INSTRUKCJA

ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

wykorzystywanego do przetwarzania danych

w Krzysztof Pakulski-TERM/SARBUZ-POLSKA

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH.

Spis treści str.

I. Cele wprowadzenia i zakres zastosowania instrukcji zarządzania systemem informatycznym.

1. „Instrukcja zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych w Krzysztof Pakulski-TERM/SARBUZ-PL , zwana dalej Instrukcją, została wprowadzona w celu spełnienia wymagań, o których jest mowa w Rozporządzenie 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)
2. Instrukcja powinna również spełniać zadania określone w Ustawie o ochronie danych z dnia 10.05.2018 roku (na tą chwile przekazana do senatu).
3. Instrukcja jest dokumentem powiązanym z „Polityką bezpieczeństwa przetwarzania danych osobowych w Krzysztof Pakulski-TERM/SARBUZ-POLSKA
4. Niniejsza instrukcja znajduje zastosowanie do systemów informatycznych, stosowanych w Krzysztof Pakulski-TERM/SARBUZ-PL, w których są przetwarzane dane osobowe.
5. Instrukcja podlega monitorowaniu i w razie potrzeby uaktualnianiu przez administratora danych osobowych lub upoważnioną przez niego osobę, w ramach sprawowania kontroli zarządczej.
6. Dokument instrukcji przechowywany jest w wersji papierowej i elektronicznej.

II. Definicje.

Ilekroć w Instrukcji jest mowa o:

1. **ustawie** – rozumie się przez to ustawę Rozporządzenie 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,
2. **danych osobowych** – rozumie się przez to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej; 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,
3. **zbiorze danych** – rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie,

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. **systemie informatycznym** – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
6. **zabezpieczeniu danych w systemie informatycznym** – rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem,
7. **usuwaniu danych** – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą.
8. **administratorze danych** – rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę, decydujące o celach i środkach przetwarzania danych osobowych,
9. **administratorze systemu ASI**– rozumie się przez to osobę zarządzającą systemem informatycznym przetwarzającym dane osobowe,
10. **użytkowniku systemu** – rozumie się przez to osobę, której został przydzielony przez administratora systemu indywidualny identyfikator w systemie informatycznym w powiązaniu z niezbędnymi uprawnieniami dostępowymi w tym systemie,
11. **elektronicznym nośniku** – rozumie się przez to elektroniczne urządzenie, na którym przechowuje się dane osobowe w celu jego ponownego odtworzenia w systemie informatycznym,
12. **zgodzie osoby, której dane dotyczą** – rozumie się przez to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści; zgoda może być odwołana w każdym czasie,
13. **odbiorcy danych** – rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem osoby, której dane dotyczą, osoby upoważnionej do przetwarzania danych, przedstawiciela, o którym mowa w art. 31a ustawy, podmiotu, o którym mowa w art. 31 ustawy, organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem,
14. **państwie trzecim** – rozumie się przez to państwo nienależące do Unii Europejskiej,
15. **obszarze przetwarzania danych** – należy przez to rozumieć wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe,
16. **wykazie zbiorów** – należy przez to rozumieć wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych,
17. **opisie struktury zbiorów** – należy przez to rozumieć opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi;
18. **opisie przepływu danych** – należy przez to rozumieć opis sposobu przepływu danych pomiędzy poszczególnymi systemami informatycznymi,
19. **środkach technicznych i organizacyjnych** – należy przez to rozumieć środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych.

III. Procedura nadawania uprawnień do przetwarzania danych osobowych.

1. Użytkownikiem systemu informatycznego wykorzystywanego do przetwarzania może być jedynie osoba posiadająca odpowiednie upoważnienie i zarejestrowana w rejestrze użytkowników.

2. Administrator Danych Osobowych udziela użytkownikowi upoważnienia do przetwarzania danych osobowych wg wzoru zamieszczonego w „Polityce bezpieczeństwa przetwarzania danych osobowych w Krzysztof Pakulski - PPHU ALLTERM -".
3. Osobami odpowiedzialnymi za administrację systemem informatycznym są: Administrator Danych Osobowych i wyznaczony przez niego pracownik zwany dalej Administrator Systemu Informatycznego (ASI).
4. Nazwę użytkownika tworzy system na wniosek ASI.
5. Dostęp do systemu informatycznego, służącego do przetwarzania danych osobowych, może uzyskać wyłącznie osoba upoważniona do przetwarzania danych osobowych, zarejestrowana jako użytkownik w tym systemie przez ASI, zgodnie z rejestrem osób upoważnionych od przetwarzania danych osobowych..
6. Rejestracja użytkownika, o którym jest mowa w punkcie 2 wyżej polega na nadaniu identyfikatora i przydzieleniu hasła oraz wprowadzeniu tych danych do bazy użytkowników systemu.
7. Rejestracji i usunięcia użytkownika systemu informatycznego dokonuje operator systemu na wniosek ASI.
8. Usunięcie następuje przez zablokowanie konta użytkownika oraz usunięcie danych użytkownika z bazy użytkowników systemu (wyrejestrowanie trwałe).
9. Czasowe usunięcie (zablokowanie) użytkownika z systemu musi nastąpić w razie nieobecności użytkownika w pracy, trwającej dłużej niż 30 dni kalendarzowych.
10. Przyczyną trwałego wyrejestrowania użytkownika z systemu informatycznego jest rozwiązanie lub wygaśnięcie stosunku pracy lub innego stosunku prawnego, w ramach którego zatrudniony był użytkownik.

IV. Stosowane metody oraz procedury uwierzytelniania i zarządzania.

1. Dostęp do danych osobowych przetwarzanych w systemie informatycznym odbywa się na podstawie uwierzytelnienia, poprzez podanie indywidualnej nazwy (identyfikatora/loginu) i hasła Użytkownika.
2. Celem stosowania identyfikatora (loginu) Użytkownika jest jednoznaczne określenie osoby, która się nim posługuje.
3. Identyfikator Użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie.
4. System informatyczny, w którym przetwarzane są dane osobowe musi automatycznie wymuszać podanie identyfikatora i hasła Użytkownika.
5. Hasło Użytkownika:
   5.1. musi się składać co najmniej z 8 znaków, w tym zawierać małe i wielkie litery oraz cyfry lub znaki specjalne.
   5.2. nie może zawierać znaków następujących po sobie na klawiaturze bądź tych samych liter lub cyfr,
   5.3. nie może zawierać imion, nazwisk, przezwisk, inicjałów, dat, numerów rejestracyjnych samochodów, numerów telefonów i innych kombinacji znaków mogących doprowadzić do łatwego rozszyfrowania go przez osoby nieupoważnione,
   5.4. nie może być zapisywane w systemie w postaci jawnej,
   5.5. nie może być wyświetlane na ekranie komputera w sposób jawny,
   5.6. nie może być ujawnione innej osobie, nawet po utracie ważności,

5.7. musi być zabezpieczone przez Użytkownika przed nieuprawnionym dostępem osób trzecich.
5.8. Hasła nadaje na wniosek Administratora Danych Osobowych administrator sieci informatycznej lub firma, której powierzono obsługę informatyczną Krzysztof Pakulski - PPHU ALLTERM -.

6. Hasła musza być utrzymywane w tajemnicy, co oznacza bezwzględny zakaz udostępniania haseł. Nie należy haseł zapisywać i pozostawiać w widocznym miejscu.
7. Hasła muszą być zmieniane nie rzadziej niż co 30 dni kalendarzowych.

V. Procedury związane z rozpoczęciem, zawieszeniem i zakończeniem pracy przez użytkowników.

1. Przed rozpoczęciem pracy w systemie informatycznym użytkownik zobowiązany jest do:
1.1. zalogowania się do systemu z wykorzystaniem zastrzeżonych tylko dla siebie: identyfikatora i hasła w sposób uniemożliwiający ich ujawnienie osobom postronnym,
1.2. wprowadzając obowiązany jest uczynić to w taki sposób, aby utrudnić jego ewentualne odczytanie,
1.3. sprawdzenia prawidłowości funkcjonowania sprzętu komputerowego i systemów, na swoim stanowisku pracy,
1.4. w razie stwierdzenia nieprawidłowości, do powiadomienia o tym fakcie ASI i Inspektora Danych Osobowych.
1.5. w razie stwierdzenia naruszenia zabezpieczenia systemu informatycznego lub stanu wskazującego na istnienie takiej możliwości, do podjęcia odpowiednich kroków stosownie do zasad postępowania w sytuacji naruszenia zabezpieczenia danych osobowych.
2. W sytuacji gdy użytkownik zmuszony jest opuścić stanowisko komputerowe poza zajmowane pomieszczenie lub kiedy wgląd do danych wyświetlanych na monitorze może mieć nieuprawniona osoba, należy skorzystać z mechanizmu czasowej blokady dostępu do komputera poprzez uruchomienie wygaszacza ekranu z hasłem. Hasło wygaszacza ekranu powinno być zbieżne z hasłem logowania do systemu.
3. Na pulpicie należy mieć foldery, w których powinny być umieszczane pliki z danymi uniemożliwiając ich odczyt bezpośrednio z pulpitu.
4. Zakończenie pracy. Przed zakończeniem pracy należy zwrócić uwagę, aby wylogować się z używanych programów i prawidłowo je zakończyć. Dopiero tak przygotowany system można zamknąć i wyłączyć komputer.
5. Użytkownik kończący pracę powinien sprawdzić, czy wszystkie elektroniczne nośniki informacji lub wydruki i dokumenty zawierające dane osobowe zostały zabezpieczone przed dostępem osób nieupoważnionych.
6. Osoba opuszająca pomieszczenie jako ostatnia powinna zamknąć okna oraz zamknąć drzwi od pomieszczenia na klucz.

VI. Sposób, miejsce i procedury tworzenia kopii zapasowych zbiorów danych.

1. Czynności związane z tworzeniem kopii zapasowych, ich testowaniem oraz likwidacją nośników są prowadzone przez ASI Krzysztof Pakulski-TERM/SARBUZ-PL bądź w przypadku jego braku, na zasadzie umowy powierzenia z zachowaniem procedur określonych w RODO przez firmę zewnętrzną.

2. Elektroniczne nośniki informacji zawierające dane osobowe przechowuje się na dyskach twardych komputerów lub dyskach serwerów w zależności od zastosowanego systemu.
   Stacje robocze, na których są przechowywane dane osobowe wyznacza ASI.
3. W przypadku serwerów ich ochrona polega na wyizolowaniu urządzeń w odrębnych, zamkniętych pomieszczeniach, do których dostęp posiada administrator sieci informatycznej.
4. Metody tworzenia kopii.
   4.1. W systemach informatycznych, które opierają się o pracę w technologii klient-serwer kopie bezpieczeństwa wykonuje się po stronie serwera.
   4.2. Do indywidualnych systemów informatycznych na pojedynczych komputerach, lub w małym otoczeniu sieciowym, kopie wykonuje się na komputerze, na którym zainstalowany jest dany program a także na serwerze.
5. Niedopuszczalne jest przechowywanie pojedynczej kopii danych wyłącznie na tym samym komputerze, w którym pracuje lub jest zainstalowane oprogramowanie (serwer). W związku z tym wykonuje się kopie na nośnikach zewnętrznych. Kopie oprogramowania wykonuje się dla każdego egzemplarza posiadanego systemu.
6. Cykliczność wykonywania kopii bezpieczeństwa backup opiera się o następujący schemat roczny – kopie dzienne, kopie tygodniowe, kopie miesięczne, kopie roczne. W celu zapewnienia pewności co do poprawności wykonywanych kopii bezpieczeństwa należy poddać testowi cyklicznie wybraną kopię.
7. Nośniki elektroniczne przeznaczone do przechowywania danych osobowych powinny się charakteryzować odpowiednią trwałością zapisu, zależną od planowanego okresu przechowywania na nich danych.
8. Likwidacja nośników zawierających kopie. Nośniki zawierające nieaktualne kopie danych likwiduje się. W przypadku nośników takich jak pendrive, dyski komputerów likwidacja polega na ich fizycznym zniszczeniu w taki sposób, aby nie można było odczytać ich zawartości.
9. Kopie zapasowe i elektroniczne nośniki informacji przechowywane są w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem, a kopie awaryjne należy bezzwłocznie usuwać po ustaniu ich użyteczności w przypadku lokalnego przetwarzania danych osobowych na stacjach roboczych.
10. Kopie zapasowe i elektroniczne nośniki informacji przechowywane są przez okres, w którym istnieją przesłanki do ich przetwarzania. Po ustaniu przesłanek, o których mowa w zdaniu pierwszym, dane znajdujące się na kopiach zapasowych muszą zostać usunięte w sposób uniemożliwiający ich odtworzenie.

VII. Sposób zabezpieczenia systemu informatycznego przed nieuprawnionym dostępem.

1. Obszary systemu informatycznego narażone na ingerencję wirusów komputerowych oraz wszelkiego innego oprogramowania. Na działanie wirusów komputerowych narażone są wszystkie stanowiska komputerowe, które są przyłączone do sieci komputerowej oraz te, które są wyposażone w czytniki nośników elektronicznych takich jak nośniki danych umożliwiające wprowadzanie danych lub programów z zewnątrz.
2. Źródła przedostawania się szkodliwego oprogramowania do systemów Do źródeł szkodliwego oprogramowania można zaliczyć:
   2.1. pliki zapisane na nośnikach elektronicznych,
   2.2. pliki przesyłane za pomocą poczty elektronicznej,
   2.3. pliki pobierane ze stron internetowych,
   2.4. pliki prywatne użytkowników.

3. Sieć komputerowa, serwery oraz komputery pracujące w sieci muszą podlegać centralnie ochronie antywirusowej.
4. Za legalność oprogramowania odpowiada Administrator Danych oraz Firma, której powierzono przetwarzanie danych.
5. System informatyczny, przetwarzający dane osobowe posiada mechanizm uwierzytelniający użytkownika, wykorzystujący identyfikator i hasło. Posiadane mechanizmy, pozwalają na określenie uprawnień użytkownika do korzystania z przetwarzanych informacji (np. prawo do odczytu danych, modyfikacji istniejących danych, tworzenia nowych danych, usuwania danych).
6. System informatyczny, przetwarzający dane osobowe, posiada mechanizmy, pozwalające na odnotowanie faktu wykonania operacji na danych. W szczególności zapis ten powinien obejmować: rozpoczęcie i zakończenie pracy przez użytkownika systemu, operacje wykonywane na przetwarzanych danych, a w szczególności ich dodanie, modyfikację oraz usunięcie, przesyłanie za pośrednictwem systemu danych osobowych przetwarzanych w systemie informatycznym innym podmiotom niebędącym właścicielem ani współwłaścicielem systemu, nieudane próby dostępu do systemu informatycznego, przetwarzającego dane osobowe oraz nieudane próby wykonania operacji na danych osobowych, błędy w działaniu systemu informatycznego podczas pracy danego użytkownika.
7. Zapis działań użytkownika uwzględnia: identyfikator użytkownika, datę i czas, w którym zdarzenie miało miejsce, rodzaj zdarzenia, określenie informacji, których zdarzenie dotyczy (identyfikatory rekordów).
8. System informatyczny zapewnia zapis faktu przekazania danych osobowych z uwzględnieniem: identyfikatora osoby, której dane dotyczą, osoby przesyłającej dane, odbiorcy danych, zakresu przekazanych danych osobowych, daty operacji, sposobu przekazania danych.

VIII. Poziom bezpieczeństwa.

1. Na wszystkich stacjach roboczych, na których przetwarzane są dane osobowe wprowadza się wysoki poziom zabezpieczeń.
2. Na każdym stanowisku komputerowym musi być zainstalowane oprogramowanie antywirusowe z włączoną ochroną antywirusową i antyspamowe.
3. System informatyczny musi być chroniony równolegle na wielu poziomach m.in. poprzez stosowanie oprogramowania antywirusowego, systemów typu firewall, odpowiednią konfigurację systemu aktualizacji systemu operacyjnego oraz realizację kopii bezpieczeństwa.
4. Przesyłanie danych poza obszar przetwarzania: zabezpiecza się w sposób zapewniający poufność i integralność tych danych, w szczególności poprzez login hasło dostępu.
5. Stosuje się następujące sposoby kryptograficznej ochrony danych:
   a) przy przesyłaniu danych za pomocą poczty elektronicznej stosuje się POP – 9 tunelowanie, szyfrowanie połączenia
   b) przy przesyłaniu danych pracowników, niezbędnych do wykonania przelewów wynagrodzeń, używa się bezpiecznych stron https://.
   c) przy przesyłaniu danych z programu Płatnik stosuje się łącze szyfrowane za pomocą certyfikatu kwalifikowanego.
6. W celu zapewnienia ochrony systemu informatycznego może być stosowany monitoring wykorzystania infrastruktury informatycznej, w szczególności obejmujący następujące elementy:
   6.1. analizę oprogramowania wykorzystanego na stacjach roboczych,

6.2. analizę stacji roboczych pod względem wykorzystania nielegalnego oprogramowania, plików multimedialnych oraz innych elementów naruszających prawo autorskie,
6.3. analizę godzin pracy na stanowiskach komputerowych,
6.4. analizę dostępów (autoryzowanych oraz nieautoryzowanych),
6.5. analizę ruchu sieciowego pod względem komunikacji, szkodliwej dla bezpieczeństwa danych przetwarzanych w systemie.

7. Monitoring bezpieczeństwa musi odbywać się z zachowaniem obowiązującego prawa.
8. Postępowanie w przypadku naruszenia ochrony danych osobowych opisane są w Polityce Bezpieczeństwa.
9. Zabezpieczenie integralności systemu informatycznego realizowane jest również poprzez zakaz:
   9.1. wysyłania masowej poczty kierowanej do losowych odbiorców (spam),
   9.2. przechowywania w systemie informatycznym treści łamiących prawo autorskie (filmy, utwory muzyczne lub oprogramowanie),
   9.3. nieuzasadnionego wynoszenia lub wysyłania danych osobowych poza obszar przetwarzania danych,
   9.4. instalowania przez Użytkownika oprogramowania na sprzęcie komputerowym, które nie uzyskało akceptacji ASI,
   9.5. wykorzystywania przeglądarek internetowych, które nie uzyskały akceptacji ASI oraz odwiedzania witryn internetowych zawierających potencjalnie niebezpieczne treści,
   9.6. podłączania innych urządzeń niż teleinformatyczne do wydzielonej instalacji elektrycznej (gniazdka w kolorze czerwonym),
   9.7. przemieszczania sprzętu komputerowego do innej lokalizacji (pokoju) lub zmiany Użytkownika bez uzgodnienia z ASI,
   9.8. fizycznego ingerowania w konfigurację sprzętową urządzeń,
   9.9. podejmowania prób wykorzystania obcego konta, uruchamiania aplikacji deszyfrujących hasła, prowadzenia działań mających na celu podsłuchanie lub przechwycenie informacji przepływających w systemach informatycznych.

IX. Zasady stosowania bezpiecznych technologii i dobrych praktyk.

1. Zdalny dostęp do sieci jest możliwy tylko poprzez technologie zapewniające szyfrowanie całej transmisji algorytmami powszechnie uznanymi za silne np.: VPN, IPSEC, SSL.
2. Sieci WI-FI współpracujące z siecią LAN ENEA i Spółek powinny mieć zaimplementowany standard szyfrowania WPA2 i algorytm AES oraz protokół sieciowy realizujący zadanie centralnego uwierzytelniania i autoryzacji np.: RADIUS lub inny o porównywalnej funkcjonalności.
3. Wszystkie fizyczne elementy rozdzielające i sterując sygnał IT (Routery, switche, firewall) powinny być umiejscowione w zamkniętych szafach dystrybucyjnych z dostępem jedynie dla upoważnionych osób odpowiedzialnych za zarządzanie siecią LAN.
4. Wszystkie fizyczne elementy rozdzielające i sterując sygnał IT (Routery, switche, firewall) oraz powinny być zunifikowane i mieć możliwości zaimplementowania rozwiązań zabezpieczających i usług zdalnego zarządzania.
5. Wszystkie punkty postępowe do sieci LAN powinny być uwierzytelniane i autoryzowane w systemie centralnym np.: RADIUS lub inny o porównywalnej funkcjonalności.

6. Użytkownicy stacji roboczych nie mogą mieć uprawnień administracyjnych do instalacji oprogramowania i zarządzania stacją. W uzasadnionych przypadkach możliwe są odstępstwa od tej zasady za zgodą Administratora.
7. Węzeł dystrybucji sygnału internetowego powinien umożliwiać zbieranie danych o aktywności użytkowników oraz umożliwiać historyczną analizę logów do celów kontroli przez Zamawiającego lub udzielania odpowiedzi dla organów ścigania przestępstw elektronicznych. Z tego powodu wykluczone jest stosowanie kont wspólnych dla użytkowników.
8. Do czyszczenia danych komputerów przeznaczonych do odsprzedaży lub utylizacji, należy używać program umożliwiający niskopoziomowe formatowanie dysków twardych.
9. Do aktualizacji standardowego oprogramowania stacji roboczych i serwerów należy stosować metody zautomatyzowane np. serwer WSUS (Windows Server Update Services).

X. Procedura w przypadku stwierdzenia naruszenia zasad bezpieczeństwa systemu informatycznego.

1. W przypadku stwierdzenia przez Użytkownika naruszenia zabezpieczeń systemu informatycznego przez osoby nieuprawnione, jest on zobowiązany niezwłocznie poinformować o tym fakcie ASI.
2. ASI jest zobowiązany niezwłocznie podjąć czynności zmierzające do ustalenia przyczyn naruszeń zasad bezpieczeństwa i zastosować środki uniemożliwiające ich naruszanie w przyszłości oraz bezzwłocznie powiadomić o tym fakcie Inspektora Danych Osobowych.
3. W przypadku wykrycia zagrożenia automatycznym działaniem, możliwe jest zablokowanie pracy w systemie do chwili podjęcia decyzji o sposobie postępowania.
4. W celu minimalizacji zagrożeń dąży się, w miarę możliwości organizacyjnych, do maksymalnej unifikacji sprzętu, stosowanego oprogramowania, konfiguracji sprzętu i oprogramowania, a także rozwiązań organizacyjnych.

XI. Korzystanie z firm zewnętrznych na zasadzie powierzenia przetwarzania danych.

1. W przypadku podpisania Umowy powierzenia przetwarzania danych osobowych oraz obsługi wspomagania w zakresie infrastruktury informatycznej z podmiotem zewnętrznym, musi on zagwarantować spełnienie wszystkich procedur zawartych w powyższej Instrukcji.