejrzenia ujawnienia jakiegokolwiek hasła, w tym również haseł należących do klientów, administrator danego systemu powinien niezwłocznie wymusić zmianę hasła

j) jeśli użytkownik podejrzewa, że jego hasło jest znane innej osobie, powinien niezwłocznie zmienić to hasło

k) systemy powinny wymuszać zmianę hasła w regularnych odstępach czasowych nie rzadziej jednak niż co trzydzieści (30) dni

m) przy zmianie hasła nie powinno wykorzystywać się żadnego z piętnastu (15) ostatnio użytych haseł;

n) System nie powinien wskazywać konkretnego powodu, dla którego wprowadzone przez użytkownika hasło nie może zostać zaakceptowane

o) należy poinformować klientów, pracowników i usługodawców zewnętrznych o zasadach zarządzania hasłami.

§ 3 Profil Użytkownika i hasła

1. Profil użytkownika związany z hasłem statycznym należy:

a) zablokować po okresie nieaktywności w systemie (maksymalnie do sześćdziesięciu (60) dni);

b) zablokować w systemie, jeżeli upłynęło trzydzieści (30) dni od daty jego utworzenia i w tym okresie profil nie był wykorzystany;

c) zablokować, kiedy jego użytkownik jest na urlopie dłuższym niż trzydzieści (30) dni;

d) powinno się wymusić na użytkowniku powtórne uwierzytelnienie po dziesięcio (10) minutowym okresie bezczynności;

e) po zakończeniu pracy użytkownik jest zobowiązany do wylogowania się, a następnie do wyłączenia komputera

Relexus Sp. z o.o.
ul. Zielona 8/18
61-851 Poznań

NIP 7831698739
REGON 302403780
KRS 0000458750

Clauzula.pl

2. Haseł oraz identyfikatorów nie należy przechowywać lub ustawiać w systemach lub aplikacjach w taki sposób aby możliwe było automatyczne logowanie się bez podawania hasła.
3. Profile użytkownika z hasłem statycznym są blokowane po trzech (3) kolejnych nieudanych próbach logowania.
4. Za pośrednictwem jednego identyfikatora i hasła może pracować tylko i wyłącznie osoba, dla której dedykowany jest dany identyfikator. Wykrycie nadużycia w postaci „dzielenia" się identyfikatorem i hasłem skutkować będzie natychmiastowym zablokowaniem danego konta. Dopiero po formalnym wyjaśnieniu konto takie może zostać ponownie odblokowane.

§ 4 Nowe oprogramowanie: hasła domyślne oraz opuszczenie stanowiska pracy - zalecenia

1. Przed wdrożeniem lub zakupem nowej wersji oprogramowania bądź sprzętu, na którym preinstalowany jest system należy zidentyfikować wszystkie ustawione domyślnie profile i hasła.
2. Wszystkie domyślne hasła należy zmienić natychmiast po instalacji stosując kombinację co najmniej ośmiu (8) znaków, obejmujących znaki alfabetu pisane wielką i małą literą, a także cyfry i znaki specjalne.
3. Wszystkie profile domyślne należy (jeśli jest to możliwe) wykasować, zablokować, opatrzyć zmienioną nazwą lub w inny udokumentowany sposób ukryć.
4. Każda stacja robocza użytkownika powinna mieć włączony wygaszacz ekranu zabezpieczony hasłem. Włączenie wygaszacza ekranu zabezpieczonego hasłem powinno wystąpić maksymalnie po dziesięciu (10) minutach nieaktywności użytkownika.
5. Jeśli użytkownik opuszcza na dowolny okres czasu stanowisko pracy, na którym korzystał z aplikacji lub dedykowanego systemu, powinien aktywować wygaszacz ekranu poprzez zablokowanie komputera (najczęściej poprzez jednoczesne naciśnięcie klawiszy Control + Alt + Delete).
6. W przypadku planowanego zakończenia pracy w danym systemie, użytkownik ma obowiązek wylogowania się z tej aplikacji lub doprowadzenia tej aplikacji lub komputera do takiego stanu, aby nie było możliwe korzystanie z danej aplikacji przez innego użytkownika bez podania identyfikatora i hasła. Komputer po zakończonej pracy powinien zostać całkowicie wyłączony jak również monitor.

§ 5 Procedury stosowane przy tworzeniu i przechowywaniu kopii zapasowych zbiorów

1. Stosuje się następujące procedury tworzenia oraz przechowywania kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania:
   a) raz na miesiąc ASI wykonuje kopię przyrostową
   b) raz na rok ASI wykonuje kopię pełną

Relexus Sp. z o.o.
ul. Zielona 8/18
61-851 Poznań

NIP 7831698739
REGON 302403780
KRS 0000458750

Clauzula.pl

c) wykonane kopie zapasowe przechowuje się na pamięci przenośnej (*pendrive*) lub na nośnikach CD\DVD, nośniki zawierające kopie zapasowe są przechowywane w szafie zamykanej na klucz, do której dostęp posiada wyłącznie ASI lub w sytuacji wyjątkowej, osoba przez niego wyznaczona. Kopie zapasowe przechowywane są w odrębnym pomieszczeniu

2. Niedopuszczalne jest pozostawianie wydrukowanych dokumentów na ogólnodostępnych drukarkach tzw. sieciowych jak również na drukarkach osobistych tzw. lokalnych.
3. Wydrukowane dokumenty powinny być przechowywane w miejscach, do których dostęp mają osoby posiadające prawo wglądu w dany typ wydrukowanych dokumentów. Miejsca takie powinny być odpowiednio zabezpieczone przed niepowołanym dostępem.
4. Sposób zewnętrznego przechowywania powinien być zgodny z obowiązującymi w tym zakresie standardami rynkowymi zatwierdzonymi przez dedykowane do tego celu instytucje oraz obowiązujące w tym zakresie normy.
5. Dane archiwizowane na nośnikach powinny być szyfrowane celem uniemożliwia odtworzenia ich zawartości w przypadku ich utraty.

§ 6 Miejsca przechowywania danych osobowych

1. Elektroniczne nośniki informacji zawierające dane osobowe przechowywane są w szafach zamykanych na klucz, do których dostęp ma jedynie ASI oraz, w sytuacjach wyjątkowych, osoba przez niego wyznaczona, dane są przechowywane przez okres, w którym istnieją przesłanki do ich przetwarzania, po ustaniu przesłanek do przetwarzania, dane muszą zostać usunięte w sposób uniemożliwiający ich odtworzenie. Dane przechowywane są w odrębnym pomieszczeniu.
2. Sprzęt komputerowy, na którego dyskach twardych zawarte są dane osobowe, przechowywany jest w obszarze przetwarzania danych osobowych, w pomieszczeniach zabezpieczonych zgodnie z załącznikiem nr 1 do Polityki Bezpieczeństwa.

§ 7 System zabezpieczeń – programy antywirusowe

1. Na wszystkich stacjach roboczych, komputerach przenośnych oraz serwerach aktywny powinien być system zabezpieczeń antywirusowych, antyszpiegowskich oraz wykrywający złośliwe oprogramowanie.
2. Aktualizacja powinna być wykonywana na bieżąco w miarę pojawiania się kolejnych aktualizacji zbiorów definicji wirusów komputerowych.
3. Częściowa kontrola antywirusowa zasobów komputera (pamięć, boot sektor itd.) odbywać się powinna przy jego włączaniu. Pełna kontrola powinna odbywać się, jeśli to możliwe, w trakcie jego pracy lub przynajmniej raz w tygodniu. Wszelkie nośniki zewnętrzne przed użyciem w systemie sieciowym firmy bezwzględnie powinny być sprawdzane pod kątem obecności wirusów.
4. Programy antywirusowe powinny być konfigurowane w taki sposób, aby przeprowadzały kontrolę w czasie normalnej pracy tzw. tryb on-line.

Relexus Sp. z o.o.
ul. Zielona 8/18
61-851 Poznań

NIP 7831698739
REGON 302403780
KRS 0000458750

Clauzula.pl

5. Aktualizacje programów antywirusowych oraz aktualizacje plików identyfikujących wirusy w stacjach roboczych podłączonych przez sieć lokalną LAN, powinny dokonywać się automatycznie.
6. System informatyczny zabezpiecza się przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do tego systemu poprzez stosowanie specjalistycznego oprogramowania,
   a) w systemie informatycznym stosowane jest oprogramowanie firewall zapewniające kontrolę przepływu informacji oraz działań inicjowanych z zewnątrz i od wewnątrz systemu
   b) użytkownikom nie wolno otwierać na komputerach, na których odbywa się przetwarzanie danych osobowych, plików pochodzących z niewiadomego źródła bez zgody ASI
   c) za wdrożenie i korzystanie z oprogramowania antywirusowego, określonego w lit. a oraz oprogramowania firewall, określonego w lit. b niniejszego paragrafu, odpowiada ASI

§ 8 Informacje o odbiorcach

Odnotowanie informacji o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia (z wyłączeniem osób, których dane dotyczą, osób posiadających upoważnienie do przetwarzania danych, organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem), odbywa się poprzez zapisanie tej informacji w utworzonym na dysku twardym komputera pliku dotyczącym danej osoby, zgodnie z systemem zapisywania informacji.

§ 9 Procedury przeglądów i konserwacji

1. Stosuje się następujące procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych:
   a) ASI raz na 3 miesiące wykonuje generalny przegląd systemu informatycznego, polegający na ustaleniu poprawności działania tych jego elementów, które są niezbędne do zapewnienia realizacji funkcji wynikających z niniejszej Instrukcji
   b) w przypadku stwierdzenia przez ASI nieprawidłowości w działaniu elementów systemu opisanych w lit. a niniejszego paragrafu podejmuje on niezwłocznie czynności zmierzające do przywrócenia ich prawidłowego działania
   c) jeżeli do przywrócenia prawidłowego działania systemu niezbędna jest pomoc podmiotu zewnętrznego, wszelkie czynności na sprzęcie komputerowym dokonywane w obszarze przetwarzania danych osobowych, powinny odbywać się w obecności ASI lub w sytuacji wyjątkowej – osoby przez niego wyznaczonej.

§ 10 Zabezpieczenia w przypadku utraty zasilania lub zakłóceń

1. System informatyczny służący do przetwarzania danych osobowych jest zabezpieczony przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej poprzez stosowanie (alternatywnie a lub b, lub oba

Relexus Sp. z o.o.
ul. Zielona 8/18
61-851 Poznań

NIP 7831698739
REGON 302403780
KRS 0000458750

Clauzula.pl

na raz):

a) oprogramowania dokonującego automatycznego wykonywania kopii awaryjnych w celu ochrony przed utratą danych
b) listew przepięciowych, połączonych pomiędzy siecią zasilającą a komputerami

§ 11 Komputer przenośny - zabezpieczenie

Osoba użytkująca komputer przenośny zawierający dane osobowe zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem przetwarzania danych osobowych, w tym dodatkowo zabezpiecza hasłem pliki lub foldery zawierające dane osobowe.

§ 12 Awarie, likwidacje, naprawy, kradzieże – system działania

1. Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:
   a) likwidacji – pozbawia się wcześniej zapisu tych danych, a w przypadku, gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie
   b) przekazania podmiotowi nieuprawnionemu do przetwarzania danych – pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie
   c) naprawy – pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem ASI załącznik numer 1 do „Instrukcji Zarządzania Systemem Informatycznym". Wydruki, które zawierają dane osobowe i są przeznaczone do usunięcia, powinny zostać zniszczone z wykorzystaniem urządzeń przeznaczonych do niszczenia dokumentów lub przy wykorzystaniu dedykowanych pojemników na dokumenty, których zawartość w późniejszym terminie jest niszczona.

2. Sprzęt komputerowy który uległ awarii przed przekazaniem do naprawy powinien zostać zabezpieczony w taki sposób, aby dane zawarte w jego pamięci nie mogły być odczytane przez osoby do tego nie upoważnione. Działania te muszą być dostosowane do danej sytuacji i muszą w należyty sposób uwzględniać ochronę danych.
3. W przypadku uszkodzenia nośnika i przekazania go na zewnątrz w celu odzyskania danych bezwzględnie powinna zostać podpisana umowa o zachowaniu poufności z podmiotem usługowym.
4. W przypadku dokonywania przeglądów bądź konserwacji systemu konieczne jest wykonanie kopii bezpieczeństwa danych.
5. Wszelkie prace konserwacyjne w systemie muszą być wykonywane zgodnie z przyjętym harmonogramem prac. Przyjęty harmonogram powinien pozwalać na odtworzenie stanu systemu istniejącego przed konserwacją.
6. Dane osobowe w formie elektronicznej nie powinny być przechowywane na dyskach twardych w stacjach roboczych. W miarę możliwości informacje te powinny być przechowywane na dedykowanych do tego celu serwerach plików lub serwerach aplikacyjnych. Z zawartości mniejszych serwerów, których regularnie tworzone są kopie zapasowe.
7. Wszystkie komputery stacjonarne i komputery przenośne powinny zostać skonfigurowane w taki sposób aby

Relexus Sp. z o.o.
ul. Zielona 8/18
61-851 Poznań

NIP 7831698739
REGON 302403780
KRS 0000458750

Clauzula.pl

zapewnić następujące funkcje:

a) hasło do zmian na poziomie BIOS;
b) ograniczenie uruchomienia systemu wyłącznie z twardego dysku;
c) uwierzytelnienie użytkownika przed uzyskaniem dostępu do zasobów komputera lub sieci;
d) włączenie wygaszacza ekranu zabezpieczonego hasłem maksymalnie po dziesięciu (10) minutach
e) nieaktywności użytkownika.

8. Wszystkie kradzieże komputerów osobistych powinny być natychmiast zgłaszane. Rodzaj informacji zapisanych na dysku skradzionego komputera powinien być rozpoznany.
9. Domyślnie we wszystkich stacjach roboczych powinien być zablokowany dostęp do napędów CD/DVD, stacji dyskietek (FDD) oraz portów USB.
10. Oprogramowanie znajdujące się w komputerach powinno być uaktualniane na bieżąco w celu usuwania znanych zagrożeń dla bezpieczeństwa informacji oraz w celu poprawiania stabilności działania samych aplikacji.
11. Aktualizacje powinny być dokonywane automatycznie lub zdalnie. Każdy użytkownik odchodząc od komputera jest zobowiązany do zablokowania stacji, po zakończeniu pracy użytkownicy są zobowiązani do wyłączenia komputera oraz monitora.

§ 13 Informacje odnotowane w przypadku każdej osoby, od której zbierane są dane osobowe

1. Dla każdej osoby, której dane są przetwarzane, system informatyczny służący do przetwarzania danych osobowych (z wyjątkiem systemów służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie) zapewnia odnotowanie:

a) daty pierwszego wprowadzenia danych do systemu (automatycznie)
b) identyfikatora użytkownika wprowadzającego dane osobowe do systemu (automatycznie)
c) źródła danych (jedynie w przypadku zbierania danych nie od osoby, której dotyczą)
d) informacji o odbiorcach w rozumieniu art. 7 pkt 6 ustawy o ochronie danych osobowych
e) sprzeciwu, o którym mowa w art. 32 ust. 1 pkt 8 ustawy o ochronie danych osobowych

§ 14 Raport

1. Dla każdej osoby, której dane osobowe są przetwarzane system informatyczny, zapewnia sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje.

§ 15 Naruszenie zasad bezpieczeństwa

1. Stosuje się następującą procedurę w przypadku stwierdzenia naruszenia zasad bezpieczeństwa systemu

Relexus Sp. z o.o.
ul. Zielona 8/18
61-851 Poznań

NIP 7831698739
REGON 302403780
KRS 0000458750

Clauzula.pl

informatycznego:

a) w przypadku stwierdzenia przez użytkownika naruszenia zabezpieczeń przez osoby nieuprawnione jest on zobowiązany niezwłocznie poinformować o tym fakcie ASI
b) ASI jest zobowiązany niezwłocznie podjąć czynności zmierzające do ustalenia przyczyn naruszeń zasad bezpieczeństwa i zastosować środki uniemożliwiające ich naruszanie w przyszłości.

2. Administratorzy systemów są odpowiedzialni za identyfikowanie nowych zagrożeń dla bezpieczeństwa administrowanych przez siebie systemów.
3. Administratorzy systemów są odpowiedzialni za jak najszybsze wdrażanie rozwiązań uniemożliwiających wykorzystanie zidentyfikowanego zagrożenia poprzez instalację patcha systemowego bądź rekonfigurację systemu.
4. Zabrania się używania systemów operacyjnych i oprogramowania, które nie jest serwisowane przez producenta tzn. nie ma podmiotu, który weźmie odpowiedzialność za prawidłowość działania danego systemu operacyjnego lub oprogramowania.

§ 16 Usuwanie danych osobowych z nośników

1. Usuwanie danych osobowych utrwalonych na nośnikach elektronicznych następuje poprzez powierzenie tych nośników w celu usunięcia zapisanych na nich danych wyspecjalizowanej w tej dziedzinie firmie informatycznej, lub poprzez nadpisanie usuwanych informacji przez ASI w taki sposób, by nie istniała możliwość ich ponownego odczytania. W celu usunięcia danych zapisanych na elektronicznych nośnikach ASI może dokonać ich fizycznego uszkodzenia w taki sposób, by nie istniała możliwość odtworzenia zapisanych na nich danych.

§ 17 Dostęp służbowy a prywatny

1. Dostęp do Internetu powinien służyć wyłącznie do celów służbowych. Dopuszcza się też korzystanie z bezpiecznych stron na komputerze przeznaczonym do zadań służbowych.
2. Zakazuje się kopiowania oprogramowania i dokumentów z nieznanych źródeł.
3. Zakazane są połączenia telefoniczne (dial-up) z komputerami stacjonarnymi jak również przenośnymi chyba, że:
   a) istnieje uzasadniona i udokumentowana potrzeba,
   b) nie istnieje stosowne rozwiązanie alternatywne.
4. Systemy poczty elektronicznej nie powinny być wykorzystywane do przechowywania lub transmisji danych osobowych, chyba, że dane takie zostaną zaszyfrowane.
   a) Zakazuje się instalowania i używania prywatnych narzędzi służących do obsługi prywatnej poczty elektronicznej w komputerach służbowych,

Relexus Sp. z o.o.
ul. Zielona 8/18
61-851 Poznań

NIP 7831698739
REGON 302403780
KRS 0000458750

Clauzula.pl

b) Systemy poczty elektronicznej są przeznaczone wyłącznie do użytku służbowego. Korzystanie z systemu poczty elektronicznej może być nadzorowane i monitorowane,
c) Zakazuje się przesyłania pocztą elektroniczną treści obraźliwych, pornograficznych, terrorystycznych, dyskryminujących ludzi pod względem rasy, płci, wyznania lub jakimkolwiek innym względem,
d) Zakazuje się użytkownikom korzystania z systemów poczty elektronicznej w sposób zakłócający pracę innym użytkownikom (np. spam), bądź stwarzający niebezpieczeństwo dla systemu sieci teleinformatycznej (np. przesyłanie poczty elektronicznej zawierającej duże załączniki do wielu adresatów jednorazowo).

5. Zakazuje się podłączania do sieci prywatnych urządzeń służących do przetwarzania danych informatycznych.

§ 18 Proces szyfrowania dla aplikacji

1. Dla każdej aplikacji wykorzystującej szyfrowanie powinien być stworzony udokumentowany proces opisujący generowanie, rozprowadzanie, używanie, przechowywanie, aktywację, zastępowanie oraz niszczenie wszystkich kluczy szyfrujących.
2. Wszystkie klucze kryptograficzne powinny mieć wyznaczonego właściciela. Częstotliwość zmiany klucza ustala właściciel, jednak powinna ona odbywać się nie rzadziej niż:
   a) raz w roku dla kluczy głównych (tj. kluczy stosowanych do szyfrowania innych kluczy), jeśli produkt zezwala na zautomatyzowaną aktualizację kluczy głównych oraz jeżeli klucze główne są w użyciu. Nowe systemy powinny zapewniać zautomatyzowane zarządzanie kluczem głównym;
   b) raz w ciągu dwóch lat dla kluczy prywatnych (np. prywatne klucze RSA).
3. Procedura dystrybucji kluczy powinna zapewnić, by w czasie przesyłania klucz nie był czytelny w całości. Gdy używane są klucze zabezpieczające hasła (tak jak w przypadku plików samo rozszyfrowujących się), hasło powinno być przesłane osobno, a nie razem z plikiem zaszyfrowanym. Jeśli to tylko możliwe,hasło powinno być przesyłane przy użyciu innego kanału dystrybucji (np. telefon komórkowy).
4. W przypadku, gdy klucze kryptograficzne są zapisywane w oprogramowaniu, powinny one być zaszyfrowane, gdy nie są używane. Wyjątki od tej reguły powinny być udokumentowane wraz z opisem dodatkowych mechanizmów kontrolnych minimalizujących ryzyko.

§ 19 Powierzenie danych w celu przetworzenia

1. Na podstawie stosownych umów (w tym bezwzględnie o zachowaniu poufności) możliwe jest powierzanie innym podmiotom danych w celu ich przetworzenia. Szczegóły oraz zakres prac każdorazowo określać powinna stosowna umowa w formie pisemnej.
2. Zewnętrznym obszarem przetwarzania danych osobowych są współpracujące firmy i instytucje finansowe świadczące

Relexus Sp. z o.o.
ul. Zielona 8/18
61-851 Poznań

NIP 7831698739
REGON 302403780
KRS 0000458750

Clauzula.pl

usługi przetwarzania danych. Firmy i instytucje finansowe te są objęte stosownymi umowami zapewniającymi bezpieczeństwo przesyłania i przetwarzania danych osobowych.

3. Należy dołożyć wszelkich starań, aby dane przekazywane podmiotom trzecim były w należyty sposób zabezpieczone, oraz docierały do osób upoważnionych do ich przetwarzania.
4. Niedopuszczalne jest przekazywanie niezabezpieczonych danych za pośrednictwem sieci Internet, na nośnikach elektronicznych oraz w wersjach papierowych.
5. Sposób pozyskiwania i przesyłania danych do innych podmiotów powinien być w sposób ciągły monitorowany pod kątem bezpieczeństwa. Jeśli nie ma możliwości ciągłego monitorowania pod kątem bezpieczeństwa kontrole powinny mieć charakter wyrywkowy i udokumentowany.
6. W tym celu należy stosować instrumenty takie jak audyt wewnętrzny, audyt wykonywany na zlecenie przez firmę audytorską, doraźnie należy stosować kontrolę oraz weryfikację zabezpieczeń (np. szyfrowanie plików) oraz poprawności transmisji danych.

§ 20 Zabezpieczenie danych przechowywanych w formie papierowej

1. Niniejszy dokument ma na celu wprowadzenie zwyczaju zabezpieczania danych przechowywanych między innymi w formie papierowej. Ma na celu uczulenie pracowników na zabezpieczanie dokumentacji papierowej, dbanie o ochronę danych osobowych oraz przestrzegania zasad bezpieczeństwa informacji.
2. Wszystkie dokumenty zawierające dane osobowe powinny być wyraźnie oznaczone, a wszyscy pracownicy i zewnętrzni usługodawcy powinni być świadomi tych oznaczeń.
3. Dokumenty lub nośniki zawierające dane osobowe powinny podlegać nadzorowi i kontroli:
   a) wszystkie dokumenty, „foldery“ i inne nośniki służące do przechowywania takich informacji nie powinny być pozostawiane na biurkach lub w pomieszczeniach biurowych bez nadzoru;
   b) nośniki z danymi powinny być zamknięte w zabezpieczonych miejscach po zakończeniu pracy.

§ 21 Naruszenie bezpieczeństwa informacji

1. Do przypadków naruszenia bezpieczeństwa informacji zaliczają się m.in.:
   a) naruszenie poufności;
   b) zniszczenie danych;
   c) utrata integralności systemu;
   d) niedostępność systemu lub aplikacji;
   e) utrata integralności danych;
   f) nieautoryzowane wykorzystanie zasobów;
   g) oszustwo;
   h) kradzież informacji (np. komputera przenośnego, komputera stacjonarnego, dysku twardego);
   i) wirus;

Relexus Sp. z o.o.
ul. Zielona 8/18
61-851 Poznań

NIP 7831698739
REGON 302403780
KRS 0000458750

Clauzula.pl

j) innego rodzaju wtargnięcia do systemu.

2. Wszelkie podejrzane wydarzenia, które mogą wskazywać na zaistnienie naruszenia bezpieczeństwa informacji, powinny być raportowane.
3. Wszelkie logi, dane, raporty, logi systemowe, system informatyczny i inne użyteczne dane związane z incydentem powinny być chronione od momentu jego zgłoszenia. Wszelkie dokumenty dotyczące naruszenia bezpieczeństwa informacji powinny być przechowywane co najmniej trzy lata.
4. Dla dobra postępowania nie należy rozpowszechniać informacji o zaistniałym incydencie i ograniczyć do minimum krąg osób poinformowanych.
5. W przypadku powiadomienia organów ścigania - data i godzina przyjazdu przedstawiciela organów ścigania, imię, nazwisko oraz stopień.
6. Do raportu należy również dołączyć protokół sporządzony przez organy ścigania.

III – Postanowienia końcowe

§ 1

W sprawach nieuregulowanych niniejszą Instrukcją, znajdują zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2002 r. Nr 101, poz. 926 z późn. zm.) oraz rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. z 2004 r. Nr 100, poz. 1024 z późn. zm.).

§ 2

Niniejszy dokument wchodzi w życie z dniem:

_____ - _____ - _____ r.

_____

podpis Administratora Danych Osobowych

Relexus Sp. z o.o.
ul. Zielona 8/18
61-851 Poznań

NIP 7831698739
REGON 302403780
KRS 0000458750

Clauzula.pl