OŚRODEK TECHNIKI LEŚNEJ
63-460 Jarocin, ul. Przemysłowa 2D
Bank Zachodni WBK S.A. Oddział Jarocin
91 1090 1131 0000 0000 1300 9303
tel. (62) 7472582, fax 062/7472933
Nr ident. NIP 617-00-03-354
REGON 250027011

ZARZĄDZENIE NR 24 /15

Dyrektora Ośrodka Techniki Leśnej w Jarocinie

znak: FE.0210.1.2015

z dnia 21 grudnia 2015 roku

w sprawie wprowadzenie dokumentacji opisującej sposób przetwarzania i zabezpieczenia informacji.

Na podstawie art. 36 ustawy z dnia 29.08.1997r. o ochronie danych osobowych (Dz. U. z 2014 r. poz. 1182 ze zm.) i Rozporządzenia Ministra Spraw Wewnętrznych i Administracji 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) **zarządzam**, co następuje:

§ 1

1. W Ośrodku Techniki Leśnej w Jarocinie wprowadza się:
   1) Polityka bezpieczeństwa informacji, która stanowi załącznik nr 1 do niniejszego zarządzenia;
   2) Politykę Bezpieczeństwa Przetwarzania Danych Osobowych, która stanowi załącznik nr 2 do niniejszego zarządzenia;
   3) Instrukcję Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych, która stanowi załącznik nr 3 do zarządzenia;
   4) Instrukcję Postępowania w Sytuacji Naruszenia Bezpieczeństwa Informacji, która stanowi załącznik nr 4 do zarządzenia.
2. Nadzór nad przestrzeganiem postanowień dokumentacji ochrony danych osobowych oraz stosowania niniejszego Zarządzenia sprawuje wyznaczony przez dyrektora Ośrodka koordynator ds. bezpieczeństwa informacji w osobie Kierownika działu Księgowo-ekonomicznego.

§ 2

1. Stosowanie przepisów ustawy o ochronie danych osobowych jest obowiązkiem każdego pracownika Ośrodka Techniki Leśnej w Jarocinie.
2. Przed podjęciem pracy przez nowo zatrudnianego pracownika, pracodawca jest zobowiązany do zapoznania go z przepisami dotyczącymi ochrony danych osobowych.
3. Zapoznanie z przepisami o ochronie danych pracownik potwierdza podpisaniem oświadczenia o znajomości tych przepisów.

§ 3

Zobowiązuje się wszystkich pracowników do zapoznania się z postanowieniami niniejszego zarządzenia i przestrzegania ich realizacji,

§ 4

Zarządzenie wchodzi w życie z dniem podpisania.

Otrzymują kierownicy działów z obowiązkiem zapoznania pracowników działu:

1. F-
2. Kier.działu ZW-
3. Kier.działu ZP-
4. Kier.działu ZA-
5. Kier.działu ZM-
6. Stan. DK-
7. Sekretariat-
8. Dział FE-a/a

DYREKTOR ZAKŁADU

inż. Ryszard Misiek

Załącznik nr 1
do Zarządzenia Nr 24
Dyrektora Ośrodka Techniki Leśnej w Jarocinie
z dnia 21 grudnia 2015 roku

POLITYKA BEZPIECZEŃSTWA INFORMACJI

§ 1

WSTĘP

1. Ośrodek Techniki Leśnej w Jarocinie wdrożył Politykę Bezpieczeństwa Informacji w celu zachowania bezpieczeństwa, poufności, integralności i dostępności posiadanych informacji oraz zapewnienia wysokiej jakości usług świadczonych na rzecz klientów Ośrodka.
2. Politykę bezpieczeństwa informacji należy rozumieć, jako zestaw praw, reguł i praktycznych doświadczeń regulujących sposób zarządzania, ochrony i dystrybucji informacji wewnątrz Ośrodka. Jest obowiązującym dokumentem określającym procedury przetwarzania informacji w formie tradycyjnej jak i zarządzania systemami informatycznymi służącymi do przetwarzania tych informacji ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji.
3. Dokument opisuje procedury bezpieczeństwa informacji zawartych w zbiorach tradycyjnych (papierowych) oraz w systemach informatycznych Ośrodka Techniki Leśnej w Jarocinie. Opisane zbiory zasad i procedur określają granice dopuszczalnego zachowania wszystkich użytkowników systemu informatycznego wspomagającego pracę Ośrodka. Dokument zawiera również opis konsekwencji, jakie mogą ponieść osoby przekraczające określone granice oraz procedury postępowania dla zapobiegania i minimalizowania skutków zagrożeń.

§ 2

CEL

Celem Polityki Bezpieczeństwa Informacji jest:

1. zapewnienie ochrony danych osobowych,
2. podnoszenie wiedzy i świadomości pracowników przetwarzających dane osobowe,
3. zaangażowanie wszystkich pracowników w ochronę informacji,
4. zmniejszenie ryzyka utraty informacji,
5. zapewnienie ciągłości działania Ośrodka.

§ 3

DOKUMENT

1. Polityka Bezpieczeństwa Informacji dotyczy wszystkich pracowników, stażystów oraz praktykantów Ośrodka Techniki Leśnej w Jarocinie.
2. Polityka realizowana jest przez:
   1) szkolenia pracowników,
   2) wdrażanie oprogramowania wspomagającego,
   3) tworzenie procedur i instrukcji,
   4) zapewnienie zgodności z wymaganiami prawnymi oraz regulacjami wewnętrznymi,

5) monitorowanie stanu zabezpieczeń środków technicznych, organizacyjnych oraz zasobów informatycznych,
6) informowanie pracowników o konsekwencjach wynikających z braku należytej dbałości o bezpieczeństwo informacji lub naruszenia bezpieczeństwa informacji,
7) raportowanie incydentów związanych z bezpieczeństwem informacji.

§ 4

PRZEPISY PRAWA

1. Niniejszy dokument zgodny jest z przepisami prawa:
   1) ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r. poz. 1182, ze zm.),
   2) 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),
   3) Rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2012 r. poz. 526).

§ 5

ZABEZPIECZENIA INFORMACJI

1. Każda informacja mająca wpływ na funkcjonowanie Ośrodka powinna być chroniona.
2. Chronione przede wszystkim powinny być dane osobowe przetwarzane przez Ośrodek oraz dokumentacja projektowa.
3. Dokumentacja projektowa powinna być chroniona na każdym szczeblu i przez każdego pracownika mającego dostęp do dokumentacji.
4. Dostęp do danych powinien odbywać się zgodnie z ustalonymi procedurami.
5. Dane w formie papierowej i elektronicznej powinny być chronione przed zagrożeniami mającymi wpływ na żywotność dokumentacji.
6. Dane należy chronić na każdym etapie tworzenie dokumentacji by zminimalizować ryzyko utraty danych.
7. Kopie bezpieczeństwa danych powinny być przechowywane przynajmniej w innym pomieszczeniu niż oryginały.
8. Dostęp do danych powinien być nadzorowany i ograniczony tylko do niezbędnych osób.

§ 6

OGRANICZENIA

1. Należy pamiętać, że wszystkie dane (w tym dokumentacja projektowa) przetwarzane przez Ośrodek podlegają ochronie i przekazywanie informacji bez zezwolenia może być potraktowane jako naruszenie przepisów między innymi:

1) Kodeks Kary - Art. 266. § 1. Kto, wbrew przepisom ustawy lub przyjętemu na siebie zobowiązaniu, ujawnia lub wykorzystuje informację, z którą zapoznał się w związku z pełnioną funkcją, wykonywaną pracą, działalnością publiczną, społeczną, gospodarczą lub naukową, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do2 lat.

2) Kodeks Karny - Art. 267. § 1. Kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

§ 2. Tej samej karze podlega, kto bez uprawnienia uzyskuje dostęp do całości lub części systemu informatycznego.

§ 3. Tej samej karze podlega, kto w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem.

DYREKTOR ZAKŁADU

inż. Ryszard Misiek

Załącznik nr 2
do Zarządzenia Nr ..24
Dyrektora Ośrodka Techniki Leśnej w Jarocinie
z dnia 21 grudnia 2015 roku

POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH

ROZDZIAŁ I

Postanowienia ogólne

§ 1

1. Politykę bezpieczeństwa należy rozumieć, jako zestaw praw, reguł i praktycznych doświadczeń regulujących sposób zarządzania, ochrony i dystrybucji informacji o danych osobowych wewnątrz organizacji. Jest obowiązującym dokumentem określającym procedury przetwarzania danych osobowych w formie tradycyjnej jak i zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji w Ośrodku Techniki Leśnej w Jarocinie.
2. Dokument opisuje procedury bezpieczeństwa danych osobowych zawartych w zbiorach tradycyjnych (papierowych) oraz w systemach informatycznych Ośrodka. Opisane zbiory zasad i procedur określają granice dopuszczalnego zachowania wszystkich użytkowników systemu informatycznego wspomagającego pracę Ośrodka. Dokument zawiera również opis konsekwencji, jakie mogą ponieść osoby przekraczające określone granice oraz procedury postępowania dla zapobiegania i minimalizowania skutków zagrożeń.
3. Celem utworzenia dokumentacji jest podniesienie bezpieczeństwa dokumentów i systemów informatycznych, w których są gromadzone i przetwarzane dane oraz określenie odpowiedzialności pracowników za prawidłowe działanie tych systemów i bezpieczeństwo przetwarzanych w nim danych.
4. Administratorem Danych jest Ośrodek Techniki Leśnej w Jarocinie reprezentowane przez Dyrektora Ośrodka.
5. Ośrodek przetwarza dane osobowe:
   1) własnych pracowników;
   2) byłych pracowników Ośrodka;
   3) kontrahentów Ośrodka;
   4) innych osób, na przetwarzanie których zezwalają przepisy prawa lub posiadają zgodę tych osób.
6. Niniejszy dokument zgodny jest z przepisami prawa:
   1) Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 poz. 1182 ze zm.)
   2) 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. 2004 nr 100 poz. 1024).

§ 2

„Polityka" zawiera:
1) wykaz budynków oraz pomieszczeń stanowiących obszar, gdzie przetwarzane są dane osobowe (załącznik nr 1);
2) wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych oraz struktury zbiorów danych osobowych (załącznik nr 2);
3) sposób przepływu danych pomiędzy poszczególnymi systemami (załącznik nr 3);
4) określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych (załącznik nr 4);

5) Wzór upoważnienia do przetwarzania danych osobowych (załącznik nr 5);
6) Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych (załącznik nr 6).

ROZDZIAŁ II
Organizacja przetwarzania danych osobowych

§ 3

Administrator Danych realizuje zadania w zakresie ochrony danych osobowych, w tym zwłaszcza:
1) podejmuje decyzje o celach i środkach przetwarzania danych osobowych z uwzględnieniem przede wszystkim zmian w obowiązującym prawie, organizacji administratora danych, oraz technik zabezpieczenia danych osobowych,
2) upoważnia poszczególne osoby do przetwarzania danych osobowych w określonym indywidualnym zakresie, odpowiadającym zakresowi jej obowiązków,
3) może wyznaczyć Koordynator ds. bezpieczeństwa informacji oraz określa zakres jego zadań i obowiązków,
4) podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia procedur bezpieczeństwa przetwarzania danych osobowych.

§ 4

1. Koordynator ds. bezpieczeństwa informacji realizuje zadania w zakresie nadzoru nad przestrzeganiem procedur i zasad ochrony danych osobowych, w tym zwłaszcza:
   1) nadzorowanie opracowania i aktualizowania dokumentacji bezpieczeństwa,
   2) zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych;
   3) koordynuje wewnętrzne audyty przestrzegania przepisów o ochronie danych osobowych,
   4) nadzoruje udostępnianie danych osobowych odbiorcom danych i innym podmiotom,
   5) przygotowuje wnioski zgłoszeń rejestracyjnych i aktualizacyjnych zbiorów danych oraz prowadzi inną korespondencję z Generalnym Inspektorem Ochrony Danych Osobowych, Biurem Generalnego Inspektora Ochrony Danych Osobowych.

§ 5

Administrator SILP realizuje zadania w zakresie zarządzania i bieżącego nadzoru nad systemem informatycznym Administratora Danych, w tym zwłaszcza:
1) zarządza systemem informatycznym zlokalizowanym w Ośrodku, w którym przetwarzane są dane osobowe, posługując się hasłem dostępu do wszystkich stacji roboczych z poziomu administratora,
2) przeciwdziała dostępowi osób niepowołanych do systemu informatycznego,
3) zakłada konta w systemie informatycznym w związku z zatrudnieniem pracownika;
4) przydziela uprawnienia w systemach informatycznych upoważnionym użytkownikom zgodnie z przekazanym wnioskiem,
5) dokonuje zmian w systemie informatycznym zgodnie z przekazanym wnioskiem,
6) nadzoruje stosowanie mechanizmów uwierzytelniania użytkowników poprzez kontrolę poprawności użytkowania kont,
7) w sytuacjach stwierdzenia naruszenia zabezpieczeń systemu informatycznego, informuje Administratora Danych o naruszeniu i współdziała z nim przy usuwaniu skutków naruszenia,
8) podejmuje działania służące zapewnieniu niezawodności zasilania komputerów, innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych oraz zapewnieniu bezpiecznej wymiany danych w sieci wewnętrznej i bezpiecznej teletransmisji.

§ 6

Pracownicy realizują zadania w zakresie ochrony danych osobowych zawartych z zbiorach, do których mają dostęp, a w szczególności zobowiązani są do:

1) przestrzegania zasad przetwarzania danych osobowych zapisanych w dokumentacji bezpieczeństwa przetwarzania danych osobowych,
2) przekazywania koordynatorowi ds. bezpieczeństwa informacji oraz bezpośredniemu przełożonemu wszelkich niezgodności związanych z ochroną danych osobowych,
3) informowania koordynatora ds. bezpieczeństwa informacji o zmianach zaistniałych w przetwarzanych zbiorach, .
4) niezwłocznego powiadomienia bezpośredniego przełożonego i koordynatora ds. bezpieczeństwa informacji w sytuacji, gdy pracownik uzna, że dane osobowe zostały bądź są bezprawnie przetwarzane,
5) dopilnowania by w umowach z firmami, które będą miały dostęp do danych osobowych lub innych ważnych informacji dla Urzędu były zawarte klauzule odnoszące się do poufności informacji.

ROZDZIAŁ III
Obowiązek informacyjny

§ 7

1. Kierownicy tych komórek organizacyjnych Ośrodka, którzy zbierają i przetwarzają dane osobowe, są odpowiedzialni za poinformowanie osób, których dane przetwarzają o:
   1) adresie siedziby Ośrodka, pod którym dane są zbierane i przetwarzane.
   2) celu zbierania danych, dobrowolności lub obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.
   3) prawie wglądu do treści swoich danych oraz możliwości ich poprawiania.
2. W przypadku zbierania danych osobowych nie bezpośrednio od osoby, której one dotyczą, osobę tę należy poinformować ponadto o:
   1) źródle danych.
   2) Uprawnieniach wynikających z art. 32 ust. 1 pkt. 7 i 8 Ustawy.
3. Administrator danych zwolniony jest z obowiązku wynikającego z pkt. 1 i 2 w przypadkach, gdy:
   1) przepis innej ustawy zezwala na przetwarzanie danych bez ujawniania faktycznego celu ich zbierania,
   2) osoba, której dane dotyczą, posiada informacje, o których mowa w pkt 1 i 2.
4. Wzór dokumentów stosowanych dla spełnienia przez Ośrodek obowiązków wymienionych w ust. 1 i 2, o ile nie gwarantują spełnienia tego obowiązku inne dokumenty wypełniane i podpisywane przez zainteresowaną osobę, zatwierdzany jest przez koordynatora ds. bezpieczeństwa informacji.

ROZDZIAŁ IV
Przekazywanie danych osobowych poza obszar Ośrodka

§ 8

1. Zgodnie z obwiązującymi przepisami dane osobowe udostępniane są tylko i wyłącznie na pisemny, umotywowany wniosek.
2. Wszystkie udostępnienia danych są ewidencjonowane.
3. Ewidencja zawiera informacje o tym, kto jest odbiorcą danych, datę kiedy zostały udostępnione oraz jaki zakres danych został udostępniony.
4. Dane mogą być przekazywane tylko na pisemny wniosek.

5. Dane mogą być udostępniane, przesyłane jednostkom, którym akty prawne zezwalają na otrzymywanie takich danych.
6. Podczas przekazywania danych osobowych poza obszar przetwarzania danych osobowych należących do Ośrodka dane zabezpiecza się przed ich nieuprawnionym dostępem
7. Dane przesyłane drogą teleinformatyczną muszą być odpowiednio zabezpieczone przed utratą ich poufności i integralności za pomocą zabezpieczeń kryptograficznych, umożliwiających ich bezpieczne przesyłanie.

ROZDZIAŁ VI
Postanowienia końcowe

§ 9

1. O wszystkich przypadkach naruszenia, podejrzenia naruszenia ochrony danych osobowych użytkownik zobowiązany jest powiadomić koordynatora ds. bezpieczeństwa informacji, zgodnie z „Instrukcją postępowania w sytuacji naruszenia ochrony danych osobowych".
2. Wobec osoby, która w przypadku naruszenia ochrony danych osobowych, zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także nie zrealizowała stosownego działania dokumentującego ten przypadek, wszczyna się postępowanie dyscyplinarne.
3. Pracownik zajmujący się sprawami kadrowymi zobowiązany jest prowadzić ewidencję osób, które zostały zapoznane z niniejszym dokumentem oraz które przetwarzają dane osobowe w Ośrodku.
4. Koordynator ds. bezpieczeństwa informacji zobowiązany jest do przeprowadzania przeglądu polityki bezpieczeństwa przynajmniej raz w roku. Przegląd powinien się opierać przede wszystkim na zgodności polityki bezpieczeństwa z aktami prawa oraz wewnętrznymi dokumentami.
5. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane, jako naruszenie obowiązków pracowniczych, w szczególności przez osobę, która wobec naruszenia zabezpieczenia systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie powiadomiła o tym koordynatora ds. bezpieczeństwa informacji.
6. Polityka bezpieczeństwa jak i dokumenty będące załącznikami do polityki bezpieczeństwa obowiązują wszystkich pracowników Ośrodka.
7. Procedury i zasady zawarte w niniejszym dokumencie jak i jego załącznikach obowiązują, także stażystów, praktykantów oraz inne osoby, które mają dostęp do przetwarzania danych osobowych w Ośrodka.
8. Orzeczona kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia koordynatora ds. bezpieczeństwa informacji nie wyklucza odpowiedzialności karnej tej osoby zgodnie z ustawą z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. z 2014 r. poz. 1182 z późn. zm.) oraz możliwość wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.
9. W sprawach nieuregulowanych niniejszym dokumentem mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. z 2014 r. poz. 1182), rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024).

DYREKTOR ZAKŁADU

inż. Ryszard Misiek

Załącznik nr 1
do Polityki bezpieczeństwa
przetwarzania danych osobowych

Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe

1. Pomieszczenia Ośrodka, w których przetwarzane są dane osobowe zlokalizowane są w budynkach przy ulicy Przemysłowa 2D, 63-200 Jarocin.
2. Dane osobowe mogą być przetwarzane przez pracowników Ośrodka którzy zostali do tego upoważnieni.
3. Dane osobowe przetwarzane są także w COPD (Centralnych Ośrodkach Przetwarzania Danych) zgodnie z umową powierzenia podpisaną przez Ośrodek.

DYREKTOR ZAKŁADU

inż. Ryszard Misiek

Załącznik nr 2
do Polityki bezpieczeństwa
przetwarzania danych osobowych

Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych oraz struktura przetwarzanych danych

1. Dane osobowe w Ośrodku są przetwarzane w zbiorach przedstawionych w poniższej tabeli.
2. Tabela przedstawia także programy stosowane do przetwarzania danych osobowych w zbiorach a także lokalizacje przetwarzania.
3. Struktury zbiorów danych osobowych opisane zostały w dokumentacji dotyczącej systemów informatycznych.
4. Wszystkie dane przetwarzane są także w formie tradycyjnej.

Lp.	Nazwa zbioru danych	Użyte programy do przetwarzania danych	Struktura	Miejsce przetwarzania	Zgłoszenie
1.	*Dane przetwarzane w związku z zatrudnieniem pracowników*	• SIŁP • Płatnik • Pakiet biurowy • Tradycyjnie	Imiona, nazwiska, nazwisko rodowe, tytuł naukowy, NIP, PESEL, dane adresowe, data urodzenia, miejsce urodzenia, płeć, składniki i kwoty wynagrodzenia, kwoty składek ubezpieczeniowych, zaliczki podatku, kwoty potrąceń, imiona, nazwiska, data i miejsce urodzenia dziecka, imiona rodziców, stan rodziny, wykształcenie, zawód, odbyte szkolenia, informacje o poprzednim zatrudnieniu, informacje o służbie wojskowej, informacje o nagrodach i karach, staż pracy, stanowisko służbowe, stopień zawodowy, absencja, urlopy, seria i numer dowodu osobistego, seria i numer książeczki	Budynek Ośrodka	Zwolnione ze zgłoszenia art. 43 ust. 1 pkt 4

			wojskowej, numer paszportu,		
2.	*Dane osobowe byłych pracowników*	• SILP • Płatnik • Pakiet biurowy • Tradycyjnie	Imiona, nazwiska, nazwisko rodowe, tytuł naukowy, NIP, PESEL, dane adresowe, data urodzenia, miejsce urodzenia, płeć, składniki i kwoty wynagrodzenia, kwoty składek ubezpieczeniowych, zaliczki podatku, kwoty potrąceń, imiona, nazwiska, data i miejsce urodzenia dziecka, imiona rodziców, stan rodziny, wykształcenie, zawód, odbyte szkolenia, informacje o poprzednim zatrudnieniu, informacje o służbie wojskowej, informacje o nagrodach i karach, staż pracy, stanowisko służbowe, stopień zawodowy, absencja, urlopy, seria i numer dowodu osobistego, seria i numer książeczki wojskowej, numer paszportu,	Budynek Ośrodka	Zwolnione ze zgłoszenia art. 43 ust. 1 pkt 4
3.	*Dane osób przesyłane w CV*	• Pakiet biurowy	Imię, nazwisko, dane zawarte w przesyłanych aplikacjach	Budynek Ośrodka	Zwolnione ze zgłoszenia art. 43 ust. 1 pkt 4
4.	*Dziennik korespondencyjny*	• Tradycyjnie	Imię, nazwisko, adres zamieszkania,	Budynek Ośrodka	Zwolnione ze zgłoszenia art. 43 ust. 1 pkt 12
5.	*Dane zawarte w zamówieniach publicznych*	• Tradycyjnie	Imię, nazwisko, adres zamieszkania, NIP, uprawnienia specjalistyczne (np. budowlane) osób uczestniczących w realizacji zamówienia	Budynek Ośrodka	Zwolnione ze zgłoszenia art. 43 ust. 1 pkt 9
6.	*Monitoring kamer*	• zapis na nośniku elektronicznym	Wizerunek osób	Budynek Ośrodka	
7.	*Dane księgowe*	• SILP • Aplikacja bankowa	Imiona, nazwiska, wysokość przelewu, numer rachunku bankowego, dane adresowe, PESEL, NIP	Budynek Ośrodka	Zwolnione ze zgłoszenia art. 43 ust. 1 pkt 8
8.	*Dane dostawców*	• SILP	Imiona, nazwiska, wysokość przelewu, numer rachunku bankowego, dane adresowe, PESEL, NIP	Budynek Ośrodka	Zwolnione ze zgłoszenia art. 43 ust. 1 pkt 4, 8

9.	*Klienci stacji diagnostycznej*	• Stacja SQL	Imiona, nazwiska, adres, nazwa firmy, numer rejestracyjny, numer telefonu	Budynek Ośrodka	Zwolnione ze zgłoszenia art. 43 ust. 1 pkt 8
10.	*Baza klientów, odbiorców*	• SILP	Imiona, nazwiska, wysokość przelewu, numer rachunku bankowego, dane adresowe, NIP, dane przewoźników	Budynek Ośrodka	

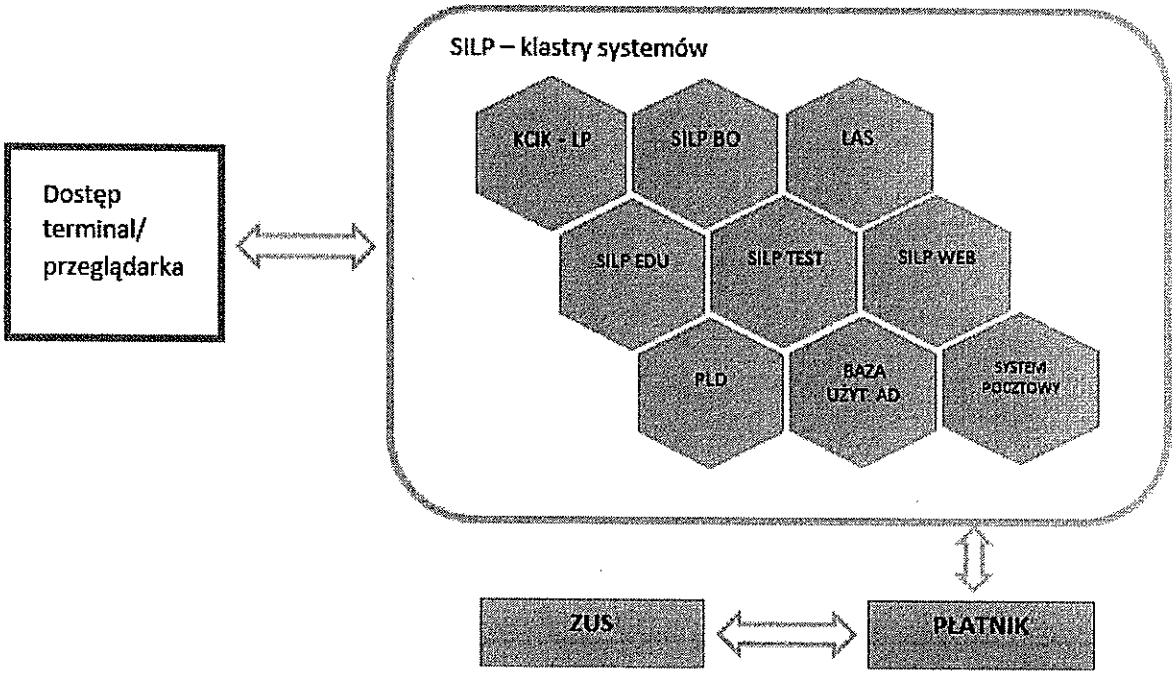
DYREKTOR ZAKŁADU

inż. Ryszard Misiek

Załącznik nr 3
do Polityki bezpieczeństwa
przetwarzania danych osobowych

Sposób przepływu danych pomiędzy poszczególnymi systemami.

Przepływ danych pomiędzy systemami informatycznymi obrazują zamieszczone poniżej grafiki.



DYREKTOR ZAKŁADU

inż. Ryszard Misiek

Załącznik nr 4
do Polityki bezpieczeństwa
przetwarzania danych osobowych

Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności integralności i rozliczalności przetwarzanych danych.

Środki organizacyjne

1. Został wyznaczony Koordynator ds. bezpieczeństwa informacji.
2. W Ośrodku funkcjonuje administrator SILP, którego zadaniem jest zapewnienie prawidłowego funkcjonowania systemu informatycznego.
3. Dla podniesienia świadomości pracowników, a także dla spisania procedur została przygotowana Polityka bezpieczeństwa definiująca zachowania pracowników przy przetwarzaniu danych osobowych, z którą muszą zapoznać się wszyscy pracownicy Ośrodka.
4. Przygotowane i spisane zostały, także szczegółowe zasady zachowania się przy przetwarzaniu danych osobowych w systemach informatycznych. Zasady te zostały spisane w „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych".
5. Koordynator ds. bezpieczeństwa informacji odpowiedzialny jest za nadzór nad odpowiednim przestrzeganiem ochrony danych osobowych.
6. Każdy użytkownik przetwarzający dane osobowe w Ośrodku posiada pisemne upoważnienie do przetwarzania danych osobowych wydane przez Administratora Danych.
   1) Osoba zajmująca się sprawami kadrowymi przygotowuje upoważnienie do przetwarzania danych osobowych.
   2) Administrator Danych podpisuje upoważnienie.
   3) Osoba zajmująca się sprawami kadrowymi aktualizuje ewidencję osób upoważnionych do przetwarzania danych osobowych.
2. Upoważnienia do przetwarzania danych osobowych, przechowywane są w teczce zawierającej wszystkie upoważnienia.
3. Pracownikom Ośrodka, którzy nie przetwarzają danych osobowych, ale przebywają w pomieszczeniach przetwarzania danych osobowych zostały wydane upoważnienia do przebywania w pomieszczeniach przetwarzania danych osobowych.
4. Dokumentacja ewidencji osób upoważnionych do przetwarzania danych osobowych przechowywana jest w zamkniętym niedostępnym dla osób nieupoważnionych miejscu.
5. Do przetwarzania danych osobowych nie może zostać dopuszczona osoba nieposiadająca upoważnienia nadanego przez Administratora Danych.
6. Każdy użytkownik, który przetwarza dane osobowe został przeszkolony z ochrony danych osobowych.
7. Każdy użytkownik jest odpowiedzialny za odpowiednie zabezpieczenie danych osobowych, na których pracuje oraz które przechowuje w formie tradycyjnej (papierowej) jak i w formie elektronicznej.
8. Pracownik odpowiedzialny jest za właściwe zabezpieczenie danych gromadzonych w formie tradycyjnej poprzez odpowiednie ich zabezpieczenie przed dostępem osób nieupoważnionych.
9. Formę uporządkowania dokumentacji wewnętrznej danego działu określa bezpośrednio przełożony, kierownik działu i jest on odpowiedzialny za wdrożenie tych zasad.
10. W Ośrodku stosowana jest zasada „czystego biurka". Oznacza ona, że na stanowisku pracy powinny znajdować się dokumenty tylko te, na których obecnie pracownik pracuje. Inne dokumenty powinny być schowane.
11. Dane w formie papierowej przechowywane są w zabezpieczonych pomieszczeniach.

12. Dane na stanowiskach pracy są odpowiednio zabezpieczane przed ich nieupoważnionym zdobyciem poprzez zabezpieczanie danych w zamykanych szafkach.
13. Dane w formie papierowej archiwizowane są zgodnie z wewnętrznymi regulacjami.
14. Dane zarchiwizowane przechowywane są w pomieszczeniach składnicy akt Ośrodka, do którego dostęp jest ograniczony.
15. W przypadku, gdy określone materiały papierowe nie podlegają wewnętrznym regulacjom, za ustalenie archiwizacji tych danych odpowiada kierownik właściwego działu.
16. Do likwidowania zbędnych dokumentów służą niszczarki dobierane według stopnia tajności danych.
17. Zabronione jest udzielania jakichkolwiek informacji dotyczących danych osobowych drogą telefoniczną, gdyż nie jesteśmy w stanie potwierdzić danych osoby dzwoniącej.
18. Pracownicy nie rzadziej niż raz na dwa lata przechodzą szkolenie z ochrony danych osobowych w celu przypomnienia zasad.
19. Każdy pracownik Ośrodka jest odpowiedzialny za przetwarzania danych osobowych zgodnych ze swoim zakresem obowiązków.

Środki techniczne

1. Teren, na którym znajdują się budynki Ośrodka jest ogrodzony.
2. Po godzinach pracy teren ten jest zamykany.
3. Wejścia do budynków zabezpieczone zostały za pomocą zamykanych drzwi.
4. Dostęp do kluczy posiadają tylko upoważnione osoby.
5. W budynkach został zainstalowany system alarmowy.
6. Do systemu alarmowego zostały podłączone czujniki ruchu.
7. W budynkach zostały rozgraniczone strefy bezpieczeństwa, do których dostęp posiadają tylko upoważnione osoby.
8. W budynkach w oznakowanych miejscach zostały rozstawione gaśnice przeciwpożarowe.
9. Dostęp do komputerów posiadają tylko upoważnione osoby.
10. Dostęp do aplikacji, na których przetwarzane są dane osobowe zabezpieczony został za pomocą hasła.
11. Każdy użytkownik posiada indywidulany identyfikator oraz hasło logowania.
12. Na komputerach został zainstalowany program zabezpieczający przed działanie złośliwego oprogramowania.
13. Kopie bezpieczeństwa oprogramowania wykonywane są regularnie.

DYREKTOR ZAKŁADU

inż. Ryszard Misiak

Załącznik nr 5
do Polityki bezpieczeństwa
przetwarzania danych osobowych

Upoważnienie nr

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2014 poz. 1182 ze zm.)

Upoważniam Panią/Pana

Zatrudnioną/Zatrudnionego na stanowisku

Do przetwarzania danych osobowych w formie papierowej oraz do obsługi systemu informatycznego służącego do przetwarzania danych osobowych w Ośrodku Techniki Leśnej w Jarocinie w zakresie zgodnym z wykonywaną pracą.
Upoważnienie traci moc z chwilą ustania stosunku pracy/stażu/praktyki.

Zadania i czynności do wykonywania

1. Ochrona danych osobowych w systemie informatycznym i ręcznym, a w szczególności przeciwdziałanie dostępowi osób niepowołanych oraz przeciwdziałanie w przypadku wykrycia naruszeń zabezpieczeń systemu zgodnie z ustawą o ochronie danych osobowych (Dz. U. z 2014 poz. 1182 z póz. zm.).
2. Przestrzeganie zasad określonych w instrukcji określającej sposób zarządzania systemem informatycznym i ręcznym.
3. Przestrzeganie zasad określonych w instrukcji postępowania w sytuacji naruszania ochrony danych osobowych.

Administrator Danych

.....

Oświadczam, że zapoznałem(łam) się z przepisami prawa dotyczącymi ochrony danych osobowych, a w szczególności z ustawą z 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. z 2014r. poz. 1182 z późn. zm.) oraz rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z 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) i zobowiązuję się do ich przestrzegania.
Oświadczam ponadto, że zapoznałem(łam) się z wewnętrzną dokumentacją to jest: polityką bezpieczeństwa oraz instrukcją określającą sposób zarządzania systemem informatycznym, służącym przetwarzaniu danych osobowych ze szczególnym uwzględnieniem bezpieczeństwa informacji i instrukcją postępowania w sytuacji naruszenia ochrony danych osobowych.
Świadomy(a) odpowiedzialności porządkowej i karnej oświadczam, że znane mi dane osobowe będę przetwarzać zgodnie z prawem, i nie dopuszczę do bezprawnego naruszenia tajemnicy również w sytuacji, gdy ustanie moje zatrudnienie w Ośrodku Techniki Leśnej w Jarocinie.

.....
(podpis pracownika)

Jarocin, dnia .....

Załącznik nr 6
do Polityki bezpieczeństwa
przetwarzania danych osobowych

Lp.	*Nazwisko i Imię*	*Identyfikator (login)*	*Data nadania upoważnienia*	*Data odebrania upoważnienia*	*Zakres upoważnienia*	*Uwagi*

DYREKTOR ZAKŁADU

inż. Ryszard Misiek

Załącznik nr 3
do Zarządzenia Nr 24
Dyrektora Ośrodka Techniki Leśnej w Jarocinie
z dnia 21 grudnia 2015 roku

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

I. Postanowienia ogólne

1. Zasady określone w Rozporządzeniu 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. 2004 nr 100 poz.1024) dotyczące funkcjonowania Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych zostały ujęte w Zarządzeniu nr 58 Dyrektora Generalnego Lasów Państwowych z dnia 20 czerwca 2013 r. w sprawie zasad funkcjonowania i zasad bezpieczeństwa systemu informatycznego w Państwowym Gospodarstwie Leśnym Lasy Państwowe.
2. Do pracy w systemie informatycznym służącym do przetwarzania danych osobowych może zostać dopuszczona tylko i wyłącznie osoba posiadająca upoważnienie do przetwarzania danych osobowych wydane przez Administratora Danych.

II. Przetwarzanie danych osobowych

1. Praca na komputerach może odbywać się tylko w miejscach wyznaczonych do tego. Każdy pracownik posiada wydzielone miejsce pracy.
2. Za umożliwienie korzystania z komputera przez osobę nieupoważnioną odpowiada pracownik, któremu sprzęt ten został przydzielony.
3. Na każdym użytkowniku systemu informatycznego spoczywa odpowiedzialność za rodzaj i zakres danych przetwarzanych przez niego w ramach przydzielonych mu uprawnień systemowych i programowych, oraz odpowiedzialność za ochronę tych danych przed niepowołanym dostępem, niepowołaną modyfikacją, zniszczeniem, nielegalnym ujawnieniem lub pozyskaniem, w stopniu odpowiednim do zadań tej osoby przy przetwarzaniu danych osobowych.

III. Nadawanie uprawnień Rejestrowanie użytkownika

1. Za rejestracje i nadawanie uprawnień w systemie informatycznym odpowiedzialny jest Administrator SILP.
2. Bezpośredni przełożony pracownika składa wniosek o założenia konta w systemie informatycznym.
3. Nadanie uprawnień w systemie zatwierdzane jest przez Dyrektora Ośrodka.
4. Uprawnienia nadawane są zgodnie z wewnętrznymi instrukcjami.
5. Wgląd do uprawnień w systemie informatycznym dostępny jest w formie elektronicznej.
6. Każdemu użytkownikowi przypisywany jest indywidualny identyfikator.
7. Identyfikator budowany jest na podstawie wewnętrznych instrukcji.
8. Identyfikator, o którym mowa wyżej wpisywany jest do ewidencji osób upoważnionych.

Wyrejestrowanie użytkownika

1. Pracownik zajmujący stanowisko do spraw pracowniczych jest zobowiązany do niezwłocznego poinformowania Administratora SILP o zakończeniu stosunku pracy z użytkownikiem systemu informatycznego.
2. Administrator SILP blokuje identyfikator użytkownika, któremu upłynął termin lub zostało odebrane upoważnienie do przetwarzania danych osobowych, zgodnie z przekazanymi mu informacjami przez pracownika zajmującego stanowisko do spraw pracowniczych.
3. Administrator SILP wyrejestrowuje użytkowników z systemu informatycznego na wniosek przełożonego.

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

1. W Ośrodku jako metody uwierzytelniania można stosować karty chipowe wraz z kodem PIN lub identyfikatory użytkownika z hasłem.
2. Każdy użytkownik posiada indywidualną kartę chipową.
3. kod PIN może zawierać cyfry oraz litery.
4. Logowanie do stacji roboczych oraz poczty może odbywać się przy pomocy kart chipowych.
5. Logowanie do systemu informatycznego odbywa się za pomocą identyfikatora (loginu) oraz hasła.
6. Hasło logowania powinno zawierać minimum 8 znaków, w tym duże i małe litery oraz cyfrę lub znak specjalny.
7. Hasło logowania powinno być regularnie zmieniane.
8. Hasło powinno być znane tylko i wyłącznie użytkownikowi.
9. Nie wolno podawać hasła osobom trzecim.
10. Hasło nie może być widoczne na ekranie podczas jego wpisywania.
11. Zabrania się zapisywania hasła w łatwo dostępnym miejscu.

Hasło administracyjne

1. Administrator SILP ustala hasło administracyjne.
2. Hasło administracyjne do systemu informatycznego powinien znać tylko Administrator SILP.
3. Otwarcie koperty może zostać dokonane tylko i wyłącznie, gdy Administrator SILP nie jest dostępna.

V. Procedura rozpoczęcia, zawieszenia i zakończenia pracy

1. Administrator SILP zobowiązany jest do sprawdzenia poprawności uruchomienia systemu informatycznego oraz urządzeń wspomagających w razie zauważenia nieprawidłowości w uruchomieniu systemu powinien zablokować dostęp użytkowników do systemu i jak najszybciej usunąć usterkę.
2. Administrator SILP w razie pojawienia się problemów z poprawnym działaniem systemu lub brakiem zasilania elektrycznego, zobowiązany jest do sprawdzenia przyczyn awarii.
3. Po awaryjnym przerwaniu pracy komputera, np. zanik napięcia w sieci energetycznej, należy sprawdzić czy zostały zapisane ostatnio wprowadzane dane do używanych w tym czasie programów.
4. Administrator SILP monitoruje logowanie oraz wylogowanie użytkowników z systemu.

Rozpoczęcie pracy

1. W razie podejrzenia prób włamania do systemu, pomieszczenia użytkownik zobowiązany jest niezwłocznie powiadomić o tym fakcie bezpośredniego przełożonego.
2. Bezpośredni dostęp do systemu przetwarzania danych osobowych może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła.
3. W przypadku pojawienia się trudności w autoryzacji, pomimo prawidłowo wpisanej nazwy użytkownika i hasła, użytkownik zobowiązany jest skontaktować się z Administratorem SILP.

Przerywanie pracy

1. Przerywając pracę użytkownik, który opuszcza swoje stanowisko i pomieszczenie pracy zobowiązany jest do zablokowania systemu.
2. Użytkownik udostępniający stanowisko pracy innej upoważnionej osobie musi wylogować się z systemu.

Zakończenie pracy w systemie

1. Zakończenie pracy polega na wylogowaniu użytkownika i zakończeniu pracy systemu.
2. Wyłączenie komputera może nastąpić wyłącznie po uprzednim zamknięciu wszystkich aktywnych aplikacji (programów):
3. Kategorycznie zabrania się wyłączać komputery w czasie działania programu przyciskiem „POWER" lub „RESET", gdyż takie działanie może spowodować trwałe uszkodzenie zbiorów danych. Nie należy wyłączać przewodów zasilających i sieciowych z gniazda elektrycznego.

VI. Procedura tworzenia kopii zapasowych

1. Za sporządzanie i bezpieczeństwo kopii danych elektronicznych, przetwarzanych w Ośrodku odpowiedzialny jest Administrator SILP.
2. Kopie bezpieczeństwa wykonywane są automatycznie.
3. Odpowiednie mechanizmy archiwizują dane zgodnie z ustawieniami automatycznymi.
4. Kopie bezpieczeństwa powinny być wykonywane regularnie zgodnie z określonym planem tworzenia kopii zapasowych.
5. Codziennie na dedykowany serwer wykonywane są kopie danych zdeklarowanych przez użytkowników.
6. Kopie te wykonywane są automatycznie.

VII. Przechowywanie elektronicznych nośników informacji zawierających dane osobowe

1. Zbiory danych w formie elektronicznej w dużej mierze przechowywane są na serwerach obsługujących system informatyczny Administratora Danych. Wszelkie dane przetwarzane na stacjach roboczych oraz komputerach przenośnych zgrywane są na wyznaczone miejsce na serwerach.
2. Kopie bezpieczeństwa przechowywane są w zabezpieczonym miejscach, do których jest ograniczony dostęp.
3. Elektroniczne nośniki danych (pamięci flash, nośniki optyczne, itp.), na których znajdują się dane osobowe muszą być przechowywane w miejscach, do których dostęp jest ograniczony.
4. Po wykorzystaniu danych z elektronicznego nośnika informacji, nośnik ten należy zniszczyć lub trwale usunąć z niego dane.
5. Zabrania się wynoszenia z Ośrodka danych zawartych na nośnikach elektronicznych lub papierowych zawierających informacje dotyczące działalności Ośrodka lub dane osobowe bez zgody kierownika właściwego działu lub koordynatora ds. bezpieczeństwa informacji.

6. Zabrania się wnoszenia i używania jakichkolwiek prywatnych lub innych „niesłużbowych" nośników magnetycznych, optycznych oraz pamięci przenośnych bez zgody Administratora SILP.
7. Pracownik jest zobowiązany do odpowiedniego zabezpieczenia danych przechowywanych na powierzonym mu sprzęcie.

VIII. Przekazywanie danych poza teren Ośrodka

1. Dane przekazywane za poza teren Ośrodka za pomocą łączy internetowych lub na nośnikach elektronicznych muszą być odpowiednio zabezpieczone.
2. Przekazywane informacje muszą być zabezpieczone w taki sposób by ich nieuprawnione odczytanie było niemożliwe.
3. Haseł dostępu, czy kluczy aktywacyjnych do danych nie można przekazywać tą samą droga, co danych.

IX. Ochrona przed złośliwym oprogramowaniem

1. Na wszystkich komputerach będących w posiadaniu Ośrodka został zainstalowany program antywirusowy, który chroni je przed zagrożeniami wynikającymi z działania złośliwego kodu.
2. Za instalacje programu odpowiedzialny jest Administrator SILP.
3. Na styku sieci wewnętrznej z siecią publiczną został zlokalizowany firewall.

X. Korzystanie z Internetu

1. Użytkownikom zabrania się dostępu do Internetu za pośrednictwem łączy, które nie są autoryzowane przez osoby upoważnione. Osobą upoważnioną jest w tym wypadku Administrator SILP.
2. Zabrania się korzystania z Internetu w sposób mogący narazić Ośrodek na jakiekolwiek straty finansowe lub inne.
3. Pracownicy, którzy posiadają dostęp do łączy internetowych, zobowiązani są do ich wykorzystywania wyłącznie w celach służbowych z jednoczesnym zachowaniem dobrych obyczajów i poszanowania praw autorskich i ich dzieł udostępnianych przez sieć Internet.
4. Niedozwolone dla pracownika jest:
   1) udostępnianie osobom trzecim nazw kont i haseł,
   2) samodzielna zmiana konfiguracji stacji roboczych związanych ściśle z przyłączem internetowym,
   3) ściąganie i instalowanie oprogramowania z Internetu bez zgody Administratora SILP nawet w przypadkach, gdy ww. oprogramowanie jest darmowe.
5. Nie przestrzeganie zasad określonych w pkt 4 będzie traktowane jak naruszenie obowiązków pracowniczych. O zaistniałym fakcie Administrator SILP powiadamia Administratora Danych.
6. Uzyskiwanie dostępu, przeglądanie lub rozprowadzanie niewłaściwych materiałów (np. rozrywkowych, pornografii) poprzez sieć wewnętrzną Ośrodka lub sieć Internet jest surowo zabronione.
7. Niedopuszczalne jest ujawnianie za pośrednictwem Internetu informacji prawnie chronionych.

XI. Praca na urządzeniach mobilnych

1. O ile to możliwe, przy przetwarzaniu danych osobowych na urządzeniach mobilnych (komputery przenośne, tablety, smartphone) obowiązują procedury określone w niniejszej instrukcji.
2. Użytkownik, któremu zostało powierzone urządzenie mobilne, powinien chronić go przed uszkodzeniem, kradzieżą i dostępem osób postronnych, szczególną ostrożność należy zachować podczas transportu takiego urządzenia. Obowiązuje zakaz przechowywania na

urządzeniach mobilnych całych zbiorów danych lub szerokich z nich wpisów nawet w postaci zaszyfrowanej.

3. Obowiązuje zakaz używania urządzenia mobilnego przez osoby inne niż użytkownicy, którym zostały one powierzony.
4. Przy pracy na urządzeniach mobilnych powinno zwrócić się szczególną uwagę na podłączanie ich do nieznanych sieci bezprzewodowych.
5. Każdy użytkowni urządzenia mobilnego powinien go zabezpieczyć przed możliwością włączenia urządzenia przez osoby nieuprawnione.
6. Pliki zawierające dane osobowe i przechowywane na urządzeniach mobilnych muszą być zaszyfrowane i zabezpieczone hasłem.
7. Szyfrowane mogą być same pliki lub pliki mogą się znajdować na zaszyfrowanej części urządzenia.

XII. Przeglądy i konserwacje systemów informatycznych oraz nośników informacji

1. Osobą odpowiedzialną za prawidłowe działanie systemu informatycznego jest Administrator SILP.
2. Administrator SILP sprawuje nadzór nad stanem technicznym sprzętu i sieci lokalnej, dokonuje przeglądów i konserwacji systemu i urządzeń.
3. Gdy naprawa systemu musi się odbyć w serwisie zewnętrznym lub przez osobę niebędącą upoważnioną do przetwarzania danych osobowych, Administrator SILP zobowiązany jest do odpowiedniego zabezpieczenia danych znajdujących się na dyskach urządzenia.
4. Jeżeli nie jest możliwe odpowiednie zabezpieczenie danych zawartych na dyskach, wszelkie naprawy wykonuje się w obecności Administratora SILP.
5. Konserwacje sprzętu komputerowego wykonywane są na bieżąco. Każda zgłoszona usterka usuwana jest niezwłocznie przez Administratora SILP lub zlecona zostaje naprawa do serwisu zewnętrznego.

XIII. Kontrola nad wprowadzaniem, dalszym przetwarzaniem i udostępnianiem danych osobowych

1. Każde udostępnienie danych osobowych musi zostać odnotowane w ewidencji udostępnień danych osobowych.
2. Jeżeli system informatyczny umożliwia odnotowywanie udostępnień, za ewidencję uznaje się raporty z systemu informatycznego.
3. System informatyczny, na którym przetwarzane są dane osobowe umożliwia odnotowywanie informacji na temat osób które wprowadzają, edytują dane.

XIV. Kontrola przestrzegania zasad

1. Koordynator ds. bezpieczeństwa informacji sprawuje nadzór nad przestrzeganiem Polityki Bezpieczeństwa przetwarzania danych osobowych w Ośrodku.
2. Koordynator ds. bezpieczeństwa informacji może dokonywać okresowych kontroli i oceny funkcjonowania mechanizmów zabezpieczeń oraz przestrzegania zasad i procedur bezpieczeństwa zawartych w niniejszym dokumencie.
3. Okresowe kontrole przestrzegania zasad powinny odbywać się przynajmniej raz na rok.
4. Koordynator ds. bezpieczeństwa informacji zobowiązany jest do sporządzania protokołów z kontroli.
5. Raport z kontroli przekazywany jest do Administratora Danych.
6. Przedmiotem kontroli w szczególności powinny być:
   1) zgodność z wymaganiami prawnymi w zakresie przetwarzania danych osobowych,
   2) funkcjonowanie systemów informatycznych i zabezpieczeń fizycznych,
   3) poprawność funkcjonowania aplikacji przetwarzających dane osobowe,
   4) zgodność liczby użytkowników i ich uprawnień ze stanem oczekiwanym,
   5) zasady i sposoby niszczenia poszczególnych dokumentów i nośników elektronicznych,

6) zasad przestrzegania zabezpieczenia pomieszczeń i systemów informatycznych, podczas nieobecności pracownika,
7) zasady przechowywania dokumentów zawierających dane osobowe.

7. W przypadku wykrycia niesprawności jednostki komputerowej lub jednej z jej części należy przekazać urządzenie do Administratora SILP w celu diagnostyki i usunięcia awarii. Gdy naprawa wymaga działania osoby trzeciej dane przechowywane na dyskach twardych należy w odpowiedni sposób zabezpieczyć poprzez usunięcie danych lub zaszyfrowanie.
8. Kontroli wykorzystania systemu informatycznego dokonuje Administrator SILP.
9. Przynajmniej raz w roku Administrator SILP wykonuje weryfikację zainstalowanego oprogramowania.

XV. Odpowiedzialność użytkownika

1. Zasady i procedury zawarte w niniejszej Instrukcji obowiązują tak samo każdego pracownika w Ośrodku.
2. Instalacje oprogramowania na stanowiskach pracowniczych mogą dokonywane być z nośników znajdujących się w zasobach Ośrodka. Ich instalacja może być dokonywana przez Administratora SILP lub osobę przez niego upoważnioną tylko i wyłącznie po wydaniu zgody na autoryzowaną instalację.
3. Każdy jest indywidualnie odpowiedzialny za powierzony mu sprzęt.
4. Użytkownicy nie mogą sami dokonywać jakiejkolwiek zmiany komponentów sprzętu komputerowego, ani przyłączać własnych komponentów.
5. Wszelkie zapotrzebowanie na dodatkowe komponenty takie jak: RAM, dysk twardy, karta sieciowa, napęd optyczny i inne muszą być zgłaszane do Administratora SILP, który osobiście dokonuje zmian.
6. Sprzęt komputerowy nie może być wynoszony z Ośrodka lub przenoszony w inne miejsce w Ośrodku bez wcześniejszej zgody Administratora Danych.
7. Utrata lub kradzież sprzętu powinna być niezwłocznie zgłaszana bezpośredniemu przełożonemu i który zawiadamia Administratora Danych.
8. Każdy pracownik jest indywidualnie odpowiedzialny za przechowywanie przez siebie informacje w formie tradycyjnej (papierowej) jak i w formie elektronicznej.
9. Za umożliwienie korzystania z komputera przez osobę nieupoważnioną odpowiada pracownik, któremu sprzęt ten został przydzielony.
10. Na każdym użytkowniku systemu informatycznego spoczywa odpowiedzialność za rodzaj i zakres danych przetwarzanych przez niego w ramach przydzielonych mu uprawnień systemowych i programowych, oraz odpowiedzialność za ochronę tych danych przed niepowołanym dostępem, niepowołaną modyfikacją, zniszczeniem, nielegalnym ujawnieniem lub pozyskaniem, w stopniu odpowiednim do zadań tej osoby przy przetwarzaniu danych osobowych.

DYREKTOR ZAKŁADU

inż. Ryszard Mielek

Załącznik nr 4
do Zarządzenia Nr 24
Dyrektora Ośrodka Techniki Leśnej w Jarocinie
z dnia 21 grudnia 2015 roku

INSTRUKCJA POSTĘPOWANIA W SYTUACJI NARUSZENIA BEZPIECEZŃSTWA INFORMACJI

§ 1

Instrukcja postępowania w sytuacji naruszenia bezpieczeństwa informacji obowiązuje każdego pracownika Ośrodka Techniki Leśnej w Jarocinie.

§ 2

Zagrożenie to potencjalna przyczyna niepożądanego incydentu, którego skutkiem może być szkoda dla Ośrodka. Każda sytuacja, która powoduje niedostępność danych (czasowe lub trwałe uniemożliwienie przetwarzania zbiorów danych), ich niekontrolowany wypływ, ujawnienie czy utratę lub przekłamanie – jest zagrożeniem systemu, niezależnie od tego czy jest to celowy sabotaż, czy przypadkowe zdarzenie.

§ 3

Za naruszenie bezpieczeństwa uważa się również stwierdzone nieprawidłowości w zakresie bezpieczeństwa miejsc przechowywania danych osobowych (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych tj. na papierze (wydrukach), kliszach, folii, zdjęciach, dyskietkach, pamięciach flash itp. w formie niezabezpieczonej.

§ 4

Dane osobowe oraz informacje zostają ujawnione, gdy stają się znane w całości lub części pozwalającej na określenie osobom nieuprawnionym tożsamości osoby, której dane dotyczą.

§ 5

W przypadku stwierdzenia naruszenia:

1) zabezpieczenia systemu informatycznego,
2) technicznego stanu urządzeń,
3) zawartości zbioru danych osobowych,
4) ujawnienia metody pracy lub sposobu działania programu,
5) jakości transmisji danych w sieci telekomunikacyjnej mogącej wskazywać na naruszenie zabezpieczeń tych danych,
6) innych zdarzeń mogących mieć wpływ na naruszenie danych osobowych,

każda osoba zatrudniona przy przetwarzaniu danych osobowych oraz informacji jest zobowiązana niezwłocznie powiadomić o tym fakcie bezpośredniego przełożonego i koordynatora ds. bezpieczeństwa informacji.

§ 6

Do czasu przybycia na miejsce naruszenia bezpieczeństwa informacji koordynatora ds. bezpieczeństwa informacji lub innej upoważnionej przez Administratora Danych osoby, należy:

1) niezwłocznie podjąć czynności niezbędne do powstrzymania niepożądanych skutków zaistniałego naruszenia, o ile istnieje taka możliwość, a następnie uwzględnić w działaniu również ustalenie przyczyn i sprawców,
2) rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia,
3) zaniechać - o ile to możliwe - dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę,

4) podjąć inne działania przewidziane i określone w instrukcjach technicznych i technologicznych stosownie do objawów i komunikatów towarzyszących naruszeniu,
5) podjąć stosowne działania, jeśli zaistniały przypadek jest określony w dokumentacji systemu operacyjnego, dokumentacji bazy danych lub aplikacji użytkowej,
6) zastosować się do innych instrukcji i regulaminów, jeśli odnoszą się one do zaistniałego przypadku,
7) udokumentować wstępnie zaistniałe naruszenie,
8) nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia koordynatora ds. bezpieczeństwa informacji lub osoby upoważnionej.

§ 7

Po przybyciu na miejsce naruszenia lub ujawnienia bezpieczeństwa informacji koordynatora ds. bezpieczeństwa informacji lub osoba upoważniona:
1) rozpoznaje zaistniałą sytuację i dokonuje wyboru metody dalszego postępowania mając na uwadze ewentualne zagrożenia dla prawidłowości pracy Ośrodka,
2) może żądać dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem,

§ 8

Po przywróceniu prawidłowego stanu należy przeprowadzić szczegółową analizę w celu określenia przyczyny naruszenia bezpieczeństwa informacji oraz przedsięwziąć kroki mające na celu wyeliminowanie podobnych zdarzeń w przyszłości.

§ 9

Koordynator ds. bezpieczeństwa informacji dokumentuje zaistniały przypadek naruszenia oraz sporządza raport, określony w załączniku nr 1 do niniejszego dokumentu.

§ 10

Raport, o którym mowa w § 9, koordynator ds. bezpieczeństwa informacji niezwłocznie przekazuje Administratorowi Danych, a w przypadku nieobecności Administratora Danych osobie uprawnionej.

§ 11

1. Zaistniałe naruszenie może stać się przedmiotem szczegółowej, zespołowej analizy prowadzonej przez Kierownictwo Ośrodka, koordynatora ds. bezpieczeństwa informacji oraz osoby zainteresowane.
2. Analiza, o której mowa w ust. 1, powinna zawierać wszechstronną ocenę zaistniałego naruszenia, wskazanie odpowiedzialnych, wnioski, co do ewentualnych przedsięwzięć proceduralnych, organizacyjnych, kadrowych i technicznych, które powinny zapobiec podobnym naruszeniom w przyszłości.

DYREKTOR ZAKŁADU

inż. Ryszard Misiek

Załącznik nr 1

do Instrukcji postępowania w sytuacji

naruszenia bezpieczeństwa informacji

Raport nr ...../.....

z naruszenia bezpieczeństwa informacji w Ośrodka Techniki Leśnej w Jarocinie

1. Data:..... Godzina:.....

(dd.mm.rrrr) (00:00)

2. Osoba powiadamiająca o zaistniałym zdarzeniu:

.....

(Imię i Nazwisko, stanowisko służbowe, nazwa użytkownika jeśli występuje)

3. Lokalizacja zdarzenia:

.....

(np. nr pokoju; nazwa pomieszczenia)

4. Rodzaj naruszenia bezpieczeństwa, oraz okoliczności towarzyszące:

.....

.....

5. Podjęte działania:

.....

.....

6. Przyczyny wystąpienia zdarzenia:

.....

.....

7. Postępowanie wyjaśniające:

.....

.....

.....

data, podpis koordynatora ds. bezpieczeństwa informacji lub

osoby upoważnionej