

Zarządzenie nr 8/2013

**LUBUSKIEGO WOJEWÓDZKIEGO INSPEKTORA
OCHRONY ROŚLIN I NASIENICTWA**

z dnia 22 kwietnia 2013 r.

w sprawie wprowadzenia Polityki Bezpieczeństwa Danych Osobowych i Instrukcji Zarządzania Systemami Informatycznymi w Wojewódzkim Inspektoracie Ochrony Roślin i Nasiennictwa w Gorzowie Wlkp.

Na podstawie art. 36 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t. j. Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.) oraz § 3, 4 i 5 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. Nr 100, poz. 1024) zarządza się co następuje:

§1. Wprowadza się do stosowania w Wojewódzkim Inspektoracie Ochrony Roślin i Nasiennictwa w Gorzowie Wlkp. Politykę bezpieczeństwa danych osobowych stanowiącą załącznik nr 1 do niniejszego zarządzenia oraz Instrukcję zarządzania systemami informatycznymi, stanowiącą załącznik nr 2.

§2. Zobowiązuje się pracowników Wojewódzkiego Inspektoratu Ochrony Roślin i Nasiennictwa w Gorzowie Wlkp. do zapoznania z dokumentami, o których mowa w §1. Wzór oświadczenia o zapoznaniu się z tymi dokumentami stanowi załącznik nr 3.

§3. Traci moc Zarządzenie Wojewódzkiego Inspektora Ochrony Roślin i Nasiennictwa w Gorzowie Wlkp. nr 5/2008 z dnia 14 marca 2008 r. w sprawie podejmowanych środków ochrony danych osobowych przetwarzanych w Zintegrowanym Systemie Informatycznym w Ochronie Roślin i Nasiennictwie.

§4. Wykonanie Zarządzenia powierza się Samodzielnemu Stanowisku ds. Informatyki.

§5. Zarządzenie wchodzi w życie z dniem podpisania.

Wojewódzki Inspektor
Ochrony Roślin i Nasiennictwa
w Gorzowie Wlkp.
Ryszard Mróz
Ryszard Mróz

Aliceptys pod wzgl. formalno-prawnym
RADCA PRAWNY
Paweł Witt
RZG-G-292

Załącznik nr 1 do Zarządzenia nr 8/2013
z dnia 22 kwietnia 2013 r.

w sprawie wprowadzenia polityki bezpieczeństwa
danych osobowych i instrukcji zarządzania systemami
informatycznymi w Wojewódzkim Inspektoracie
Ochrony Roślin i Nasiennictwa w Gorzowie Wlkp.

Polityka bezpieczeństwa danych osobowych



SPIS TREŚCI

I.	Wprowadzenie	3
II.	Obszar przetwarzania danych osobowych	4
III.	Zbiory danych i systemy informatyczne do przetwarzania tych danych	5
IV.	Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi	9
V.	Sposób przepływu danych pomiędzy poszczególnymi systemami	12
VI.	Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych	12
	Załącznik nr 1. Arkusz aktualizacji	15

I. Wprowadzenie

1. Cel dokumentu

Polityka bezpieczeństwa danych osobowych wyznacza reguły i zasady ochrony danych osobowych w organizacji, a w szczególności:

- a) obszar przetwarzania danych osobowych,
- b) zbiory danych i systemy informatyczne do przetwarzania tych danych,
- c) opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi,
- d) sposób przepływu danych pomiędzy poszczególnymi systemami,
- e) środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

Polityka bezpieczeństwa dotyczy danych przetwarzanych zarówno w systemach informatycznych jak i zbiorach tradycyjnych (papierowych).

2. Wyjaśnienie pojęć

- a) **dane osobowe** – wszelkie informacje, poprzez które można zidentyfikować osobę fizyczną,
- b) **przetwarzanie danych osobowych** – jakiegokolwiek operacje wykonywane na danych osobowych, tj. zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonywane są w systemie informatycznym,
- c) **zбір danych osobowych** – zestaw danych posiadający strukturę o charakterze osobowym, dostępny według określonych kryteriów (np. rejestr, ewidencja, baza danych),
- d) **system informatyczny** – zbiór powiązanych ze sobą elementów (sprzęt, oprogramowanie itp.), których funkcją jest przetwarzanie danych osobowych przy użyciu techniki komputerowej,
- e) **administrator danych osobowych (ADO)** – osoba lub podmiot decydujący o celach i środkach przetwarzanych danych osobowych, funkcję tą sprawuje Lubuski Wojewódzki Inspektor Ochrony Roślin i Nasiennictwa,
- f) **administrator systemów informatycznych (ASI)** – osoba zajmująca się zarządzaniem danego systemu informatycznego m.in. rejestrowaniem i wyrejestrowaniem użytkownika, nadawaniem uprawnień,
- g) **administrator bezpieczeństwa informacji (ABI)** – osoba wyznaczona przez administratora danych, odpowiedzialna za bezpieczeństwo przetwarzanych

danych osobowych. Funkcję tą sprawuje Samodzielne stanowisko ds. informatyki,

- h) **sieć lokalna** – sieć komputerowa łącząca urządzenia komputerowe na określonym obszarze,
- i) **sieć publiczna** – sieć Internet,
- j) **elektroniczny nośnik danych** - płyta CD/DVD, pendrive, dysk twardy komputera,
- k) **poufność danych** – właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym osobom,
- l) **integralność danych** – właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieprawidłowy,
- m) **rozliczalność danych** – właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.

II. Obszar przetwarzania danych osobowych

1. Wojewódzki Inspektorat Ochrony Roślin i Nasiennictwa w Gorzowie Wlkp. przy ul. Zielenieckiej 11:

a) Parter:

- pomieszczenie biurowe nr 1 – Kierownik Działu Nadzoru Nasiennego,
- pomieszczenie biurowe nr 2 – Dział Nadzoru Nasiennego,
- pomieszczenie biurowe nr 3 – Kierownik Oddziału WI w Gorzowie Wlkp.,
- pomieszczenie biurowe nr 4 – Oddział WI w Gorzowie Wlkp.,
- pomieszczenie biurowe nr 5 – Dział Ochrony Roślin i Techniki,
- pomieszczenie nr 6 – serwerownia,
- pomieszczenie biurowe nr 7 – Kierownik Działu Nadzoru Fitosanitarnego,
- pomieszczenie biurowe nr 8 – Dział Nadzoru Nasiennego,
- pomieszczenie biurowe nr 9 – Administracja / Informatyk,
- pomieszczenie biurowe nr 10 – Kierownik Działu Ochrony Roślin i Techniki,
- pomieszczenie biurowe nr 11 – Kierownik Laboratorium Wojewódzkiego,
- pomieszczenie biurowe nr 12 – Laboratorium Wojewódzkie,
- magazyn pod schodami – niesprawne lub zużyte komputery z nośnikami danych,
- korytarz – drukarka / kserokopiarka.

b) I piętro:

- pomieszczenie biurowe nr 13 – Sekretariat,
- pomieszczenie biurowe nr 14 – Zastępca Wojewódzkiego Inspektora,
- pomieszczenie biurowe nr 15 – Wojewódzki Inspektor,
- pomieszczenie biurowe nr 16 – Kadry / Radca prawny,
- pomieszczenie biurowe nr 17 – Księgowość,
- pomieszczenie biurowe nr 18 – Główny księgowy,

- sala konferencyjna – kserokopiarka.

c) II piętro:

- archiwum zakładowe.

2. Jednostki organizacyjne Wojewódzkiego Inspektoratu:

- Delegatura WI w Zielonej Górze – ul. Olbrychta 10b
- Oddział WI w Krośnie Odrzańskim – ul. Poznańska 9,
- Oddział WI w Lubsku – ul. Powstańców Wielkopolskich 9,
- Oddział WI w Międzyrzeczu – ul. Krótka 2,
- Oddział WI w Nowej Soli – ul. Wojska Polskiego 30b,
- Oddział WI w Słubicach – ul. Kilińskiego 9h,
- Oddział WI w Strzelcach Krajeńskich - ul. Gorzowska 15,
- Oddział WI w Sulęcinie – ul. Nowokolejowa 1,
- Oddział WI w Świebodzinie – ul. 1-go Maja 22,
- Oddział WI we Wschowie – ul. Kazimierza Wielkiego 23,
- Oddział WI w Żaganiu – ul. Bema 15.

III. Zbiory danych i systemy informatyczne do przetwarzania tych danych

1. Objaśnienie systemów informatycznych, w których przetwarzane są dane osobowe :

- a) **Arkusz kalkulacyjny** – Microsoft Excel.
- b) **Edytor tekstu** – Microsoft Word.
- c) **ZSIORin** – Zintegrowany System Informatyczny w Ochronie Roślin i Nasiennictwie obsługiwany przez państwowych inspektorów w Wojewódzkim Inspektoracie Ochrony Roślin i Nasiennictwa w Gorzowie Wlkp. i w jego jednostkach organizacyjnych.
- d) **QNT Qwark** – program płacowy wspierający obliczanie i wypłatę wynagrodzeń. Obsługiwany przez pracownika na stanowisku ds. płacowych.
- e) **Lider KP** – system do obsługi kadrowo-płacowej, obsługiwany przez samodzielne stanowisko ds. kadr oraz pracownika na stanowisku ds. płacowych.
- f) **Videotel** – system do obsługi bankowości elektronicznej, obsługiwany przez pracownika na stanowisku ds. obrotu gotówkowego i ewidencji operacji gospodarczych.
- g) **Program Z-12** - program do rejestracji i kontroli sprawozdania Z-12 dla GUS, obsługiwany przez samodzielne stanowisko ds. kadr oraz pracownika ds. płacowych.

- h) **ePUAP** - ogólnopolska platforma teleinformatyczna służąca do komunikacji obywateli z jednostkami administracji publicznej.
- i) **CEIDG** – Centralna Ewidencja i Informacja o Działalności Gospodarczej, ogólnopolski system teleinformatyczny zawierający spis przedsiębiorców będących osobami fizycznymi.

2. Zbiory danych i systemy informatyczne

Lp.	Zbiór danych	System informatyczny / forma papierowa	Budynek, pomieszczenie, kondygnacja
1	Ewidencja dostawców	ZSIORiN, edytor tekstu	- WIORiN w Gorzowie Wlkp., pomieszczenia nr 1-4, parter - jednostki organizacyjne WIORiN
2	Ewidencja przedsiębiorców	ZSIORiN, edytor tekstu	- WIORiN w Gorzowie Wlkp., pomieszczenia nr 1-4, parter - jednostki organizacyjne WIORiN
3	Ewidencja rolników	ZSIORiN, edytor tekstu	- WIORiN w Gorzowie Wlkp., pomieszczenia nr 1-4, parter - jednostki organizacyjne WIORiN
4	Wykaz próbobiorców	ZSIORiN, edytor tekstu, forma papierowa	- WIORiN w Gorzowie Wlkp., pomieszczenia nr 1,2, parter - budynek Delegatury - Pracownia Oceny Nasion, parter
5	Wykaz kwalifikatorów	ZSIORiN, edytor tekstu, forma papierowa	- WIORiN w Gorzowie Wlkp., pomieszczenia nr 1,2, parter - budynek Delegatury - Pracownia Oceny Nasion, parter
6	Rejestr przedsiębiorców prowadzących obrót środkami ochrony roślin	ZSIORiN, edytor tekstu, arkusz kalkulacyjny, forma papierowa	- WIORiN w Gorzowie Wlkp., pomieszczenia nr 5,10, parter
7	Rejestr IP i wydanych certyfikatów IP	ZSIORiN, arkusz kalkulacyjny, forma papierowa	- WIORiN w Gorzowie Wlkp., pomieszczenia nr 5,10, parter
8	Ewidencja jednostek upoważnionych do prowadzenia szkoleń	ZSIORiN, edytor tekstu, forma papierowa	- WIORiN w Gorzowie Wlkp., pomieszczenia nr 5,10, parter
9	Ewidencja jednostek upoważnionych do przeprowadzania badań sprawności technicznej opryskiwaczy	ZSIORiN, edytor tekstu, forma papierowa	- WIORiN w Gorzowie Wlkp., pomieszczenia nr 5,10, parter
10	Rejestr osób przeszkolonych	ZSIORiN, edytor tekstu, forma papierowa	- WIORiN w Gorzowie Wlkp., pomieszczenia nr 1-4, parter - jednostki organizacyjne WIORiN
11	Rejestr przedsiębiorców	ZSIORiN, edytor tekstu, arkusz kalkulacyjny, forma papierowa	- WIORiN w Gorzowie Wlkp., pomieszczenie nr 7, parter - jednostki organizacyjne WIORiN
12	Krajowy System Ewidencji Producentów, Ewidencji Gospodarstw Rolnych oraz Ewidencji Wniosków o Przyznanie Płatności	forma papierowa	- WIORiN w Gorzowie Wlkp., pomieszczenia 5,10, parter - jednostki organizacyjne WIORiN

13	Centralna Ewidencja i Informacja o Działalności Gospodarczej	system informatyczny CEIDG	- WIORiN w Gorzowie Wlkp., pomieszczenia nr 5, 10
14	Ewidencja występowania organizmów szkodliwych	edytor tekstu, arkusz kalkulacyjny, forma papierowa	- WIORiN w Gorzowie Wlkp., pomieszczenie nr 7, parter
15	Sprawozdanie z badań	ZSIORiN, edytor tekstu, forma papierowa	- WIORiN w Gorzowie Wlkp., pomieszczenia nr 7, 11, 12, parter - jednostki organizacyjne WIORiN
16	Protokoły z pobrania prób	ZSIORiN, forma papierowa	- WIORiN w Gorzowie Wlkp., pomieszczenia nr 7, 11, 12, parter - jednostki organizacyjne WIORiN
17	Rejestr skarg i wniosków	forma papierowa	- WIORiN w Gorzowie Wlkp., pomieszczenie nr 13, I piętro
18	Rejestr upoważnień do kontroli	edytor tekstu, forma papierowa	- WIORiN w Gorzowie Wlkp., pomieszczenie nr 13, I piętro
19	Rejestr wniosków o udzielenie informacji publicznej	forma papierowa	- WIORiN w Gorzowie Wlkp., pomieszczenie nr 13, I piętro
20	Rejestr otrzymanej korespondencji	forma papierowa	- WIORiN w Gorzowie Wlkp., pomieszczenie nr 13, I piętro
21	Rejestr wysłanej korespondencji	forma papierowa	- WIORiN w Gorzowie Wlkp., pomieszczenie nr 13, I piętro
22	Rejestr wpływających faktur	forma papierowa	- WIORiN w Gorzowie Wlkp., pomieszczenie nr 13, I piętro
23	Rejestr delegacji	forma papierowa	- WIORiN w Gorzowie Wlkp., pomieszczenie nr 13, I piętro
24	Korespondencja ePUAP	ePUAP	- WIORiN w Gorzowie Wlkp., pomieszczenia nr 9, 13-14
25	Ewidencja mandatów karnych	edytor tekstu, forma papierowa	- WIORiN w Gorzowie Wlkp., pomieszczenie nr 9, parter
26	Dane płacowe	QNT Qwark, Płatnik, Lider KP, Videotel, forma papierowa	- WIORiN w Gorzowie Wlkp., pomieszczenia nr 17-18, I piętro
27	Świadczenia ZFŚS	Lider KP, arkusz kalkulacyjny, forma papierowa	- WIORiN w Gorzowie Wlkp., pomieszczenia nr 16-18, I piętro
28	Obsługa gotówkowa i bezgotówkowa PKZP	arkusz kalkulacyjny, forma papierowa	- WIORiN w Gorzowie Wlkp., pomieszczenie nr 17, I piętro
29	Rejestr umów cywilno-prawnych	forma papierowa	- WIORiN w Gorzowie Wlkp., pomieszczenia nr 17-18, I piętro
30	Dane kadrowe	Lider KP, forma papierowa	- WIORiN w Gorzowie Wlkp., pomieszczenie nr 16, I piętro
31	Akta personalne pracowników	edytor tekstu, forma papierowa	- WIORiN w Gorzowie Wlkp., pomieszczenie nr 16, I piętro
32	Sprawozdanie Z-12 GUS	Program Z-12	- WIORiN w Gorzowie Wlkp., pomieszczenie nr 16, I piętro

IV. Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi

Lp.	Nazwa zbioru danych	Pola informacyjne	Powiązanie
1	Ewidencja dostawców	dane podmiotów (nazwa pełna / nazwisko i imię, nazwa skrócona, kraj, nr NIP, nr REGON, nr zagraniczny, adres e-mail, nr rejestracyjny, nr decyzji, nr zaświadczenia, nr PESEL, miejscowość siedziby, miejscowość poczty, data rejestracji od/do, data wyrejestrowania od/do)	tak
2	Ewidencja przedsiębiorców	dane podmiotów (nazwa pełna / nazwisko i imię, nazwa skrócona, kraj, nr NIP, nr REGON, nr zagraniczny, adres e-mail, nr rejestracyjny, nr decyzji, nr zaświadczenia, nr PESEL, miejscowość siedziby, miejscowość poczty, data rejestracji od/do, data wyrejestrowania od/do)	tak
3	Ewidencja rolników	dane podmiotów (nazwa pełna / nazwisko i imię, nazwa skrócona, kraj, nr NIP, nr REGON, nr zagraniczny, adres e-mail, nr rejestracyjny, nr decyzji, nr zaświadczenia, nr PESEL, miejscowość siedziby, miejscowość poczty, data rejestracji od/do, data wyrejestrowania od/do)	tak
4	Wykaz próbobiorców	dane próbobiorky (identyfikator, imię i nazwisko)	tak
5	Wykaz kwalifikatorów	dane kwalifikatora (identyfikator, imię i nazwisko)	tak
6	Rejestr przedsiębiorców prowadzących obrót środkami ochrony roślin	nazwa przedsiębiorcy, miejscowość, ulica, nr domu, nr mieszkania	tak
7	Rejestr IP i wydanych certyfikatów IP	nazwisko, imię, nazwa, miejscowość, ulica, nr domu, nr mieszkania, kod pocztowy, poczta, gmina, powiat	tak
8	Ewidencja jednostek upoważnionych do prowadzenia szkoleń	nazwa upoważnionej jednostki, adres upoważnionej jednostki	tak
9	Ewidencja jednostek upoważnionych do przeprowadzania badań sprawności technicznej opryskiwaczy	nazwa upoważnionej jednostki, adres upoważnionej jednostki	tak
10	Rejestr osób przeszkolonych	imię i nazwisko, adres zamieszkania, PESEL, NIP	tak
11	Rejestr przedsiębiorców	imię, nazwisko, adres zamieszkania, NIP, PESEL, regon, adres zamieszkania (ulica, nr domu, miejscowość), adres e-mail, fax, nr telefonu, nr rejestracyjny	tak
12	Ewidencja występowania organizmów szkodliwych	imię, nazwisko, adres zamieszkania, NIP, PESEL, regon, adres zamieszkania (ulica, nr domu, miejscowość), adres e-mail, fax, nr telefonu, nr rejestracyjny	tak
13	Sprawozdanie z badań	imię, nazwisko, nazwa, adres, wykryte organizmy szkodliwe	tak

14	Protokoły z pobrania prób	nr PPP, Nr lab. Próbk/próbek, imię i nazwisko próbobiorky, producent, właściciel, imię i nazwisko osoby sporządzającej, imię i nazwisko osoby autoryzującej, imię i nazwisko osoby zatwierdzającej	tak
15	Rejestr upoważnień do kontroli	imię i nazwisko osoby upoważnionej, numer upoważnienia	tak
16	Korespondencja ePUAP	imię, nazwisko, PESEL, NIP, ulica, budynek, lokal, miasto, kod pocztowy, poczta	tak
17	Centralna Ewidencja i Informacja o Działalności Gospodarczej	imię, nazwisko, NIP, województwo, miejscowość, ulica, numer lokalu, nr nieruchomości	tak
18	Ewidencja mandatów karnych	numer mandatu, data ukarania mandatem, imię i nazwisko ukaranego, adres ukaranego, kwota	tak
19	Dane płacowe	<p>QNT Qwark:</p> <ul style="list-style-type: none"> • Podstawowe dane pracownika: nr ewidencyjny, imię i nazwisko, data rozpoczęcia pracy, staż pracy. • Dane personalne, adres zamieszkania: drugie imię, data urodzenia, PESEL, stawka zasadnicza, seria i nr dowodu osobistego, NIP, miejsce urodzenia, nazwisko rodowe matki, imię matki, imię ojca, miejsce zamieszkania (kraj, województwo, powiat, gmina ulica, miejscowość, kod pocztowy, telefon, data zameldowania), data zameldowania; • pożyczki i kredyty: składnik płacy, spłata od-do, pierwsza rata, następna rata; • rachunek bankowy, przelewy: rodzaj przelewu, wypłata normalna, wypłaty dodatkowe, składnik płacy, nazwa oddziału, nr rachunku; • <p>Płatnik:</p> <ul style="list-style-type: none"> • id płatnika, NIP, PESEL, seria i numer dokumentu tożsamości, nazwa skrócona płatnika, imię, nazwisko, data urodzenia, kod pocztowy, miejscowość, gmina, ulica, nr domu, lokalu; <p>Lider KP</p> <ul style="list-style-type: none"> • Karta zatrudnionego: numer, nazwisko, imię1, imię2, nazwisko rodowe, data urodzenia, stan cywilny, PESEL, NIP, Seria i nr dowodu osobistego, seria i nr paszportu; • Adres zameldowania na stałe miejsce pobytu: miejscowość, kod pocztowy, poczta, ulica, nr domu, nr lokalu, gmina, powiat, województwo, telefon, adres e-mail • Adres zamieszkania: miejscowość, kod pocztowy, poczta, ulica, nr domu, nr lokalu, gmina, powiat, województwo, telefon, adres e-mail • Listy płac: Numer, imię nazwisko, wartość; • Akcje socjalne: data, nazwa świadczenia, wartość; • Angaże: data angażu, płaca zasadnicza, typ płacy; 	tak

		<ul style="list-style-type: none"> • Inne: nr rachunku; • Rodzina: imię, nazwisko, data urodzenia, pokrewieństwo, zasiłek rodzinny; • Nagrody i kary: data, rodzaj nagrody lub kary, opis kary lub nagrody; <p>Videotel</p> <ul style="list-style-type: none"> • Kartoteka adresowa: nazwa firmy (osoba fizyczna), nazwa rachunku, właściciel, ulica, miasto kraj; • Rachunki: rachunek, nazwa rachunku, waluta, typ, bank, informacja, właściciel (imię i nazwisko). 	
20	Świadczenia ZFŚS	imię i nazwisko, nr konta rozrachunków, kwota brutto dofinansowania z zfśś	tak
21	Obsługa gotówkowa i bezgotówkowa PKZP	nazwisko i imię, adres prywatny, udzielone poręczenia spłaty pożyczek, wkłady konto (winien, ma, saldo), pożyczki konto (winien, ma, saldo), obroty konta (winien, ma, saldo).	tak
22	Dane kadrowe	<p>Lider KP</p> <ul style="list-style-type: none"> • Karta zatrudnionego: numer, nazwisko, imię1, imię2, nazwisko rodowe, data urodzenia, stan cywilny, PESEL, NIP, Seria i nr dowodu osobistego, seria i nr paszportu; • Adres zameldowania na stałe miejsce pobytu: miejscowość, kod pocztowy, poczta, ulica, nr domu, nr lokalu, gmina, powiat, województwo, telefon, adres e-mail • Adres zamieszkania: miejscowość, kod pocztowy, poczta, ulica, nr domu, nr lokalu, gmina, powiat, województwo, telefon, adres e-mail • Listy płac: Numer, imię nazwisko, wartość; • Akcje socjalne: data, nazwa świadczenia, wartość; • Angaże: data angażu, płaca zasadnicza, typ płacy; • Inne: nr rachunku; • Rodzina: imię, nazwisko, data urodzenia, pokrewieństwo, zasiłek rodzinny; • Nagrody i kary: data, rodzaj nagrody lub kary, opis kary lub nagrody; 	tak
23	Sprawozdanie Z-12	identyfikator, imię, nazwisko, wykształcenie, rok i miesiąc urodzenia, wynagrodzenie osobowe ogółem brutto, premie regulaminowe, dodatki za pracę zmianową, wynagrodzenie zasadnicze, nagrody i premie uznaniowe, honoraria, dod. wynagrodzenie roczne	tak

V. Sposób przepływu danych pomiędzy poszczególnymi systemami

1. W Wojewódzkim Inspektoracie oraz jego jednostkach organizacyjnych przepływ informacji pomiędzy zbiorem danych, a systemem informatycznym jest dwukierunkowy (odczyt i zapis).
2. ZSIORiN pracuje na serwerach Głównego Inspektoratu Ochrony Roślin i Nasiennictwa w Warszawie. Dostęp do systemu jest możliwy wyłącznie poprzez sieć publiczną.
3. Dostęp do systemu Lider KP, Z-12 możliwy jest z pojedynczego stanowiska komputerowego oraz komputera w sieci lokalnej.
4. Dostęp do systemów: Videotel, Płatnik, możliwy jest z pojedynczego stanowiska komputerowego.
5. Dane z systemu Lider KP są eksportowane, a następnie importowane w systemie Płatnik oraz VideoTel.
6. W poniższych systemach przesyłanie danych za pośrednictwem sieci publicznej następuje w sposób szyfrowany:
 - a) Zintegrowany System Informatyczny w Ochronie Roślin i Nasiennictwie (serwer produkcyjny i testowy),
 - b) Płatnik,
 - c) Videotel,
 - d) ePUAP,
 - e) CEIDG,
 - f) Program Z-12.

VI. Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

1. Środki ochrony fizycznej:
 - a) budynki i/lub pomieszczenia Wojewódzkiego Inspektoratu oraz jednostek organizacyjnych posiadają jedno z niżej wymienionych zabezpieczeń antywłamaniowych:
 - system alarmowy wraz całodobowym monitoringiem,
 - fizyczna ochrona budynku,
 - okratowanie,
 - podwójne zamki w drzwiach wejściowych.
 - b) dokumentacja papierowa, elektroniczne nośniki danych oraz stanowiska komputerowe służące do przetwarzania danych osobowych znajdują się w pomieszczeniach zamykanych na oddzielny klucz,
 - c) przebywanie osób nieupoważnionych w pomieszczeniach objętych obszarem przetwarzania dopuszczalne jest za zgodą administratora danych osobowych lub w obecności pracownika upoważnionego,

- d) pracownicy przed opuszczeniem pomieszczenia:
- zamykają okna,
 - zabezpieczają dokumentację papierową i elektroniczne nośniki danych w szufladach, szafach biurowych, metalowych lub pancernych,
 - klucze do szafek zabezpieczane są przed dostępem osób nieupoważnionych,
 - w przypadku czasowego opuszczenia - blokują komputer, a po zakończonej pracy wyłączają komputer.
- e) w chwili opuszczenia pomieszczenia przez ostatniego pracownika, drzwi zamykane są na klucz (konieczne jest usunięcie klucza z zamka), dotyczy to również opuszczania pomieszczeń w godzinach pracy,
- f) osoba użytkująca komputer przenośny zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania,
- g) serwer oraz macierze dyskowe są zabezpieczone dodatkowo w szafie teleinformatycznej zamykanej na klucz,
- h) dostęp do pomieszczenia serwerowni posiada administrator bezpieczeństwa informacji oraz osoby posiadające jego zgodę.

2. Środki sprzętowe, informatyczne i telekomunikacyjne.

- a) administrator bezpieczeństwa informacji monitoruje zabezpieczenia systemu informatycznego w imieniu administratora danych osobowych,
- b) stosuje się logiczne zabezpieczenia w celu ochrony przed nieuprawnionym dostępem
- ruch na styku z siecią publiczną jest na bieżąco monitorowany w celu kontroli przepływu danych między siecią publiczną a siecią jednostki oraz kontroli działań w sieciach,
 - system wykrywania intruzów.
- c) na wszystkich komputerach zainstalowane jest licencjonowane oprogramowanie,
- d) serwer oraz komputery chroni program antywirusowy oraz programowa zaporą ogniową „firewall”,
- e) baza sygnatur programu antywirusowego jest uaktualniana raz dziennie w sposób automatyczny,
- f) na każdym stanowisku komputerowym system operacyjny zabezpieczony jest hasłem,
- g) systemy operacyjne są automatycznie uaktualniane poprzez najnowsze aktualizacje i poprawki zabezpieczeń,
- h) poczta wychodząca i przychodząca jest automatycznie skanowana przez program antywirusowy,

- i) monitory ustawione są tak, aby ograniczyć dostęp do danych osobom nieupoważnionym do przetwarzania danych,
- j) zastosowanie zasilaczy awaryjnych UPS chroni serwer oraz komputery przed zanikami zasilania – użytkownik posiada krótką rezerwę czasu, aby zapisać dane, wylogować się z systemu i wyłączyć komputer.

3. Niszczenie elektronicznych nośników danych i dokumentacji papierowej:

- a) dokumentacja papierowa, w przypadku której wystąpiła konieczność usunięcia danych osobowych, niszczone jest wyłącznie w niszczarce dokumentów,
- b) płytę CD z danymi osobowymi należy zniszczyć w niszczarce dokumentów z funkcją niszczenia płyt CD; w przypadku braku niszcarki z powyższą funkcją, nośnik należy przekazać ABI lub uszkodzić mechanicznie, poprzez kilkukrotne przełamanie nośnika,
- c) dysk twardy lub pendrive przeznaczony do likwidacji jest mechanicznie uszkodzany,
- d) dysk twardy komputera przekazywanego jako zbędny lub zużyty składnik majątku jest „zerowany” programowo, w celu uniemożliwienia odzyskania; czynności te wykonuje ABI.

Arkusz aktualizacji

Lp.	Data	Czego dotyczy aktualizacja	Zakres aktualizacji	Imię i Nazwisko osoby dokonującej zmiany

Załącznik nr 2 do Zarządzenia nr 8/2013
z dnia 22 kwietnia 2013 r.

w sprawie wprowadzenia polityki bezpieczeństwa
informacji i instrukcji zarządzania systemami
informatycznymi w Wojewódzkim Inspektoracie
Ochrony Roślin i Nasiennictwa w Gorzowie Wlkp.

Instrukcja zarządzania systemami informatycznymi



SPIS TREŚCI

I.	Wprowadzenie	3
II.	Nadawanie oraz rejestrowanie uprawnień w systemie informatycznym	4
III.	Metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem.....	5
IV.	Rozpoczęcie, zawieszenie i zakończenie pracy w systemie informatycznym	6
V.	Tworzenia kopii zapasowych.....	6
VI.	Sposób, miejsce i okres przechowywania elektronicznych nośników informacji oraz kopii zapasowych zawierających dane osobowe.	7
VII.	Zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest nieuprawnionego dostępu do systemu informatycznego lub ingerencja w ten system.....	8
VIII.	Sposób odnotowywania przez system informatyczny informacji o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia.	8
IX.	Przeglądy i konserwacje systemów oraz nośników informacji służących do przetwarzania danych	9
	Załącznik nr 1. Arkusz aktualizacji.....	10
	Załącznik nr 2. Ewidencja osób upoważnionych do przetwarzania danych osobowych.....	11

I. Wprowadzenie

1. Instrukcja określa reguły zarządzania systemami informatycznymi, w których przetwarzane są dane osobowe, a w szczególności:
 - a) nadawanie oraz rejestrowanie uprawnień w systemie informatycznym,
 - b) metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem,
 - c) rozpoczęcie, zawieszenie i zakończenie pracy w systemie informatycznym,
 - d) tworzenie kopii zapasowych,
 - e) sposób, miejsce i okres przechowywania elektronicznych nośników informacji oraz kopii zapasowych zawierających dane osobowe,
 - f) zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest nieuprawnionego dostępu do systemu informatycznego lub ingerencja w ten system,
 - g) sposób odnotowywania przez system informatyczny informacji o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia,
 - h) przeglądy i konserwacje systemów oraz nośników informacji służących do przetwarzania danych.
2. Uwzględniając kategorie przetwarzanych danych oraz zagrożenia wprowadza się wysoki poziom bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym.
3. Wyjaśnienie pojęć:
 - a) **wysoki poziom bezpieczeństwa** – środki bezpieczeństwa określone w Rozporządzeniu MSWiA 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,
 - b) **identyfikator (login)** – niepowtarzalna nazwa przypisana konkretnemu użytkownikowi w systemie informatycznym, podczas uwierzytelniania wraz z hasłem umożliwia dostęp do systemu,
 - c) **koordynator ZSIORiN** – koordynuje działania w WIORiN Gorzów Wlkp. z zakresu pracy w Zintegrowanym Systemie Informatycznym w Ochronie Roślin i Nasiennictwie,
 - d) **rejestracja użytkownika** – założenie konta dla użytkownika w systemie informatycznym zawierającego identyfikator, hasło, uprawnienia,
 - e) **wyrejestrowanie użytkownika** – usunięcie konta użytkownika z systemu informatycznego.

II. Nadawanie oraz rejestrowanie uprawnień w systemie informatycznym

1. Systemy informatyczne mogą być używane tylko na potrzeby realizacji działań nałożonych na Wojewódzki Inspektorat Ochrony Roślin i Nasiennictwa w Gorzowie Wlkp.
2. Administratorem danych osobowych systemu informatycznego ZSIORiN jest Główny Inspektor Ochrony Roślin i Nasiennictwa z siedzibą w Warszawie.
3. Do pracy w systemie informatycznym może być dopuszczona wyłącznie osoba posiadająca upoważnienie do przetwarzania danych osobowych.
4. ADO w porozumieniu z samodzielnym stanowiskiem ds. kadr prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych w systemie informatycznym (Załącznik nr 2 do instrukcji).
5. Ewidencja zawiera: imię i nazwisko upoważnionego pracownika, jednostkę organizacyjną, datę nadania/ustania upoważnienia, zakres upoważnienia (system informatyczny), uprawnienia oraz identyfikator.
6. Upoważnienia do przetwarzania danych osobowych przechowywane są razem z aktami osobowymi pracowników.
7. Rejestracja użytkownika w systemie informatycznym następuje po wpisaniu do ewidencji osób upoważnionych, wyrejestrowanie – po usunięciu z ewidencji.
8. Rejestrowania oraz wyrejestrowania użytkownika dokonuje:
 - w przypadku systemu ZSIORiN – Administrator Systemu Informatycznego w Głównym Inspektoracie Ochrony Roślin i Nasiennictwa w Warszawie, poprzez Koordynatora systemu ZSIORiN,
 - w przypadku pozostałych systemów - ABI, który dokonuje tej czynności w porozumieniu z Administratorem Systemu Informatycznego.
9. Po zarejestrowaniu:
 - w przypadku systemu ZSIORiN – Koordynator ZSIORiN,
 - w przypadku pozostałych systemów – ABI,przekazuje użytkownikowi identyfikator, hasło początkowe, zakres dostępu, rolę na wydruku papierowym oraz informuje o obowiązku zmiany hasła początkowego.
10. Jeśli upoważniony pracownik pracuje poza siedzibą Wojewódzkiego Inspektoratu, identyfikator, hasło początkowe wysyłane są pocztą elektroniczną z zaszyfrowanym załącznikiem, którego hasło do odszyfrowania zna Koordynator System ZSI i pracownik upoważniony.
11. Użytkownikom nadaje się uprawnienia tylko w niezbędnych do pracy modułach i funkcjach.
12. Wyrejestrowanie użytkownika następuje wskutek rozwiązania umowy lub zmiany zakresu obowiązków.
13. Administrator Bezpieczeństwa Informacji nadaje Administratorowi Systemów Informatycznych uprzywilejowane uprawnienia w systemie informatycznym.

14. W zależności od systemu funkcję Administratora Systemu Informatycznego pełni: Główny księgowy, Samodzielne stanowisko ds. kadr, Samodzielne stanowisko ds. informatyki.
15. W przypadku systemu ZSIORiN administratorem systemu informatycznego jest pracownik Głównego Inspektoratu Ochrony Roślin i Nasiennictwa w Warszawie.
16. Dla każdego użytkownika rejestruje się odrębny i niepowtarzalny identyfikator.
17. Przyznawany identyfikator powinien jednoznacznie identyfikować, weryfikować i autoryzować tożsamość użytkownika.
18. Identyfikator użytkownika, który został wyrejestrowany, nie jest przydzielany innemu pracownikowi.

III. Metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem

1. Dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po uwierzytelnieniu się tj. poprawnym wpisaniu identyfikatora i hasła.
2. Użytkownik jest odpowiedzialny za swoje hasło, w tym za jego okresową zmianę i utrzymanie w tajemnicy, również po utracie jego ważności.
3. W przypadku wykorzystania tego hasła przez osoby trzecie pracownik ponosi konsekwencje wynikające z właściwych w tym zakresie przepisów prawa.
4. Zabrania się przekazywania haseł jakimkolwiek innym osobom.
5. Użytkownik jest odpowiedzialny za dostosowanie hasła do opisanych niżej obowiązujących reguł, jeśli przestrzegania tych reguł nie wymusza w sposób automatyczny system informatyczny.
6. Hasło początkowe należy niezwłocznie zmienić.
7. W przypadku ujawnienia lub podejrzenia ujawnienia hasła należy je niezwłocznie zmienić.
8. Hasło musi spełniać następujące wymagania:
 - minimalna długość: 8 znaków,
 - zawierać małe i wielkie litery, oraz cyfry lub znaki specjalne,
 - nie może zawierać wyrazów słownikowych,
 - nie może być identyczne jak identyfikator użytkownika,
 - zmiana hasła nie rzadziej niż co 30 dni,
 - nie może powtórzyć się 5 (pięć) poprzednich haseł.
9. Zabronione jest zapisywanie hasła na obudowie monitora, komputera, klawiaturze, lub innym łatwo dostępnym miejscu.
10. Użytkownik, który nie może zalogować się do systemu informatycznego przy użyciu aktualnego hasła zobowiązany jest zgłosić ten fakt bezzwłocznie
 - w przypadku ZSIORiN - Koordynatorowi Systemu, który kontaktuje się z Administratorem Systemu Informatycznego w Głównym Inspektoracie Ochrony Roślin i Nasiennictwa,

- w przypadku pozostałych systemów: Administratorowi Systemu Informatycznego, który kontaktuje się z Administratorem Bezpieczeństwa Informacji,

w celu wygenerowania nowego hasła.

11. Hasła Administratora Systemu Informatycznego mogą być znane Administratorowi Bezpieczeństwa Informacji. Przechowuje się je w zalakowanej kopercie w zabezpieczonym miejscu. Otwarcie koperty może nastąpić wyłącznie w przypadku uzasadnionej konieczności w porozumieniu z Administratorem Danych Osobowych.

12. Punkt 10 powyższej Instrukcji nie dotyczy systemu informatycznego ZSIORiN.

IV. Rozpoczęcie, zawieszenie i zakończenie pracy w systemie informatycznym

1. Aby rozpocząć pracę w systemie informatycznym:

- a) należy włączyć komputer,
- b) odczekać aż uruchomi się system operacyjny, wpisać prawidłowe hasło,
- c) uruchomić system informatyczny poprzez otwarcie odpowiedniej aplikacji bądź przeglądarki internetowej,
- d) zalogować się poprzez wpisanie identyfikatora oraz hasła.

2. Jeżeli użytkownik chce zawiesić (wstrzymać) pracę, powinien: wcisnąć jednocześnie trzy (3) klawisze: Ctrl + Alt + Delete i wybrać opcję „Zablokuj komputer”, a w przypadku laptopa - zamknąć pokrywę. Samoczynne blokowanie następuje po 30 minutach nieaktywności w systemie operacyjnym.

3. Aby zakończyć pracę w systemie informatycznym:

- a) zapisać lub zatwierdzić zmiany,
- b) wylogować się z systemu, zamknąć przeglądarkę lub aplikację,
- c) po zakończeniu pracy należy zakończyć pracę systemu operacyjnego poprzez opcję: Start -> Zamknij system, zabronione jest kończenie pracy przez odłączenie zasilania komputera,
- d) odczekać, aż komputer się wyłączy,
- e) wyłączyć monitor,
- f) sprawdzić, czy nośniki informacji zawierające dane osobowe nie zostały pozostawione bez nadzoru.

V. Tworzenia kopii zapasowych

1. Zbiory danych są zabezpieczone przed zniszczeniem lub utratą poprzez:

- a) zastosowanie zasilaczy awaryjnych UPS,
- b) sporządzanie kopii zapasowych.

2. W zależności od systemu informatycznego bazy danych są przechowywane na:

- a) lokalnych komputerach,
- b) zdalnych serwerach nie będących własnością Wojewódzkiego Inspektoratu Ochrony Roślin i Nasiennictwa (ZSIORiN, ePUAP, CEIDG).

3. Poniższe procedury dotyczą tworzenia kopii zapasowych baz danych programów kadrowo-płacowych, zainstalowanych na lokalnych komputerach.
4. Kopia zapasowa pełna zawiera kopię bazy danych oraz kopię systemu informatycznego, sporządza ją Administrator Bezpieczeństwa Informacji przynajmniej raz na miesiąc.
5. Kopia zapasowa przyrostowa – wyznaczeni pracownicy na podstawie odrębnych instrukcji przynajmniej raz na dzień, jeśli wprowadzane są dane do bazy danych.
6. Kopia zapasowa pełna sporządzana jest również przed aktualizacją systemów informatycznych.
7. Kopie zapasowe pełne oraz przyrostowe przechowywane są dodatkowo na oddzielnych partycjach dysku twardego są kompresowane i szyfrowane przez ABI.

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

1. Elektroniczne nośniki danych oraz kopie zapasowe przechowywane są w pokojach stanowiących obszar przetwarzania danych.
2. Elektroniczne nośniki danych po zakończeniu pracy przez użytkowników systemu są przechowywane w szufladach, szafach biurowych, metalowych lub pancernych zamykanych na klucz.
3. Kopie zapasowe przechowywane są w pomieszczeniach biurowych WIORiN nr 9, 16-17.
4. Dostęp do kopii zapasowych posiada Administrator Systemów Informatycznych, Administrator Bezpieczeństwa Informacji oraz wyznaczeni pracownicy.
5. Elektroniczne nośniki danych oraz kopie zapasowe oznaczane są krótkim opisem oraz datą, informacja ta umożliwia identyfikację zbioru danych i datę jego sporządzenia.
6. Sposób niszczenia elektronicznych nośników informacji zawiera pkt. VI polityki bezpieczeństwa.
7. Okres przechowywania kopii zapasowych:
 - przyrostowe: 30 dni,
 - pełne: 12 miesięcy,
 - roczne: 5 lat.

VII. Zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest nieuprawnionego dostępu do systemu informatycznego lub ingerencja w ten system

1. Na każdym komputerze zainstalowany jest program antywirusowy oraz programowa zaporą ogniową firewall.
2. Wymienione powyżej zabezpieczenia są aktualizowane w sposób automatyczny.
3. W przypadku wykrycia oprogramowania złośliwego, system wyświetla odpowiedni komunikat, po czym użytkownik przekazuje tę informację ABI.
4. Nośniki danych podłączone do komputera są automatycznie sprawdzane przez oprogramowanie antywirusowe.
5. Administrator Bezpieczeństwa Informacji instaluje najnowsze dostępne oprogramowanie antywirusowe udostępniane przez producenta, zgodnie z posiadaną licencją.
6. Oprogramowanie antywirusowe sprawdza pocztę przychodzącą oraz wychodzącą.
7. Poczta elektroniczna jest zabezpieczona przed przesyłaniem nie zamówionej informacji handlowej (SPAM) na serwerach Głównego Inspektoratu w Warszawie.

VIII. Sposób odnotowywania przez system informatyczny informacji o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia.

1. Kopia danych osobowych przesłanych do:

a) Zakładu Ubezpieczeń Społecznych

przechowywana jest w bazie danych programu Płatnik, w postaci dokumentów i zestawów dokumentów oznaczonych odpowiednim statusem dokumentu lub zestawu, datą utworzenia dokumentu, datą wysłania zestawu, identyfikatorem osoby tworzącej zestaw i numerem zestawu,

b) Narodowego Banku Polskiego w Zielonej Górze

przechowywana jest w bazie danych systemu VIDEOTEL w postaci zestawów dokumentów oznaczonych nazwą, statusem, statusem, datą utworzenia, datą wysłania, identyfikatorem osoby tworzącej i potwierdzającej.

IX. Przeglądy i konserwacje systemów oraz nośników informacji służących do przetwarzania danych

1. Przeglądy i konserwacje służą zachowaniu ciągłości pracy i bezpieczeństwa danych systemów informatycznych.
2. Przegląd obejmuje:
 - sprawdzenie stanu pamięci dyskowej,
 - test pamięci RAM,
 - sprawdzenie konfiguracji i komunikatów systemowych,
 - sprawdzenie przydatności nośników danych oraz kopii zapasowych.
3. Konserwacja obejmuje:
 - usuwanie zbędnych plików pozostawionych po codziennej pracy z komputerem przez różnego typu aplikacje,
 - defragmentację dysku twardego,
 - skanowanie dysków twardych programem antywirusowym,
 - instalacja najnowszego oprogramowania oraz aplikacji,
 - czyszczenie wnętrza komputera z kurzu,
 - ocenę stanu: kondensatorów płyty głównej, chłodzenia, zasilacza,
 - poprawność podłączenia przewodów,
 - usunięcie usterek, wymiana wadliwych podzespołów i błędów logicznych.
4. Powyższe czynności przeprowadzane są na bieżąco przez Administratora Bezpieczeństwa Informacji.
5. Nieprawidłowości w trakcie przeglądów bądź konserwacji są niezwłocznie usuwane.
6. W przypadku wystąpienia awarii systemu informatycznego lub utraty danych Administrator Bezpieczeństwa Informacji w porozumieniu z Administratorem Systemu Informatycznego odtwarza dane za pomocą aktualnej kopii zapasowej.
7. Komputer przeznaczony do naprawy w firmie zewnętrznej pozbawiany jest dysku twardego.
8. Dysk twardy lub pendrive przeznaczony do likwidacji jest mechanicznie uszkodzany, natomiast dysk twardy komputera zbędnego lub zużytego przeznaczonego do przekazania dla innej jednostki, jest „zerowany” programowo, w celu uniemożliwienia odzyskania; czynności te wykonuje ABI.

Arkusz aktualizacji

Lp.	Data	Czego dotyczy aktualizacja	Zakres aktualizacji	Imię i Nazwisko osoby dokonującej zmiany

Ewidencja osób upoważnionych do przetwarzania danych osobowych

Lp.	Nazwisko	Imię	Jednostka organizacyjna	Data nadania upoważnienia	Data ustania upoważnienia	Zakres upoważnienia	Uprawnienia	Identyfikator

Załącznik nr 3 do Zarządzenia nr 8/2013
z dnia 22 kwietnia 2013 r.

w sprawie wprowadzenia polityki bezpieczeństwa
informacji i instrukcji zarządzania systemami
informatycznymi w Wojewódzkim Inspektoracie
Ochrony Roślin i Nasiennictwa w Gorzowie Wlkp.

.....
(imię i nazwisko pracownika)

.....
(jednostka organizacyjna)

OŚWIADCZENIE

Oświadczam, że zapoznałam się z polityką bezpieczeństwa danych osobowych oraz instrukcją zarządzania systemami informatycznymi Wojewódzkiego Inspektoratu Ochrony Roślin i Nasiennictwa w Gorzowie Wlkp.

.....
(data i czytelny podpis pracownika)