**INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM**

**SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH**

**W „STOWARZYSZENIU PRZYJACIÓŁ OLIMPIADY ARTYSTYCZNEJ”**

**I – Część ogólna**

**§ 1**

Zgodnie z art. 39a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 1997 Nr 133 poz. 883 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), ustanawia się „Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych”.

**§ 2**

Ilekroć w niniejszym dokumencie jest mowa o:

1. ustawie – należy przez to rozumieć ustawę, o której mowa w § 1 niniejszej części
2. rozporządzeniu – należy przez to rozumieć rozporządzenie, o którym mowa   
   w § 1 niniejszej części
3. jednostce organizacyjnej – należy przez to rozumiećStowarzyszenie Przyjaciół Olimpiady Artystycznej, posługujące się numerem KRS: 204829, jako Administratora Danych Osobowych (ADO) reprezentowanego przez zarząd.
4. ASI – należy przez to rozumieć Administratora Systemu Informatycznego w rozumieniu § 3 niniejszej części
5. Instrukcji – należy przez to rozumieć niniejszy dokument
6. Polityce Bezpieczeństwa – należy przez to rozumieć przyjęty do stosowania w jednostce organizacyjnej dokument zatytułowany: „Polityka Bezpieczeństwa wStowarzyszeniu Przyjaciół Olimpiady Artystycznej”
7. użytkowniku – należy przez to rozumieć osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym w drodze upoważnienia, o jakim mowa w części II § 4 Polityki Bezpieczeństwa.
8. systemie informatycznym – należy przez to rozumieć system informatyczny, w którym przetwarzane są dane osobowe w jednostce organizacyjnej

**§ 3**

ASI wyznaczany jest przez ADO drogą pisemnego upoważnienia. W przypadku nie wyznaczenia ASI, jego funkcję pełni osoba pełniąca funkcję ADO. Wzór upoważnienia ASI stanowi załącznik nr 1 do niniejszego dokumentu. ASI jest również zobowiązany do podpisania oświadczenia, stanowiącego załącznik nr 4 do Polityki Bezpieczeństwa.

**§ 4**

ASI jest odpowiedzialny za przestrzeganie zasad bezpieczeństwa przetwarzania danych osobowych w zakresie systemu informatycznego służącego do tego celu. Do obowiązków ASI należy także kontrola przepływu informacji pomiędzy systemem informatycznym a siecią publiczną oraz kontrola działań inicjowanych z sieci publicznej i systemu informatycznego **(patrz treść II § 6 niniejszego dokumentu)**.Obowiązkiem ASI jest również zabezpieczenie sprzętu komputerowego przed nieuprawnionym dostępem oraz przeprowadzanie analizy ryzyka uwzględniającej realne zagrożenia dla systemu informatycznego.

**§ 5**

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**

Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym określa się w sposób następujący:

1. użytkownik zamierzający przetwarzać dane osobowe, po uzyskaniu upoważnienia stanowiącego załącznik nr 3 do Polityki Bezpieczeństwa, oraz podpisaniu oświadczenia stanowiącego załącznik nr 4 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.
2. w przypadku wygaśnięcia przesłanek uprawniających użytkownika do przetwarzania danych osobowych, w szczególności cofnięcia upoważnienia, stanowiącego załącznik nr 3 do Polityki Bezpieczeństwa, ASI zobowiązany jest do dopełnienia czynności uniemożliwiających ponowne wykorzystanie identyfikatora użytkownika, którego uprawnienia wygasły.

**§ 2**

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

1. hasło składa się, z co najmniej 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne
2. osobą odpowiedzialną za przydział identyfikatora i pierwszego hasła jest ASI
3. użytkownik, po pierwszym zalogowaniu się do systemu jest zobowiązany do zmiany hasła, jest również zobowiązany do zmiany hasła, co każde 30 dni
4. użytkownik jest zobowiązany do zabezpieczenia swojego hasła przed nieuprawnionym dostępem osób trzecich

**§ 3**

Stosuje się następujące procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu:

1. w celu zalogowania do systemu informatycznego, użytkownik podaje swój identyfikator oraz hasło
2. użytkownik ma obowiązek zabezpieczyć system informatyczny przy każdorazowej przerwie korzystania z niego poprzez wyłączenie systemu informatycznego. Dopuszcza się także konfiguracje systemu informatycznego w taki sposób, aby po okresie 30 minut bezczynności uruchamiany był wygaszacz ekranu. Do ponownego wznowienia pracy konieczne jest ponowne zalogowanie się przy użyciu identyfikatora i hasła
3. po zakończeniu pracy użytkownik jest zobowiązany do wylogowania się, a następnie do wyłączenia komputera

**§ 4**

Stosuje się następujące procedury tworzenia oraz przechowywania kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania:

1. raz na 3 miesiące ASI wykonuje kopię pełną
2. wykonane kopie zapasowe przechowuje się na pamięci przenośnej (*dysk zewnętrzny*), odpowiednio zabezpieczonej przestrzeni na wydzielonych serwerach (dysk sieciowy) 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 pomieszczeniach wymienionych w załączniku nr 1 do Polityki Bezpieczeństwa.

**§ 5**

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 pomieszczeniu Działu Edukacji Muzeum Pałacu Króla Jana III w Wilanowie i przylegającym do niego pokoju na dokumentację Biura Organizacyjnego Olimpiady Artystycznej.

Sprzęt komputerowy, na którego dyskach twardych zawarte są dane osobowe, przechowywany jest w obszarze przetwarzania danych osobowych, w zabezpieczonych pomieszczeniach wymienionych w załączniku nr 1 do Polityki Bezpieczeństwa.

**§ 6**

System informatyczny zabezpiecza się przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do tego systemu poprzez stosowanie specjalistycznego oprogramowania, o jakim mowa w lit. a niniejszego paragrafu:

1. oprogramowaniem antywirusowym stosowanym w jednostce organizacyjnej jest: Program antywirusowy Avast!
2. użytkownikom nie wolno otwierać na komputerach, na których odbywa się przetwarzanie danych osobowych, plików pochodzących z niewiadomego źródła bez zgody ASI
3. za wdrożenie i korzystanie z oprogramowania antywirusowego, określonego w lit. a oraz oprogramowania firewall, odpowiada ASI

**§ 7**

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 opisanym, w § 12 niniejszej części.

**§ 8**

Stosuje się następujące procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych:

1. 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
2. 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
3. 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

**§ 9**

System informatyczny służący do przetwarzania danych osobowych jest zabezpieczony przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej poprzez stosowanie

1. zasilanie laptopa baterią
2. listew przepięciowych, połączonych pomiędzy siecią zasilającą a komputerami

**§ 10**

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.

**§ 11**

Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:

1. likwidacji – pozbawia się wcześniej zapisu tych danych, a w przypadku, gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie
2. przekazania podmiotowi nieuprawnionemu do przetwarzania danych – pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie
3. naprawy – pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem ASI

**§ 12**

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:

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

**§ 13**

Dla każdej osoby, której dane osobowe są przetwarzane system informatyczny, zapewnia sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w § 12 lit. a-e.

**§ 14**

Stosuje się następującą procedurę w przypadku stwierdzenia naruszenia zasad bezpieczeństwa systemu informatycznego:

1. w przypadku stwierdzenia przez użytkownika naruszenia zabezpieczeń 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

**§ 15**

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 usunięcie ich 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.

**III – Postanowienia końcowe**

**§ 1**

W sprawach nieuregulowanych niniejszą Instrukcją, znajdują zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 1997 Nr 133 poz. 883 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).

**§ 2**

Niniejszy dokument wchodzi w życie z dniem 20 listopada 2015 roku.

……………………………..….…………………

*podpis w imieniu stowarzyszenia*