Uchwała nr 68/2017
Zarządu Stowarzyszenia Wielkie Jeziora Mazurskie 2020
z dnia 06.07.2017 r.
w sprawie wprowadzenia Instrukcji Zarządzania Systemem Informatycznym

Na podstawie § 21 ust. 1 pkt. 15 Statutu Stowarzyszenia Wielkie Jeziora Mazurskie 2020 Zarząd Stowarzyszenia uchwala co następuje:

§ 1

Wprowadza się, jako obowiązującą w Stowarzyszeniu Wielkie Jeziora Mazurskie 2020 Instrukcję Zarządzania Systemem Informatycznym stanowiącą załącznik nr 1 do uchwały.

§ 2

Uchwała wchodzi w życie z dniem podjęcia.

Przewodniczący Zarządu Stowarzyszenia
Piotr Jakubowski

STOWARZYSZENIE
Wielkie Jeziora Mazurskie 2020
11-730 Mikołajki, ul. Kolejowa 6
NIP 845-198-57-00 REGON 361222985

Stowarzyszenie Wielkie Jeziora Mazurskie 2020

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

Kod dokumentu:	ODO-IZSI-01
Wersja:	0.1
Data wersji:	2017/06/02
Utworzony przez:	Mirosław Górski
Zatwierdzony przez:	
Poziom poufności:	Użytek wewnętrzny

Historia zmian

Data	Wersja	Utworzona przez	Opis zmiany
2017-05-30	0.1	Mirosław Górski	Podstawowy szablon dokumentu

Spis treści

1. Cel, zakres i użytkownicy

Niniejsza instrukcja określa zasady eksploatacji i zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych.

Przetwarzanie danych osobowych jest dopuszczalne wyłącznie pod warunkiem przestrzegania ustawy z 29 sierpnia 1997r. o ochronie danych osobowych i wydanych na jej podstawie przepisów wykonawczych w tym niemniejszej polityki i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

Użytkownikami niniejszego dokumentu są wszyscy pracownicy i członkowie Stowarzyszenia Wielkie Jeziora Mazurskie 2020, jak również odnośne podmioty zewnętrzne.

2. Dokumenty referencyjne

- Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2016 poz. 922);
- Rozporządzenie 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. Nr 100, poz. 1024);
- Polityka Bezpieczeństwa w Stowarzyszeniu Wielkie Jeziora Mazurskie;
- inne wewnętrzne procedury odnoszące się do Polityki.

3. Określenia i skróty użyte w Instrukcji

Poufność – właściwość informacji zapewniająca jej dostęp wyłącznie dla osób uprawnionych.

Integralność – właściwość informacji zapewniająca możliwość dokonywania w niej zmian tylko przez uprawnione osoby lub procesy, w dozwolony sposób.

Dostępność – właściwość informacji zapewniająca możliwość dostępu do tej informacji przez uprawnione osoby w każdym czasie, gdy dana informacja jest potrzebna.

Bezpieczeństwo informacji – zapewnienie poufności, integralności oraz dostępności informacji.

Polityka - rozumie się przez to Politykę Bezpieczeństwa w Stowarzyszeniu Wielkie Jeziora Mazurskie;

Instrukcja - rozumie się przez to Instrukcję Zarządzania Systemem Informatycznym w Stowarzyszeniu Wielkie Jeziora Mazurskie;

Administrator Danych Osobowych – Zarząd Stowarzyszenia Wielkie Jeziora Mazurskie 2020, decydujący o celach i środkach przetwarzania danych osobowych;

Administrator Bezpieczeństwa Informacji (ABI) - osobę powołaną przez ADO w Stowarzyszeniu Wielkie Jeziora Mazurskie 2020, wpisaną do prowadzonego przez Generalnego Inspektora Ochrony Danych Osobowych rejestru administratorów bezpieczeństwa informacji, zwaną dalej „ABI";

Ustawa - rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2016 poz. 922);

Rozporządzenie - Rozporządzenie 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);

Dane osobowe (dane) - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;

Zbiór danych - zestaw danych osobowych posiadający określoną strukturę, prowadzony w/g określonych kryteriów oraz celów;

Usuwanie danych - rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;

Zgoda 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;

Baza danych osobowych - zbiór uporządkowanych powiązanych ze sobą tematycznie danych zapisanych np. w pamięci zewnętrznej komputera. Baza danych jest złożona z elementów o określonej strukturze - rekordów lub obiektów, w których są zapisane dane osobowe;

Przetwarzanie danych - wykonywanie jakichkolwiek operacji na danych osobowych, np. zbieranie, utrwalanie, opracowywanie, udostępnianie, zmienianie, usuwanie;

System informatyczny (system) - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;

Administrator systemu - osoba nadzorująca pracę systemu informatycznego oraz wykonująca w nim czynności wymagające specjalnych uprawnień;

Użytkownik - pracownik Stowarzyszenia Wielkie Jeziora Mazurskie 2020 posiadający uprawnienia do pracy w systemie informatycznym zgodnie z zakresem obowiązków służbowych;

Zabezpieczenie systemu informatycznego - należy przez to rozumieć wdrożenie stosownych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych, a także ich utratą;

Nośnik komputerowy (wymienny) - nośnik służący do zapisu i przechowywania informacji, np. taśmy, dyskietki, dyski twarde, dysku flash, pendrive;

Hasło - ciąg znaków literowych, cyfrowych lub innych, znany jedynie użytkownikowi;

Identyfikator - ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie.

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

Podstawą do nadania uprawnień do przetwarzania danych osobowych w systemie informatycznym Stowarzyszenia jest upoważnienie do przetwarzania danych osobowych. Upoważnienie wydawane jest w imieniu Administratora Danych Osobowych przez Administratora Bezpieczeństwa Informacji.

Administrator Bezpieczeństwa Informacji:

1) w przypadku, gdy dana osoba otrzymuje po raz pierwszy upoważnienie do przetwarzania danych osobowych informuje ją o obowiązkach związanych z zapewnieniem ochrony danych osobowych;
2) odbiera od powyższej osoby podpis pod upoważnieniem do przetwarzania danych osobowych i oświadczeniem o zapoznaniu się z obowiązującymi zasadami ochrony danych osobowych.

ABI prowadzi, w imieniu i z upoważnienia Administratora Danych Osobowych, ewidencję osób upoważnionych do przetwarzania danych osobowych. Każda zmiana w zakresie informacji zawartych w ewidencji podlega niezwłocznemu odnotowaniu przez ABI.

Za nadanie uprawnień w systemie informatycznym odpowiada ABI. Uprawnienia nie mogą być nadane w przypadku, jeżeli dana osoba nie posiada upoważnienia do przetwarzania danych osobowych w wymaganym zakresie.

Identyfikator użytkownika w systemie informatycznym musi być unikalny dla użytkownika. Nie może być to identyfikator, który w przeszłości był już stosowany w systemie informatycznym. Sprawdzenie unikalności identyfikatora odbywa się na podstawie ewidencji osób upoważnionych do przetwarzania danych osobowych.

Hasło użytkownika jest przydzielane indywidualnie każdemu z użytkowników i znane jest tylko użytkownikowi, który się nim posługuje.

Użytkownik jest zobowiązany do zmiany hasła przy pierwszym dostępie do systemu informatycznego.

5. Procedura odbierania uprawnień do przetwarzania danych w systemie informatycznym

W przypadku konieczności odebrania lub zmiany zakresu upoważnienia – w związku ze zmianą zakresu obowiązków służbowych pracownika lub zakończeniem pracy Administrator Bezpieczeństwa Informacji dokonuje odebrania lub zmiany zakresu upoważnienia

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

Użytkownicy systemu informatycznego przetwarzającego dane osobowe wykorzystują w procesie uwierzytelnienia identyfikatory i hasła.

Identyfikator jest w sposób jednoznaczny przypisany użytkownikowi i nie podlega zmianie.

Po załogowaniu do systemu z wykorzystaniem otrzymanego hasła użytkownik jest zobowiązany do dokonania jego natychmiastowej zmiany, nawet, jeżeli system informatyczny nie wymusza takiego działania.

Hasła dostępu do systemu informatycznego muszą spełniać poniższe warunki:

1) posiadać długość co najmniej 8 znaków,
2) zawierać litery małe i duże,
3) zawierać cyfry lub znaki specjalne.

Hasło w systemach przetwarzających danych osobowych jest zmieniane przez użytkownika nie rzadziej, niż co 30 dni lub niezwłocznie w przypadku podejrzenia, iż mogły z nim się zapoznać nieuprawnione osoby. Hasło powinno różnić się od poprzednio używanych.

Użytkownik zobowiązany jest do:

1) nieujawniania hasła innym osobom, w tym innym użytkownikom,
2) zachowania hasła w tajemnicy, również po jego wygaśnięciu,
3) niezapisywania hasła,
4) postępowania z hasłami w sposób uniemożliwiający dostęp do nich osobom trzecim,
5) przestrzegania zasad dotyczących, jakości i częstości zmian hasła,
6) wprowadzania hasła do systemu w sposób minimalizujący podejrzenie go przez innych użytkowników systemu.

W przypadku podejrzenia zapoznania się z hasłem przez osobę nieuprawnioną użytkownik jest zobowiązany do natychmiastowej zmiany hasła oraz powiadomienia o zaistniałym fakcie ABI.

7. Procedura rozpoczęcia, zawieszenia i zakończenia pracy przeznaczona dla użytkowników systemu

Rozpoczynając pracę w systemie informatycznym przetwarzającym dane osobowe, użytkownik:

1) uruchamia komputer,
2) wprowadza niezbędne do pracy identyfikatory i hasła,
3) hasła są wprowadzane w sposób minimalizujący ryzyko podejrzenia ich przez osoby trzecie,

Zawieszając pracę w systemie informatycznym (w tym odchodząc od stanowiska pracy), użytkownik blokuje stację roboczą. Kontynuacja pracy może nastąpić po odblokowaniu stacji roboczej po wprowadzeniu hasła, w sposób gwarantujący jego niepodejrzenie przez osoby trzecie.

Opuszczając pomieszczenie, w którym przetwarzane są dane osobowe, pracownik zobowiązany jest do zamknięcia pomieszczenia na klucz, jeżeli w pomieszczeniu tym nie przebywa inna osoba upoważniona do przebywania w tym pomieszczeniu. Zabronione jest pozostawianie bez nadzoru w pomieszczeniach, w których przetwarzane są dane osobowe, osób nieupoważnionych.

Kończąc pracę w systemie informatycznym pracownik wylogowuje się ze wszystkich aplikacji, z których korzystał, wyłącza stację roboczą i zabezpiecza nośniki danych.

8. Procedura tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania

Za tworzenie i przechowywanie kopii zapasowych odpowiedzialny jest użytkownik.

Kopie zapasowe systemów przetwarzających dane osobowe są tworzone na nośnikach elektronicznych wbudowanych w sprzęt informatyczny.

Utworzone kopie zapasowe podlegają weryfikacji ze względu na sprawdzenie możliwości odczytu danych.

ABI określa czas przechowywania poszczególnych kopii zapasowych, w zależności od celu przetwarzania danych zapisanych na kopiach zapasowych.

Użytkownik odpowiedzialny jest za realizację działań odtworzeniowych w przypadku konieczności podjęcia takich działań w związku z awarią systemu informatycznego użytkowanego w Stowarzyszeniu Wielkie Jeziora Mazurskie 2020.

9. Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz nośników kopii zapasowych

Dane osobowe przechowywane są w postaci elektronicznej na:

1) nośnikach elektronicznych wbudowanych w sprzęt informatyczny lub stanowiących element tego systemu,

Dane osobowe w systemie informatycznym przechowywane są przez czas wymagany do spełnienia celu, dla którego są one przetwarzane. Po jego upływie dane podlegają skasowaniu lub anonimizacji.

Przenośne elektroniczne nośniki informacji zawierające dane osobowe są przechowywane przez pracowników w sposób minimalizujący ryzyko ich uszkodzenia lub zniszczenia, w szczególności w zamykanych szafach i meblach biurowych. ABI wyznacza pomieszczenia, w których mogą być przechowywane takie nośniki.

W przypadku wycofania sprzętu komputerowego z użycia dane osobowe na nim zapisane są kasowane przy użyciu dedykowanego oprogramowania do bezpiecznego usuwania danych

zaakceptowanego do użycia w Stowarzyszeniu Wielkie Jeziora Mazurskie 2020. W przypadku braku możliwości programowego usunięcia danych dysk podlega fizycznemu zniszczeniu. Za zniszczenie danych odpowiada ABI. Zniszczenie nośnika potwierdzane jest protokołem przechowywanym przez Administratora Bezpieczeństwa Informacji.

Dopuszcza się powierzenie niszczenia nośników danych wyspecjalizowanym podmiotom zewnętrznym, pod warunkiem:

1) zawarcia umowy, o której mowa w art. 31 ustawy,
2) zagwarantowania poufności danych przez usługodawcę,
3) umożliwienia prowadzenia nadzoru nad procesem niszczenia nośników przez ABI lub upoważnionego przez niego pracownika Stowarzyszenia Wielkie Jeziora Mazurskie 2020,
4) udokumentowania faktu zniszczenia nośników protokołem.

10.Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem działania jest uzyskanie nieuprawnionego dostępu do systemu informatycznego

W celu zabezpieczenia systemu informatycznego przed działaniem niebezpiecznego oprogramowania zabrania się:

1) uruchamiania jakiegokolwiek oprogramowania, które nie zostało zatwierdzone do użytku w Stowarzyszeniu;
2) samowolnego korzystania z nośników przenośnych;
3) otwierania poczty elektronicznej, której tytuł nie sugeruje związku z pełnionymi obowiązkami służbowymi; w przypadkach wątpliwych należy skonsultować się z ABI;
4) korzystania z Internetu w celach nie związanych z pełnionymi obowiązkami służbowymi;
5) podłączania komputerów do sieci zewnętrznych za pośrednictwem modemów.

W przypadku zauważenia objawów mogących wskazywać na obecność niebezpiecznego oprogramowania użytkownik jest zobowiązany powiadomić ABI. Do objawów powyższych można zaliczyć:

1) istotne spowolnienie działania systemu informatycznego,
2) nietypowe działanie aplikacji,
3) nietypowe komunikaty,
4) utratę danych lub modyfikację danych.

System informatyczny jest zabezpieczony przed działaniem niebezpiecznego oprogramowania poprzez:

1) oprogramowanie antywirusowe,
2) aktualizację oprogramowania systemowego,
3) konfigurację oprogramowania minimalizującą ryzyko naruszenia bezpieczeństwa.

11.Odnotowanie informacji o udostępnieniu danych osobowych

Stowarzyszenie Wielkie Jeziora Mazurskie 2020 udostępnia dane osobowe jedynie w przypadkach prawnie dopuszczalnych.

Odnotowanie faktu udostępnienia danych następuje:

1) Przy odnotowywaniu przez użytkownika informacji o udostępnieniu danych, użytkownik wprowadza zapis „Dane osobowe w zakresie ››zakres‹‹ udostępniono ››odbiorca‹‹ w dniu ››data‹‹", wprowadzając zamiast zapisów w nawiasach klamrowych odpowiednie informacje.

12.Procedura wykonywania przeglądu i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych

Przegląd i konserwacja sprzętu informatycznego realizowany jest przez upoważnionych pracowników Stowarzyszenia Wielkie Jeziora Mazurskie 2020 oraz przez podmioty zewnętrzne.

Prace serwisowe wykonywane na terenie Stowarzyszenia Wielkie Jeziora Mazurskie 2020 przez podmioty zewnętrzne podlegają bezpośredniemu nadzorowi ABI.

Przekazanie sprzętu teleinformatycznego do naprawy poza teren Stowarzyszenia Wielkie Jeziora Mazurskie 2020 jest dopuszczalne, jeżeli spełnione zostaną poniższe warunki:

1) sprzęt przekazywany jest bez nośników zawierających dane osobowe, zaś fakt usunięcia nośników danych lub stwierdzenia braku nośników danych jest potwierdzany protokołem,
2) przekazanie sprzętu potwierdzane jest protokołem, pozwalającym na jednoznaczne wskazanie osoby przekazującej i osoby odbierającej sprzęt.
3) Protokoły, o których mowa w punkcie 3, lub ich kopie przechowywane są przez ABI.

Wszelkie prace serwisowe wykonywane przez podmioty zewnętrzne wymagają sporządzenia protokołu serwisowego, zawierającego co najmniej poniższe informacje:

1) wskazanie osoby przeprowadzającej prace serwisowe oraz podmiotu, którego osoba ta jest pracownikiem,
2) wskazanie osoby nadzorującej przebieg prac serwisowych (dotyczy sytuacji, gdy prace realizowane są w siedzibie Stowarzyszenia Wielkie Jeziora Mazurskie 2020),
3) przedmiot prac serwisowych (w szczególności identyfikator sprzętu w przypadku prac serwisowych dotyczących sprzętu),
4) zakres prac serwisowych i ich wynik,
5) czas przeprowadzania prac serwisowych.

13.Ważność oraz zarządzanie niniejszym dokumentem

Stwierdza się ważność niniejszego dokumentu na dzień 2017/06/02

Właścicielem niniejszego dokumentu jest Administrator Bezpieczeństwa Informacji, który jest odpowiedzialny za weryfikację oraz w razie konieczności aktualizację niniejszego dokumentu, co najmniej raz w roku.

W ocenie efektywności i właściwości niniejszego dokumentu należy wziąć pod uwagę następujące kryteria:

- liczbę pracowników i podmiotów zewnętrznych, których dotyczy proces przetwarzania danych osobowych, a którzy nie zapoznali się z niniejszym dokumentem
- niezgodność dokumentacji przetwarzania danych osobowych z przepisami prawa, obowiązkami branżowymi, zobowiązaniami umownymi oraz innymi dokumentami wewnętrznymi organizacji;
- nieefektywność wdrożenia i obsługi procesu danych osobowych
- niejasny podział odpowiedzialności za wdrożenie dokumentacji przetwarzania danych osobowych