Załącznik nr 2

do Zarządzenia nr 4/2021
Rektora ChAT w Warszawie
z dnia 15.02.2021 r.

Instrukcja zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Chrześcijańskiej Akademii Teologicznej w Warszawie

Warszawa, 2021

Spis treści

I. Słownik pojęć.

§ 1

Podstawowe pojęcia i definicje.

1. **ADO** - Administrator Danych Osobowych – Chrześcijańska Akademia Teologiczna w Warszawie reprezentowana przez Rektora.
2. **ASI** - Administrator Systemów Informatycznych wyznaczona osoba przez ADO, odpowiadającą za poszczególne systemy informatyczne służące do przetwarzania danych, w tym odpowiedzialną za bezpieczeństwo informacji przetwarzanych w systemie, w szczególności za przeciwdziałanie dostępowi osób trzecich do systemu oraz podejmowanie odpowiednich działań.
3. **AZ** - Administrator zasobów wyznaczony pracownik, który jest odpowiedzialny za prawidłowe zabezpieczenie sprzętu służącego do przetwarzania danych osobowych w poszczególnych jednostkach Akademii.
4. **Akademia** (CHAT) – należy przez to rozumieć Chrześcijańską Akademię Teologiczną w Warszawie.
5. **Dane osobowe** - informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, dane dotyczące zdrowia, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.
6. **Hasło** - ciąg znaków literowych, cyfrowych lub innych, znanych jedynie użytkownikowi systemu informatycznego.
7. **Identyfikator** – należy przez to rozumieć ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący użytkownika systemu informatycznego.
8. **IOD** - Inspektor Ochrony Danych - wyznaczona osoba w Akademii pełniąca nadzór nad ochroną danych osobowych oraz monitorująca wypełnienie mających zastosowanie obowiązków wynikających z regulacji prawnych w obszarze danych osobowych w Akademii.
9. **Instrukcja** – niniejszą Instrukcję zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Akademii stanowiąca załącznik nr 2 do zarządzenia.
10. **Polityka Bezpieczeństwa** – Polityka Bezpieczeństwa w zakresie ochrony danych osobowych w Akademii stanowiąca załącznik nr 1 do zarządzenia.
11. **Przetwarzanie** - oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.
12. **RODO** - 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.
13. **System informatyczny** - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
14. **Uwierzytelnianie** – działanie, którego celem jest weryfikacja deklarowanej tożsamości użytkownika.
15. **Użytkownik** – osoba posiadająca upoważnienie do przetwarzania danych osobowych w zbiorach tradycyjnych lub/i w systemach informatycznych, w zakresie wskazanym w upoważnieniu, może nim być pracownik lub osoba wykonująca pracę na podstawie umowy cywilnoprawnej.
16. **Zarządzenie** – należy przez to rozumieć zarządzenie Rektora w sprawie wprowadzenia Polityki bezpieczeństwa w zakresie ochrony danych osobowych w Akademii.

II. Postanowienia ogólne.

§ 2

Instrukcja określa zasady zarządzania każdym systemem informatycznym służącym do przetwarzania danych osobowych w Akademii

§ 3

Celem Instrukcji jest określenie i zastosowanie w każdym systemie informatycznym Akademii środków technicznych i zabezpieczeń logicznych, zapewniających danym osobowym bezpieczeństwo i ochronę adekwatną do rodzaju danych oraz występujących zagrożeń. Cel Instrukcji jest realizowany poprzez określenie:

1) mechanizmów ochrony przed awarią zasilania,
2) procedur nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności,
3) procedur rozpoczęcia, zawieszenia i zakończenia pracy przeznaczonych dla użytkowników systemu informatycznego,
4) procedur tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania,
5) procedur wykonywania przeglądów i konserwacji systemów informatycznych oraz nośników informacji służących do przetwarzania danych,
6) sposobu zabezpieczenia systemu informatycznego przed działalnością „oprogramowania złośliwego”,
7) sposobu, miejsca i okresu przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych, o których mowa w pkt 4,
8) stosowanych metod i środków uwierzytelnienia oraz procedur związanych z ich zarządzaniem i użytkowaniem.

§ 4

Każdy użytkownik systemu informatycznego jest zobowiązany do zapoznania się i stosowania niniejszej Instrukcji.

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

§ 5

1. Do przetwarzania danych osobowych w systemie informatycznym może zostać dopuszczona wyłącznie osoba posiadająca upoważnienie do przetwarzania danych osobowych nadane przez uprawnione osoby na zasadach określonych w Polityce Bezpieczeństwa.
2. Zakres uprawnień użytkownika w systemie informatycznym jest przyznawany na zasadach określonych w odrębnych procedurach, które są opracowywane i bieżąco aktualizowane przez ASI. Uprawnienia użytkownika w systemach informatycznych, udostępnianych przez instytucje zewnętrzne, przyznawane są przez ASI na zasadach określonych przez te instytucje a użytkownicy są zobowiązani do stosowania, oprócz zasad opisanych w niniejszej Instrukcji, zasad określonych w polityce bezpieczeństwa instytucji udostepniającej system.
3. Każdy system informatyczny Akademii, w którym są przetwarzane dane osobowe, powinien umożliwiać utworzenie co najmniej dwóch klas użytkowników:
   1) ASI – osoby zarządzające systemem informatycznym upoważnione do rejestracji użytkowników; do każdego systemu informatycznego Akademii, w którym są przetwarzane dane osobowe, musi być przyporządkowany co najmniej jeden ASI,
   2) użytkownicy – pozostałe osoby korzystające z systemu informatycznego, które uzyskały uprawnienia do korzystania z systemu; użytkownicy systemu informatycznego są zobowiązani do zastosowania się do wszystkich wskazówek i uwag ASI, w tym do respektowania nakazów i zakazów nałożonych przez ASI w zakresie użytkowania systemu informatycznego.
4. Rejestracji użytkownika w systemie informatycznym dokonuje ASI.

5. Zmianę uprawnień dostępu do danych osobowych przetwarzanych w systemie informatycznym przeprowadza się na zasadach przewidzianych dla ich nadawania.
6. W przypadku nadania lub zmiany uprawnień ASI informuje użytkownika o założonym koncie i nadanych uprawnieniach lub o zmianie zakresu uprawnień.
7. Wyrejestrowanie użytkownika z systemu informatycznego następuje, gdy:
   1) rozwiązano z użytkownikiem stosunek pracy,
   2) zakres obowiązków służbowych użytkownika uległ zmianie, która spowodowała utratę potrzeby korzystania z systemu informatycznego, w którym są przetwarzane dane osobowe,
   3) użytkownik spowodował swoim celowym działaniem incydent naruszający bezpieczeństwo systemu informatycznego lub przetwarzanych w nim danych osobowych,
   4) istnieją uzasadnione przesłanki, że korzystanie przez użytkownika z systemu informatycznego, w którym są przetwarzane dane osobowe, wiąże się z poważnym ryzykiem utraty poufności, integralności lub rozliczalności tych danych.
8. Wyrejestrowanie użytkownika z systemu informatycznego oraz zawieszenie uprawnień użytkownika w systemie informatycznym w przypadku jego długotrwałej nieobecności następuje na podstawie informacji przekazanej przez Dział Kadr do ASI.

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

§ 6

1. ADO dopuszcza możliwość przetwarzania danych osobowych w systemie informatycznym po zastosowaniu zabezpieczeń technicznych zapewniających poufność, integralność i rozliczalność przetwarzanych danych.
2. Każdy system informatyczny, w którym są przetwarzane dane osobowe, jest wyposażony w mechanizmy uwierzytelnienia użytkownika oraz kontroli dostępu. Za właściwe funkcjonowanie w systemie informatycznym tych mechanizmów odpowiada ASI.
3. Elementem mechanizmu uwierzytelnienia dostępu użytkownika do systemu informatycznego jest identyfikator, który nie powinien być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego nie może być przydzielany innej osobie.
4. Elementem mechanizmu uwierzytelnienia dostępu użytkownika do systemu informatycznego jest hasło, które:
   1) jest przekazywane użytkownikowi w formie pozwalającej na zachowanie poufności,
   2) jest wyświetlane na ekranie monitora w formie niejawnej,
   3) powinno zawierać minimum 8 znaków,
   4) powinno być zmieniane, nie rzadziej niż co 90 dni, chyba że ASI w porozumieniu z IOD określą inną procedurę w tym zakresie,
   5) powinno zawierać znaki specjalne a także znaki małe i duże,
   6) nie może zawierać znaków diakrycznych,
   7) nie może zawierać żadnych informacji, które kojarzą się z użytkownikiem, np. imienia, nazwiska, inicjałów, marki lub nr rejestracyjnego samochodu itp.,
   8) nie może być zapisywane w miejscu dostępnym dla osób nieuprawnionych,
   9) może być zmienione wyłącznie przez użytkownika bądź ASI,
   10) powinno być zmienione po pierwszym zalogowaniu.
5. Za utworzenie i przydzielenie identyfikatora i hasła użytkownikowi, który po raz pierwszy korzysta z systemu informatycznego, odpowiada ASI.
6. Uwierzytelnienie użytkownika w systemie informatycznym następuje poprzez podanie identyfikatora oraz hasła. Użytkownik nie może udostępnić osobom nieuprawnionym swojego komputera po dokonaniu uwierzytelnienia w systemie informatycznym.
7. Użytkownik ponosi odpowiedzialność za czynności wykonywane w systemie informatycznym po dokonaniu uwierzytelnienia.
8. Przed zakończeniem pracy w systemie użytkownik jest obowiązany zamknąć używane pliki lub katalogi, a następnie wyłączyć komputer.

§ 7

1. ASI posiadają indywidualne konta administracyjne.
2. Identyfikatory i hasła ASI powinny być przechowywane w opieczętowanej ciemnej kopercie w sejfie lub metalowej szafie, do której dostęp mają wyłącznie upoważnione osoby.
3. W przypadku konieczności awaryjnego użycia identyfikatora i hasła należącego do ASI konieczny jest wpis ilustrujący zaistniałą sytuację w „dzienniku haseł" znajdującym się w sejfie lub metalowej szafie wraz z kopertą, w której znajdują się identyfikatory i hasła ASI. Wpis powinien zawierać następujące informacje:
   1) imię i nazwisko oraz stanowisko osoby umożliwiającej dostęp do sejfu lub szafy, w której znajdują się identyfikatory i hasła,
   2) imię i nazwisko oraz stanowisko osoby, która pobiera identyfikator i hasło,
   3) krótki opis sytuacji, która zmusiła do awaryjnego wykorzystania identyfikatora i hasła.
4. O konieczności i okolicznościach awaryjnego użycia identyfikatora i hasła niezwłocznie powiadamia się IOD.

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

§ 8

1. Rozpoczęcie pracy w systemie informatycznym następuje poprzez:
   1) przygotowanie stanowiska komputerowego, m.in. sprawdzenie, czy monitor komputera jest ustawiony w sposób uniemożliwiający osobom postronnym wgląd w dane widoczne na ekranie,
   2) uruchomienie komputera,
   3) uwierzytelnienie w systemie operacyjnym,
   4) uwierzytelnienie w systemie informatycznym, w którym są przetwarzane dane osobowe poprzez wpisanie identyfikatora i hasła.
2. Użytkownik niezwłocznie powiadamia ASI lub AZ w przypadku, gdy:
   1) nie może zalogować się na swoje konto,
   2) powziął podejrzenie co do ingerencji w przetwarzane dane osobowe lub użytkowane narzędzia programowe lub sprzętowe,
   3) sposób działania systemu informatycznego odbiega od normalnego stanu,
   4) posiada dostęp do zasobów, do których nie powinien mieć uprawnień.
   5) nie posiada dostępu do zasobów, do których ma uprawnienia.
3. W przypadku zaistnienia sytuacji opisywanej w ust. 2 użytkownik jest zobowiązany do niedokonywania jakichkolwiek operacji aż do momentu przybycia ASI bądź AZ.

§ 9

1. Użytkownik ma obowiązek wylogowania się z/lub zablokowania systemu informatycznego, w przypadku chwilowej nieobecności w pomieszczeniu, w którym znajduje się jego stanowisko pracy.
2. W przypadku braku aktywności użytkownika podczas pracy na komputerze, na którym są przetwarzane dane osobowe w systemie informatycznym, po upływie 5 minut automatycznie powinien zostać uruchomiony wygaszacz ekranu zabezpieczony hasłem.

§ 10

1. Zakończenie pracy użytkownika w systemie informatycznym następuje poprzez:
   1) wylogowanie się z systemu informatycznego,
   2) zamknięcie systemu informatycznego.
2. Użytkownik nie powinien opuszczać stanowiska pracy, aż do momentu wyłączenia się komputera.
3. Użytkownik opuszczając stanowisko pracy powinien sprawdzić, czy nie pozostawił zewnętrznych nośników elektronicznych podłączonych do sprzętu komputerowego.

VI. Procedury tworzenie kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania.

§ 11

1. Dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przed ich utratą poprzez tworzenie kopii zapasowych. Za proces tworzenia kopii zapasowych odpowiada ASI. Kopie zapasowe tworzy się z wykorzystaniem przeznaczonych do tego celu urządzeń wchodzących w skład systemu informatycznego. Wszelkie kopie zapasowe są sporządzane automatycznie lub wywoływane w sposób ręczny. Kopie zapasowe są wykonywane na dedykowanych nośnikach w co najmniej dwóch egzemplarzach.
2. Kopie zapasowe danych osobowych przetwarzanych w systemie informatycznym są tworzone, o ile jest to technicznie możliwe, w taki sposób, że pełną kopię zapasową konfiguracji systemu i danych w nim przetwarzanych, wykonuje się co najmniej raz w miesiącu (codziennie wykonuje się kopię przyrostową lub różnicową).
3. Nie rzadziej niż raz w roku są wykonywane testy odtworzeniowe kopii zapasowych. Testy obejmują sprawdzenie możliwości odtworzenia przechowywanych danych osobowych oraz danych konfiguracyjnych. Testy są nadzorowane przez Głównego specjalistę ds. informatyki, który sporządza i przekazuje IOD notatkę potwierdzającą wykonanie testów, uwzględniającą:
   1) imiona i nazwiska osób przeprowadzających test,
   2) powodzenie lub niepowodzenie odtworzenia danych z kopii zapasowej,
   3) czas potrzebny na odtworzenie danych,
   4) problemy, które pojawiły się w czasie wykonywania testu.
5. Negatywne wyniki testu lub zaistnienie problemów w trakcie odtwarzania danych stanowi podstawę do zmiany sposobu tworzenia kopii zapasowych w Akademii lub zmiany technologii wykorzystywanej do tworzenia kopii. W przypadku wystąpienia negatywnych wyników lub problemów, IOD w porozumieniu z Kierownikiem Działu Zabezpieczenia Informatycznego przeprowadza analizę przyczyn i podejmuje działania w celu zmniejszenia ryzyka utraty danych poprzez brak możliwości odtworzenia kopii.

VII. Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania.

§ 12

1. Kopie zapasowe tworzy się według procedur określonych przez ASI.
2. Kopie zapasowe przechowuje przez czas określony odrębnymi przepisami.
3. Kopie zapasowe usuwa się niezwłocznie po ustaniu ich użyteczności.
4. Nośniki, na których utrwalono kopie zapasowe, przeznaczone do likwidacji pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie. Z przeprowadzonej likwidacji tych nośników sporządza się protokół.

§ 13

1. Nośniki elektroniczne zawierające dane osobowe (np. pendrive, płyty CD/DVD/BD, dyski zewnętrzne), nie będące kopiami zapasowymi bądź dyskami twardymi, przechowuje się w zamykanych szafach lub biurkach.
2. Użytkownicy nie mogą wynosić poza obszar przetwarzania danych osobowych w Akademii nośników, o których jest mowa w ust 1, chyba że jest to niezbędne do wykonania określonych czynności służbowych.
3. Dane osobowe zawarte na nośnikach, o których jest mowa w ust. 1, powinny być zabezpieczone kryptograficznie.
4. Nośniki elektroniczne zawierające dane osobowe przeznaczone do ponownego wykorzystania lub przekazania innemu podmiotowi należy pozbawić zapisu w sposób gwarantujący trwałe usunięcie danych. Jeżeli nie istnieje możliwość trwałego usunięcia danych z nośnika należy go fizycznie zniszczyć do stanu uniemożliwiającego jego rekonstrukcję i odzyskanie danych.

5. Nośniki elektroniczne zawierające dane osobowe przeznaczone do likwidacji pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie. Z przeprowadzonej likwidacji nośników elektronicznych sporządza się protokół.
6. Nośniki elektroniczne są przechowywane przez czas ich użyteczności.

VIII. Sposób zabezpieczenia systemu informatycznego przed działalnością „oprogramowania złośliwego".

§ 14

1. W związku z istnieniem zagrożenia dla zbiorów danych osobowych ze strony „oprogramowania złośliwego" (w tym w szczególności wirusów komputerowych), którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego, konieczna jest ochrona sieci komputerowej i stanowisk komputerowych.
2. W celu ochrony przed „oprogramowaniem złośliwym" stosuje się dwa poziomów zabezpieczeń:
   1) zabezpieczenie pierwszego stopnia – obejmujące zabezpieczenie poczty elektronicznej, oraz innych usług umożliwiających przesyłanie plików zawierających „oprogramowanie złośliwe",
   2) zabezpieczenie drugiego stopnia – obejmujące wszystkie komputery, na których są przetwarzane dane osobowe, w postaci oprogramowania antywirusowego skanującego lokalny system w poszukiwaniu „oprogramowania złośliwego".
3. Oprogramowanie antywirusowe jest instalowane centralnie na serwerze oraz na wszystkich stanowiskach komputerowych podłączonych do sieci i powinno cechować się możliwością:
   1) analizy danych wprowadzanych do systemu informatycznego za pośrednictwem sieci informatycznej poprzez monitorowanie ruchu sieciowego,
   2) przeprowadzania analizy wybranych katalogów z zapisanymi plikami pod kątem zainfekowania „oprogramowaniem złośliwym",
   3) analizy przesyłanych wiadomości e-mail,
   4) analizy nośników danych używanych do przenoszenia danych do systemu informatycznego,
   5) lokalnego a także centralnego zapisu wyników skanowania systemu informatycznego, w szczególności faktu wykrycia „oprogramowania złośliwego".
4. Za instalację, konfigurację i analizę raportów oprogramowania zabezpieczającego system informatyczny przed „oprogramowaniem złośliwym" odpowiada ASI.
5. Aktualizacja oprogramowania antywirusowego odbywa się nie rzadziej niż raz w tygodniu, w sposób automatyczny dla wszystkich komputerów posiadających dostęp do sieci.
6. Instalacja oprogramowania antywirusowego oraz jego aktualizacja na komputerach niepodłączonych do sieci, odbywa się nie rzadziej niż raz w tygodniu i jest wykonywana przy zastosowaniu nośników zewnętrznych przez właściwego AZ.
7. W przypadku, gdy użytkownik zauważy komunikat oprogramowania antywirusowego wskazujący na zaistnienie zagrożenia lub rozpozna tego typu zagrożenie, jest zobowiązany zaprzestać jakichkolwiek czynności w systemie informatycznym i niezwłocznie skontaktować się z AZ.
8. Administrator zasobów powinien w szczególności:
   1) usunąć źródło infekcji, jeżeli czynność ta nie została automatycznie wykonana przez program antywirusowy,
   2) przeskanować cały system w poszukiwaniu „oprogramowania złośliwego",
   3) określić przyczynę infekcji i podjąć działania zabezpieczające przed podobnymi sytuacjami w przyszłości.
9. W celu zminimalizowania zagrożeń ze strony „oprogramowania złośliwego" i „ataków z zewnątrz" użytkownikom zabrania się w szczególności:
   1) wyłączania, blokowania, odinstalowywania programów zabezpieczających system informatyczny przed „oprogramowaniem złośliwym" oraz nieautoryzowanym dostępem do jego zasobów,
   2) korzystania z komunikatorów internetowych, chyba że AZ, z uwagi na szczególne okoliczności, wyrazi na to zgodę,
   3) korzystania ze stron internetowych zwiększających ryzyko zainfekowania systemu informatycznego „oprogramowaniem złośliwym",
   4) pobierania z sieci, kopiowania, przechowywania lub rozprowadzania oprogramowania, które nie zostało zweryfikowane przez właściwego AZ,
   5) korzystania z prywatnej poczty elektronicznej w celach służbowych.

IX. Ochrona przed awarią zasilania.

§ 15

1. System informatyczny, w którym są przetwarzane dane osobowe, posiada mechanizmy pozwalające zabezpieczyć te dane przed ich utratą lub nieautoryzowaną zmianą spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.
2. Urządzenia podtrzymujące zasilanie stosuje się w celu umożliwienia poprawnego zapisania danych i wylogowania się użytkownika z systemu informatycznego.

X. Procedury wykonywania przeglądów i konserwacji systemów informatycznych oraz nośników informacji służących do przetwarzania danych.

§ 16

1. Wszelkie prace związane z naprawą i konserwacją systemu informatycznego i nośników danych służących do przetwarzania danych osobowych mogą być wykonywane wyłącznie przez właściwych ASI i AZ, z zastrzeżeniem ust. 2.
2. W przypadku konieczności wykonania prac serwisowych lub naprawczych przez osobę spoza Akademii, należy ją ściśle nadzorować podczas wykonywanej pracy. Za nadzór nad ww. osobą odpowiada właściwy ASI lub AZ.
3. W przypadku naprawy poza Akademią nośników elektronicznych, na których są zapisane dane osobowe, po zabezpieczeniu danych, należy je trwale usunąć z dysku. Gdy nie ma możliwości usunięcia danych naprawa powinna być nadzorowana przez osobę upoważnioną przez Akademię.

§ 17

1. Aktualizacja systemu informatycznego odbywa się w oparciu o zalecenia producentów oraz powinna zostać poprzedzona dokładną analizą w kwestii stabilności i bezpieczeństwa nowych wersji.
2. Za prawidłowy przebieg przeglądów systemu informatycznego i jego konserwację odpowiada ASI.
3. Nieprawidłowości w działaniu systemu informatycznego są niezwłocznie usuwane przez ASI, a ich przyczyny dokładnie analizowane. W przypadku podejrzenia ingerencji „osób z zewnątrz" wpływającej na funkcjonowanie systemu informatycznego, należy niezwłocznie powiadomić IOD o możliwości zaistnienia takiej sytuacji.
4. Zmiana konfiguracji sprzętu komputerowego, na którym znajdują się dane osobowe lub zmiana jego lokalizacji, może być dokonana tylko za wiedzą i zgodą AZ.

XI. Przepisy końcowe.

§ 18

Wszelkie przypadki naruszenia niniejszej Instrukcji należy niezwłocznie zgłaszać IOD.