Załącznik nr 5 do Polityki bezpieczeństwa Związku Rzemiosła Polskiego

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM W ZWIĄZKU RZEMIOSŁA POLSKIEGO

Spis treści

I. Przepisy ogólne

1. Podstawa prawna

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. Urz. UE L 119.1), dalej określane jako „Rozporządzenie" lub „RODO" i ustawa z 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r. poz. 1000).

2. Definicje pojęć

ZRP – Związek Rzemiosła Polskiego z siedzibą w Warszawie
IODO - Inspektor Ochrony Danych - osoba nadzorująca przestrzeganie zasad ochrony danych osobowych określonych w niniejszym dokumencie
ASI - Administrator Systemu Informatycznego – osoba odpowiedzialna za funkcjonowanie systemu informatycznego ZRP lub firma zewnętrzna realizująca zadania ASI na podstawie odnośnej umowy.
Użytkownik systemu – osoba upoważniona do przetwarzania danych osobowych w systemie informatycznym ZRP, przy czym użytkownikiem systemu może być pracownik ZRP, osoba wykonująca prace na podstawie umowy zlecenia lub innej umowy cywilno-prawnej.
Identyfikator użytkownika - ciąg znaków literowych, cyfrowych lub innych identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.
Hasło – ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.
Sieć telekomunikacyjna – sieć telekomunikacyjna w rozumieniu art. 2 pkt. 23 ustawy z dnia 21 lipca 2000 roku – Prawo telekomunikacyjne (Dz.U. Nr 73, poz. 852, z późn. zm.)
Teletransmisja – przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej.
Sieć lokalna – połączenie systemów informatycznych ZRP wyłącznie dla własnych potrzeb przy wykorzystaniu urządzeń i sieci telekomunikacyjnych.
Sieć rozległa – sieć publiczną w rozumieniu ustawy z dnia 21 lipca 2000 r. – Prawo telekomunikacyjne (Dz. U. Nr 73, poz. 852 z późn. zm.).
Uwierzytelnianie – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.
Integralność danych – właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany.

II. Procedury nadawania i zmiany uprawnień do przetwarzania danych

1. Każdy użytkownik systemu przed przystąpieniem do przetwarzania danych osobowych ma obowiązek zapoznać się z:
- Polityką bezpieczeństwa określającą zasady ochrony danych osobowych w ZRP
- niniejszą Instrukcją.

2. Zapoznanie się z przepisami wymienionymi w punkcie 1 pracownik potwierdza własnoręcznym podpisem na oświadczeniu, którego wzór stanowi **Załącznik Nr 1** do Instrukcji.
3. Administrator systemu informatycznego przyznaje uprawnienia w zakresie dostępu do systemu informatycznego na podstawie wniosku przekazanego lub przesłanego drogą korespondencji elektronicznej przez Dyrektora Generalnego ZRP określającego zakres uprawnień pracownika.

4. Wzór wniosku o przyznanie uprawnienia w zakresie dostępu do systemu informatycznego stanowi **załącznik Nr 2** do Instrukcji.
5. Karta ewidencyjna powinna odzwierciedlać aktualny stan systemu w zakresie użytkowników i ich uprawnień oraz umożliwiać przeglądanie historii zmian uprawnień użytkowników.
6. Wzór karty ewidencyjnej, powinien zawierać:
- imię i nazwisko użytkownika systemów informatycznych;
- rodzaj uprawnienia;
- datę nadania uprawnienia;
- datę odebrania uprawnienia;
- przyczynę odebrania uprawnienia;
- podpis IODO.
7. Wzór karty ewidencyjnej uprawnień w zakresie dostępu i obsługi programów i aplikacji systemu informatycznego w ZRP związanych z przetwarzaniem danych osobowych stanowi **załącznik Nr 3** do Instrukcji.
8. Przyznanie uprawnień w zakresie dostępu do systemu informatycznego polega na wprowadzeniu do systemu dla każdego użytkownika unikalnego identyfikatora, hasła oraz nadanie mu praw dostępu. Ustanowione hasło, Administrator Systemu Informatycznego przekazuje użytkownikowi na piśmie. Identyfikator użytkownika składa się z minimum ośmiu znaków alfanumerycznych zawierających przynajmniej dwie duże litery lub dwa znaki specjalne.
9. Pracownik ma prawo do wykonywania tylko tych czynności, do których został upoważniony.
10. Pracownik ponosi odpowiedzialność za wszystkie operacje wykonane przy użyciu jego identyfikatora i hasła dostępu.
11.Wszelkie przekroczenia lub próby przekroczenia przyznanych uprawnień traktowane są jako naruszenie podstawowych obowiązków pracowniczych.
12. Pracownik zatrudniony przy przetwarzaniu danych osobowych zobowiązany jest do zachowania ich w tajemnicy. Tajemnica obowiązuje go również po ustaniu zatrudnienia.
13.W systemie informatycznym stosuje się uwierzytelnianie dwustopniowe: na poziomie dostępu do sieci lokalnej oraz dostępu do aplikacji.
14. Identyfikator użytkownika w aplikacji (o ile działanie aplikacji na to pozwala), powinien być tożsamy z tym, jaki jest mu przydzielany w sieci lokalnej.
15.Odebranie uprawnień pracownikowi następuje na pisemny wniosek kierownika, któremu pracownik podlega z podaniem daty oraz przyczyny odebrania uprawnień.
16. Kierownicy komórek organizacyjnych zobowiązani są pisemnie informować IODO i ASI o każdej zmianie dotyczącej podległych pracowników mającej wpływ na zakres posiadanych uprawnień w systemie informatycznym.
17. Identyfikator osoby, która utraciła uprawnienia do dostępu do danych osobowych należy niezwłocznie wyrejestrować z systemu informatycznego, w którym są one przetwarzane oraz unieważnić jej hasło.
18. ASI zobowiązany jest do prowadzenia i ochrony rejestru użytkowników i ich uprawnień w systemie informatycznym.

III. Zasady posługiwania się hasłami

1. Bezpośredni dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora i hasła.
2. Hasło powinno być zmieniane przez użytkownika, co najmniej raz na 6 miesięcy.

3. Identyfikator użytkownika nie powinien być zmieniany bez wyraźnej przyczyny, a po wyrejestrowaniu użytkownika z systemu informatycznego nie powinien być przydzielany innej osobie.
4. Pracownicy są odpowiedzialni za zachowanie poufności swoich haseł.
5. Hasła użytkownika utrzymuje się w tajemnicy również po upływie ich ważności.
6. Pracownik nie ma prawa do udostępniania haseł danej grupy osobom spoza tej grupy, dla której zostały one utworzone.
7. Hasło należy wprowadzać w sposób, który uniemożliwia innym osobom jego poznanie.
8. W sytuacji, kiedy zachodzi podejrzenie, że ktoś poznał hasło w sposób nieuprawniony, pracownik zobowiązany jest do natychmiastowej zmiany hasła.
9. Przy wyborze hasła obowiązują następujące zasady:
1) minimalna długość hasła - 8 znaków;
2) zakazuje się stosować:
a) haseł, które użytkownik stosował uprzednio w okresie minionego roku,
b) swojej nazwy użytkownika w jakiejkolwiek formie (pisanej dużymi literami, w odwrotnym porządku, dublując każdą literę, itp.),
c) nazw słownikowych oraz nazw własnych,
d) ogólnie dostępnych informacji o użytkowniku takich jak: numer telefonu, numer rejestracyjny samochodu, jego marka, numer dowodu osobistego, nazwa ulicy, na której mieszka lub pracuje, itp.,
e) przewidywalnych sekwencji znaków z klawiatury np.: QWERTY", "12345678", itp.,
f) identyfikatora użytkownika jako hasła.
3) należy stosować:
a) hasła zawierające kombinacje liter i cyfr,
b) hasła, które można zapamiętać bez zapisywania,
c) hasła łatwe i szybkie do wprowadzenia, po to by trudniej było podejrzeć je osobom trzecim.
10. Zmiany hasła nie wolno zlecać innym osobom.
11. W systemach, które umożliwiają opcję zapamiętania nazw użytkownika lub jego hasła nie należy korzystać z tego ułatwienia.
12. Hasło użytkownika powinno znajdować się w zalakowanej kopercie w zamykanej na klucz szafie metalowej, do której dostęp mają:
- Inspektor Danych Osobowych;
- Administrator Danych Osobowych;
- Administrator Systemu Informatycznego.

IV. Procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemie

1. Przed rozpoczęciem pracy w systemie komputerowym należy zalogować się do systemu przy użyciu indywidualnego identyfikatora oraz hasła.
2. Przy opuszczeniu stanowiska pracy na odległość uniemożliwiającą jego obserwację należy wykonać opcję wylogowania z systemu (zablokowania dostępu), lub jeżeli taka możliwość nie istnieje wyjść z programu.
3. Osoba udostępniająca stanowisko komputerowe innemu upoważnionemu pracownikowi zobowiązana jest wykonać funkcję wylogowania z systemu.
4. Przed wyłączeniem komputera należy bezwzględnie zakończyć pracę uruchomionych programów, wykonać zamknięcie systemu i jeżeli jest to konieczne wylogować się z sieci komputerowej.

5. Niedopuszczalne jest wyłączanie komputera przed zamknięciem oprogramowania oraz zakończeniem pracy w sieci.

V. Procedury tworzenia zabezpieczeń

1. Za systematyczne przygotowanie kopii bezpieczeństwa odpowiada Administrator Systemu Informatycznego.
2. Kopie bezpieczeństwa wykonywane są nie rzadziej niż dwa razy w tygodniu po zakończeniu pracy użytkowników w sieci komputerowej.
3. Dodatkowe zabezpieczenie wszystkich programów i danych wykonywane jest w pierwszym dniu każdego miesiąca w postaci zapisu na nośnikach zewnętrznych.
4. Zewnętrzne nośniki danych zawierające kopie bezpieczeństwa przechowuje się w metalowej szafie w pokoju Inspektora Ochrony Danych w budynku Związku Rzemiosła Polskiego przy ulicy Miodowej 14 w Warszawie zarówno w przypadku sprawowania funkcji Administratora Systemu Informatycznego przez osobę zatrudniona na umowę o pracę lub umowy cywilno – prawne jak i firmę w ramach outsourcingu IT.

VI. Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz wydruki

1. Elektroniczne nośniki informacji:
1) dane osobowe w postaci elektronicznej zapisane na zewnętrznych nośnikach danych mogą być wyniesione poza siedzibę ZRP jedynie przy zgodzie IODO lub Administratora;
2) wymienne elektroniczne nośniki informacji są przechowywane w pokojach stanowiących obszar przetwarzania danych osobowych, określony w Polityce bezpieczeństwa ZRP;
3) po zakończeniu pracy przez użytkowników systemu, wymienne elektroniczne nośniki informacji są przechowywane w zamykanych szafach biurowych lub kasetkach;
4) urządzenia, dyski lub inne informatyczne nośniki, 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;
5) urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do naprawy, pozbawia się przed naprawą zapisu tych danych albo naprawia się je pod nadzorem osoby upoważnionej.
2. Kopie zapasowe:
1) kopie zapasowe zbioru danych osobowych oraz oprogramowania i narzędzi programowych zastosowanych do przetwarzania danych są przechowywane w kasie pancernej lub metalowej w pokoju Administracyjnym w budynku ZRP w Warszawie przy ul. Miodowej;
2) dostęp do danych opisanych w punkcie 1 ma IODO, ASI oraz upoważnieni przez Administratora pracownicy.
3. Wydruki:
1) w przypadku konieczności przechowywania wydruków zawierających dane osobowe należy je przechowywać w miejscu uniemożliwiającym bezpośredni dostęp osobom niepowołanym;
2) pomieszczenie, w którym przechowywane są wydruki robocze musi być należycie zabezpieczone po godzinach pracy;
3) wydruki, które zawierają dane osobowe i są przeznaczone do usunięcia, należy zniszczyć w stopniu uniemożliwiającym ich odczytanie.

VII. Środki ochrony systemu przed złośliwym oprogramowaniem, w tym wirusami komputerowymi

1. Na każdym stanowisku komputerowym musi być zainstalowane oprogramowanie antywirusowe oraz firewall pracujące w trybie monitora.
2. Każdy e-mail wpływający do IR musi być sprawdzony pod kątem występowania wirusów przez firewall.
3. Definicje wzorców wirusów aktualizowane są kilka razy w czasie dnia.
4. Zabrania się używania nośników niewiadomego pochodzenia bez wcześniejszego sprawdzenia ich programem antywirusowym. Sprawdzenia dokonuje użytkownik, który nośnik zamierza użyć.
5. Zabrania się pobierania z Internetu plików niewiadomego pochodzenia. Każdy plik pobrany z Internetu musi być sprawdzony programem antywirusowym. Sprawdzenia dokonuje użytkownik, który pobrał plik.
6. Zabrania się odczytywania załączników poczty elektronicznej bez wcześniejszego sprawdzenia ich programem antywirusowym. Sprawdzenia dokonuje pracownik, który pocztę otrzymał.
7. Administrator Systemu Informatycznego przeprowadza cykliczne kontrole antywirusowe na wszystkich komputerach - minimum, 2 razy w miesiącu.
8. Kontrola antywirusowa przeprowadzana jest również na wybranym komputerze w przypadku zgłoszenia nieprawidłowości w funkcjonowaniu sprzętu komputerowego lub oprogramowania.
9. W przypadku wykrycia wirusów komputerowych sprawdzane jest stanowisko komputerowe, na którym wirusa wykryto.

VIII. Zasady i sposób odnotowywania w systemie informacji o udostępnieniu danych osobowych

1. Dane osobowe z eksploatowanych systemów mogą być udostępniane wyłącznie osobom upoważnionym.
2. Udostępnienie danych osobowych, w jakiejkolwiek postaci, jednostkom nieuprawnionym wymaga pisemnego upoważnienia Administratora Danych Osobowych.
3. Udostępnienie danych osobowych nie może być realizowane drogą telefoniczną ani pocztą elektroniczną.
4. Udostępnienie danych osobowych następuje po przedstawieniu wniosku wg wzoru określonego w **załączniku Nr 4** do Instrukcji.
5. Pracownicy prowadzą rejestry udostępnionych danych osobowych zawierające, co najmniej: datę udostępnienia, podstawę, zakres udostępnionych informacji oraz osobę lub instytucję, dla której dane udostępniono.
6. Aplikacje wykorzystywane do obsługi baz danych osobowych powinny zapewniać odnotowanie informacji o udzielonych odbiorcom danych. Zakres informacji powinien obejmować, co najmniej: dane odbiorcy, datę wydania, zakres udostępnionych danych.

IX. Postępowanie w sytuacji naruszenia ochrony danych osobowych

Postępowanie w sytuacji naruszenia ochrony danych osobowych określa rozdział „Zasady postępowania w przypadku naruszenia ochrony danych osobowych” zawarty w dokumencie

„Polityka bezpieczeństwa w zakresie danych osobowych w ZRP.

X. Procedury wykonywania przeglądów i konserwacji systemu

1. Przeglądy i konserwacja urządzeń:
1) przeglądy i konserwacja urządzeń wchodzących w skład systemu informatycznego powinny być wykonywane w terminach określonym przez producenta sprzętu lub jeżeli termin nie został określony przynajmniej raz na 2 miesiące;
2) nieprawidłowości ujawnione w trakcie tych działań powinny być niezwłocznie usunięte, a ich przyczyny przeanalizowane. O fakcie ujawnienia nieprawidłowości należy zawiadomić IODO.
2. Przegląd programów i narzędzi programowych:
1) konserwacja baz danych przeprowadzana jest zgodnie z zaleceniami twórców poszczególnych programów;
2) IODO zobowiązany jest uaktywnić mechanizm zliczania nieudanych prób zalogowania się do systemu oraz ustawić blokadę konta użytkownika po wykryciu trzech nieudanych prób, we wszystkich systemach posiadających taką funkcję;
3) wszystkie logi opisujące pracę systemu, zalogowania i wylogowania użytkowników oraz rejestr z systemu śledzenia wykonywanych operacji w programie należy przed usunięciem zapisać na nośnik zewnętrzny.
3. Rejestracja działań konserwacyjnych, awarii oraz napraw:
1) Administrator Systemu Informacji prowadzi „Dziennik systemu informatycznego ZRP", wzór i zakres informacji rejestrowanych w dzienniku określa **załącznik Nr 5** do Instrukcji;
2) wpisów do dziennika może dokonywać Administrator, IODO, ASI lub osoby przez nich wyznaczone.

XI. Połączenie do sieci Internet

1. Połączenie lokalnej sieci komputerowej ZRP z Internetem jest dopuszczalne wyłącznie po zainstalowaniu mechanizmów ochronnych (firewall) oraz kompleksowego oprogramowania antywirusowego.
2. W przypadku przesyłania danych osobowych oraz danych wymaganych do uwierzytelniania wymagane jest zastosowanie środków kryptograficznej ochrony danych.

XII. Postanowienia końcowe

Na stanowisku pracy obowiązuje bezwzględny zakaz instalowania jakiegokolwiek oprogramowania. Pracownik chcąc zainstalować aplikację lub program musi uzyskać pisemną zgodę od Administratora Systemu Informatycznego.

Załącznik Nr 1
do INSTRUKCJI ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

Warszawa, dnia .....

.....
(nazwisko i imię)
.....
(stanowisko)

OŚWIADCZENIE

Oświadczam, iż w związku z wykonywaniem obowiązków służbowych, przetwarzam oraz mam dostęp do zbiorów, dokumentów, zestawień, kartotek lub systemów informatycznych zawierających dane osobowe i w związku z tym zapoznałem(am) się z:

1) ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018, poz. 1000);
2) ogólnym rozporządzeniem w sprawie ochrony danych osobowych z dnia 27 kwietnia 2016 (Dz. Urz. UE L 119.s1;

3) „Polityką Bezpieczeństwa w Związku Rzemiosła Polskiego wprowadzoną Uchwałą Zarządu ZRP z dnia 23.05.2018 r;

4) „Instrukcją zarządzania systemem informatycznym w ZRP".

.....
(podpis pracownika)

Załącznik Nr 2
do INSTRUKCJI ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

Wniosek o nadanie uprawnień w systemie informatycznym

Nowy użytkownik	Nadanie uprawnień w systemie informatycznym/ modyfikacja	Odebranie uprawnień w systemie informatycznym

Imię i nazwisko użytkownika	Stanowisko
Opis zakresu uprawnień użytkownika w systemie informatycznym i uzasadnienie:	
Data wystawienia	Podpis bezpośredniego przełożonego użytkownika
	Podpis Inspektora Ochrony Danych

Załącznik Nr 3
do INSTRUKCJI ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM W ZWIĄZKU RZEMIOSŁA POLSKIEGO

Karta ewidencyjna uprawnień w zakresie dostępu i obsługi programów i aplikacji systemu informatycznego w Związku Rzemiosła Polskiego związanych z przetwarzaniem danych osobowych

Identyfikator użytkownika	Nazwisko i imię użytkownika

Lp	Rodzaj uprawnienia	Data nadania uprawnień	Podpis IODO	Data i przyczyna odebrania uprawnień

Załącznik Nr 4
do INSTRUKCJI ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM W ZWIĄZKU RZEMIOSŁA POLSKIEGO

Wniosek o udostępnienie danych ze zbioru danych osobowych

1. Wniosek do Administratora Danych Osobowych.

2. Wnioskodawca ….....
(nazwa firmy i jej siedziba albo nazwisko, imię i adres zamieszkania wnioskodawcy, ew. NIP oraz nr REGON)

3. Podstawa prawna upoważniająca do pozyskania danych, albo wskazanie wiarygodnie uzasadnionej potrzeby posiadania danych w przypadku osób innych niż wymienione w art. 29 ust. 1 ustawy o ochronie danych osobowych:
.....

4. Wskazanie przeznaczenia dla udostępnionych danych:
.....

5. Oznaczenie lub nazwa zbioru, z którego mają być udostępnione dane:
.....

6. Zakres żądanych informacji ze zbioru:
.....

7. Informacje umożliwiające wyszukanie w zbiorze żądanych danych: .....

……

…….
(data, podpis i ew. pieczęć wnioskodawcy)

Załącznik Nr 5
do INSTRUKCJI ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

Dziennik systemu informatycznego Związku Rzemiosła Polskiego

Dziennik zawiera opisy wszelkich zdarzeń istotnych dla działania systemu informatycznego, a w szczególności:

1) w przypadku awarii - opis awarii, przyczyna awarii, szkody wynikłe na skutek awarii, sposób usunięcia awarii, opis systemu po awarii, wnioski;

2) w przypadku konserwacji systemu – opis podjętych działań, wnioski.

Lp.	data i godzina zdarzenia	Opis zdarzenia	Podjęte działania	Wnioski	Podpis