

ZARZĄDZENIE NR 28

Nadleśniczego Nadleśnictwa Rozwadów

z dnia 22.06.2026

w sprawie wprowadzenia Regulaminu Organizacyjnego

Nadleśnictwa Rozwadów

zn. spr.: NK.012.4.2026

Na podstawie art. 35 ustawy z dnia 28.09.1991 r o lasach (Dz. U. z 2025 r., poz. 567), § 22 pkt 3 Statutu Państwowego Gospodarstwa Leśnego Lasy Państwowe (załącznik do zarządzenia nr 50 Ministra Ochrony Środowiska, Zasobów Naturalnych i Leśnictwa z dnia 18.05.1994 r.), Zarządzenia nr 90 Dyrektora Generalnego Lasów Państwowych z dnia 12 grudnia 2012 r. z późniejszymi zmianami w sprawie ustalenia ramowego regulaminu organizacyjnego nadleśnictwa zarządzam, co następuje:

§ 1

Z dniem 22.06.2026 r. wprowadzam do stosowania Regulamin Organizacyjny Nadleśnictwa Rozwadów określający zakres i tryb pracy komórek organizacyjnych nadleśnictwa, stanowiący załącznik do niniejszego zarządzenia.

§ 2

Każdy pracownik zobowiązany jest zapoznać się z Regulaminem Organizacyjnym. Oświadczenie pracownika o zapoznaniu się z treścią regulaminu, zaopatrzone w podpis pracownika i datę, dołącza się do jego akt osobowych.

§ 3

Z dniem podpisania niniejszego zarządzenia traci moc zarządzenie nr 16 Nadleśniczego Nadleśnictwa Rozwadów z dnia 20.03.2026 r. w sprawie wprowadzenia Regulaminu Organizacyjnego Nadleśnictwa Rozwadów.

§ 4

Zarządzenie wchodzi w życie z dniem podpisania.



NADLEŚNICZY
Nadleśnictwa Rozwadów
mgr inż. Wojciech Chęłpa

Załącznik nr 1 do Zarządzenia nr...²⁸
Nadleśniczego Nadleśnictwa Rozwadów
z dnia 22.06.2026

**REGULAMIN ORGANIZACYJNY
NADLEŚNICTWA ROZWADÓW**



Rozdział I

Postanowienia ogólne

§ 1

Regulamin Organizacyjny Nadleśnictwa Rozwadów, zwany dalej Regulaminem, ustala organizację wewnętrzną, szczegółowy zakres zadań komórek organizacyjnych oraz tryb i zasady pracy nadleśnictwa.

§ 2

Ilekcroć w regulaminie jest mowa o:

1. **Lasach Państwowych (PGL LP)** – należy przez to rozumieć Skarb Państwa Państwowe Gospodarstwo Leśne Lasy Państwowe,
2. **Statucie** - należy rozumieć Statut Państwowego Gospodarstwa Leśnego Lasy Państwowe,
3. **Regionalnej Dyrekcji lub RDLP** – należy przez to rozumieć Regionalną Dyrekcję Lasów Państwowych w Lublinie,
4. **Nadleśniczym** – należy przez to rozumieć Nadleśniczego Nadleśnictwa Rozwadów
5. **Komórcie organizacyjnej** – należy przez to rozumieć: dział, leśnictwo lub samodzielne stanowisko wyodrębnione w strukturze organizacyjnej Nadleśnictwa Rozwadów,
6. **SILP** – należy przez to rozumieć System Informatyczny Lasów Państwowych,
7. **BIP** – należy przez to rozumieć Biuletyn Informacji Publicznej.
8. **Regulaminie** – należy przez to rozumieć Regulamin organizacyjny Nadleśnictwa Rozwadów;
9. **Oświadczeniu woli** w nadleśnictwie, należy przez to rozumieć każde zachowanie wyrażone przez nadleśniczego - bądź inne osoby działające z upoważnienia i w imieniu nadleśniczego – w ramach czynności prawnych w Nadleśnictwie Rozwadów, które w sposób ostateczny i zgodny z prawem ujawnia zamiar nadleśniczego.
10. **Systemie EZD lub EZD** - należy przez to rozumieć System Elektronicznego Zarządzania Dokumentacją.
11. **Przekazywaniu, akceptowaniu, podpisywaniu, udostępnianiu pism i dokumentów** - należy przez to rozumieć również wykonywanie odpowiednich czynności w systemie elektronicznego zarządzania dokumentacją (EZD).

§ 3

Nadleśnictwo Rozwadów działa na podstawie Ustawy z dnia 28 września 1991 r. o lasach, aktów wykonawczych do tej ustawy, a w szczególności statutu Państwowego Gospodarstwa Leśnego Lasy Państwowe, stanowiącego załącznik do zarządzenia nr 50 Ministra Ochrony Środowiska, Zasobów Naturalnych i Leśnictwa z dnia 18 maja 1994 r. w sprawie nadania statutu Państwowemu Gospodarstwu Leśnemu Lasy Państwowe, rozporządzenia Rady Ministrów z dn. 6.12.1994 r. w sprawie szczegółowych zasad prowadzenia gospodarki finansowej w Państwowym Gospodarstwie Leśnym Lasy Państwowe, a także na podstawie niniejszego regulaminu.

§ 4

Nadleśnictwo jest podstawową, samodzielną jednostką organizacyjną Lasów Państwowych, powołaną do prowadzenia samodzielnej gospodarki leśnej, reprezentującą Skarb Państwa w zakresie zarządzanego mienia. Jest jednostką organizacyjną nadzorowaną przez Dyrektora Regionalnej Dyrekcji Lasów Państwowych w Lublinie. Siedzibą biura Nadleśnictwa Rozwadów jest budynek przy ul. Przemysłowa 1 w Stalowej Woli.

Rozdział II Organizacja wewnętrzna

§ 5

Ogólne zadania i kompetencje nadleśniczego:

1. Kompetencje nadleśniczego wynikają z art. 35 ustawy o lasach oraz § 22, 23 i 24 Statutu PGL LP.
2. Nadleśniczy (**N**) kieruje całokształtem działalności nadleśnictwa na zasadzie jednoosobowego kierownictwa i ponosi za nią pełną odpowiedzialność, a także reprezentuje nadleśnictwo na zewnątrz.
3. Nadleśniczy wydaje zarządzenia i decyzje obowiązujące na obszarze nadleśnictwa, w szczególności ustala, wdraża i aktualizuje Regulamin organizacyjny, Regulamin kontroli wewnętrznej i Regulamin pracy.
4. Nadleśniczy może upoważnić osoby do reprezentowania i podejmowania w jego imieniu decyzji w określonych przez niego sprawach.
5. W razie nieobecności nadleśniczego pracą nadleśnictwa kieruje zastępca nadleśniczego, wg. kolejności zastępca nadleśniczego ds. marketingu i użytkowania lasu (**Z1**), a następnie zastępca nadleśniczego ds. zagospodarowania lasu (**Z2**), natomiast w przypadku nieobecności zastępców nadleśniczego główny księgowy (**K**) lub wyznaczony przez nadleśniczego inny pracownik.
6. Nadleśniczy odpowiada za organizację ochrony mienia i zwalczania szkodnictwa leśnego zgodnie z § 10 Instrukcji ochrony lasów przed szkodnictwem leśnym, stanowiącej załącznik do zarządzenia nr 46 Dyrektora Generalnego Lasów Państwowych z dnia 06 czerwca 2015 roku, znak: GS-021.2.2015.
7. Nadleśniczy realizuje zadania obronne na podstawie ustawy o powszechnym obowiązku obrony RP oraz innych przepisów i instrukcji związanych z przygotowaniem nadleśnictwa do działania w warunkach zewnętrznego zagrożenia bezpieczeństwa państwa i w czasie wojny (militaryzacja).
8. Nadleśniczy zatrudnia i zwalnia pracowników nadleśnictwa.
9. Nadleśniczego powołuje i odwołuje Dyrektor Regionalnej Dyrekcji Lasów Państwowych w Lublinie.

§ 6

Strukturę nadleśnictwa stanowią:

1. **biuro nadleśnictwa**,
2. **leśnictwa**, w tym leśnictwo Szkółki.

1. W skład biura nadleśnictwa wchodzi następujące komórki organizacyjne:

1) działy:

- Dział Gospodarki Leśnej (**ZG**) – w tym (**ZG1**) kierowany przez zastępcę nadleśniczego ds. marketingu i użytkowania lasu (**Z1**) oraz (**ZG2**) kierowany przez zastępcę nadleśniczego ds. zagospodarowania lasu (**Z2**),
- Dział Finansowo -Księgowy (**KF**) - kierowany przez głównego księgowego -**K**
- Dział Administracyjno – Gospodarczy (**SA**) - kierowany przez sekretarza - **S**
- Posterunek Straży Leśnej (**NS**) - kierowany przez Starszego Strażnika Leśnego pełniącego funkcje Komendanta Posterunku Straży Leśnej

2) Samodzielne stanowiska pracy:

- inżynierowie nadzoru (**NN1, NN2**)
- specjalista ds. pracowniczych (**NK**)

2. W skład nadleśnictwa wchodzi 10 - leśnictw rewirowych i leśnictwo Szkółki, w dwóch obrębach leśnych (wykaz leśnictw w zał. nr 2):

- 1) **obręb Rozwadów** – Leśnictwo (**ZL**): Burdze, Ciemny Kąt, Charzewice, Moskale, Zaosie, Zapolednik, Żupawa, Leśnictwo (**ZS**): Szkółki,
- 2) **obręb Pysznica** - Leśnictwo (**ZL**): Huta Deręgowska, Katy, Pysznica,

3. Nadleśnictwo zatrudnia również stażystów wg zasad obowiązujących w PGL LP.

4. Schemat struktury organizacyjnej Nadleśnictwa Rozwadów przedstawia Załącznik nr 1 do Regulaminu.

§ 7

1. Nadleśniczemu podlegają bezpośrednio:

a) zastępcy nadleśniczego (**Z1**), (**Z2**),

b) główny księgowy (**K**),

c) inżynierowie nadzoru (**NN1, NN2**),

d) sekretarz (**S**) (z zakresem administratora pomocniczego SILP)

e) specjalista ds. pracowniczych (**NK**)

f) komendant posterunku Straży Leśnej (**NS**), (w zakresie stanowisko ds. obronnych),

2. Pozostali pracownicy zatrudnieni w biurze nadleśnictwa, w poszczególnych działach podlegają bezpośrednio osobom kierującym tymi działami.

3. Zastępcy nadleśniczego ds. marketingu i użytkowania lasu (**Z1**) podlegają stanowiska działu gospodarki leśnej (**ZG1**) zajmujący się zadaniami: marketingu, obrotu drewnem, sprzedaży drewna i użytkowania lasu, stanu posiadania i urządzania.

4. Zastępcy nadleśniczego ds. zagospodarowania lasu (**Z2**) podlegają stanowiska działu gospodarki leśnej (**ZG2**) zajmujący się zadaniami: hodowli i ochrony lasu, ochrony przyrody, edukacji leśnej, ochrony p.poż i łowiectwa, szkółkarstwa i nasiennictwa.

5. Leśniczowie (**ZL**), oraz leśniczy Szkółkarz (**ZS**) podlegają bezpośrednio zastępcy nadleśniczego ds. marketingu i użytkowania lasu (**Z1**).

6. Podleśniczowie (**ZP**) przydzieleni do pracy w danym leśnictwie podlegają bezpośrednio lokalnemu leśniczemu.

7. Stażysta podlega bezpośrednio zastępcy nadleśniczego ds. marketingu i

- użytkowania lasu (**Z1**), który pełni rolę opiekuna stażysty i jest odpowiedzialny za przebieg i realizację stażu.
8. Inni pracownicy (np. instruktorzy techniczni) jeżeli zostaną przydzieleni do pracy w danym leśnictwie podlegają lokalnemu leśniczemu, natomiast jeśli zostaną przydzieleni do pracy w biurze to podlegają kierownikowi przydzielonego działu.
 9. W nadleśnictwie nie wyodrębnia się stanowiska ds. BHP. Zadania BHP zostały powierzone specjalście SL ds. hodowli lasu. Szczegółowy zakres zadań określa zakres czynności pracownika, któremu powierzono zadania BHP

Rozdział III

Zakres zadań dla stanowisk podlegających bezpośrednio nadleśniczemu i podległych im komórek organizacyjnych

§ 8

1. **Zastępca nadleśniczego ds. marketingu i użytkowania lasu (Z1)** odpowiada za całokształt sfery produkcyjnej w nadleśnictwie, kieruje Działem Gospodarki Leśnej (**ZG1**), pracą leśniczych w zakresie powierzonych kompetencji, prowadzi działalność marketingową, a w szczególności:
 - a) nadzoruje i prowadzi sprawy związane z pozyskaniem i sprzedażą drewna,
 - b) nadzoruje sprawy dotyczące stanu posiadania, ewidencji lasów i gruntów oraz ich udostępniania,
 - c) współuczestniczy w opracowaniu planu finansowo-gospodarczego nadleśnictwa,
 - d) nadzoruje prace związane z leśną mapą numeryczną (LMN),
 - e) organizuje i prowadzi szkolenia w zakresie spraw mu powierzonych,
 - f) uczestniczy w opracowaniu planu urządzania lasu dla Nadleśnictwa Rozwadów (opiniowanie, wprowadzanie niezbędnych korekt, udział w komisjach, uzgodnienie z wykonawcą ostatecznych zapisów itp.).

W przypadku nieobecności Zastępcy Nadleśniczego ds. zagospodarowania lasu (**Z2**) przejmuje w całości jego zakres zadań i obowiązków.

W zakresie ochrony mienia oraz zwalczania szkodnictwa leśnego zastępca nadleśniczego przysługują uprawnienia strażnika leśnego.

Zadania zastępcy nadleśniczego w w/w zakresie określa zarządzenie nr 46 DGLP z dnia 06.06.2015 r. – dotyczy to przede wszystkim przeciwdziałania kradzieżom drewna, sadzonek, zaśmiecania lasu oraz niszczenia roślinności leśnej.

2. **Zastępca nadleśniczego ds. zagospodarowania lasu (Z2)**, kieruje Działem Gospodarki Leśnej (**ZG2**), w zakresie powierzonych kompetencji, a w szczególności :
 - a) prowadzi sprawy związane z hodowlą lasu w tym: nasiennictwem, selekcją, szkółkarstwem
 - b) ochroną lasu, ochroną przeciwpożarową, edukacją leśną
 - c) nadzoruje i prowadzi sprawy związane z ochroną przyrody,
 - d) prowadzi sprawy związane z certyfikacją gospodarki leśnej
 - e) nadzoruje i prowadzi sprawy związane z gospodarką łowiecką,
 - f) współuczestniczy w opracowaniu planu finansowo-gospodarczego nadleśnictwa,
 - g) organizuje i prowadzi szkolenia w zakresie spraw mu powierzonych,
 - h) uczestniczy w opracowaniu planu urządzania lasu dla Nadleśnictwa Rozwadów (opiniowanie, wprowadzanie niezbędnych korekt, udział w komisjach, uzgodnienie z wykonawcą ostatecznych zapisów itp.)

W przypadku nieobecności Zastępcy Nadleśniczego ds. marketingu i użytkowania lasu (**Z1**) przejmuje w całości jego zakres zadań i obowiązków. W zakresie ochrony mienia oraz zwalczania szkodnictwa leśnego zastępcy nadleśniczego przysługują uprawnienia strażnika leśnego.

Zadania zastępcy nadleśniczego w w/w zakresie określa zarządzenie nr 46 DGLP z dnia 06.06.2015 r. – dotyczy to przede wszystkim przeciwdziałania kradzieżom drewna, sadzonek, zaśmiecania lasu oraz niszczenia roślinności leśnej.

Dział Gospodarki Leśnej (ZG1, ZG2)

1. Do zadań Działu Gospodarki Leśnej (**ZG1, ZG2**) – kierowanego przez zastępców nadleśniczego (**Z1, Z2**) w szczególności należy: realizacja zadań z zakresu nasiennictwa, selekcji, szkółkarstwa, hodowli lasu, ochrony lasu, w tym ochrony przeciwpożarowej, ochrony przyrody, łowiectwa, zagospodarowania, użytkowania i urządzania lasu oraz edukacji leśnej i kontaktów z mediami.
2. Dział prowadzi sprawy związane ze stanem posiadania i ewidencją gruntów oraz udostępnianiem lasu.
3. Obsługuje internetowy Portal Leśno-Drzewny i aplikację e-drewno.
4. Nadzoruje zagadnienia związane z utrzymaniem spójności, funkcjonalności i bezpieczeństwem SILP, urzędzeń SILP, rejestratorów, z obsługą systemu informatycznego nadleśnictwa i urzędzeń peryferyjnych oraz internetowych portali (administrator główny).
5. W zakresie ochrony mienia i zwalczania szkodnictwa leśnego: prowadzenie w ramach działalności prewencyjnej edukacji społeczeństwa, zwłaszcza przeciwdziałanie zaśmiecaniu lasu, niszczeniu obiektów turystycznych oraz roślinności leśnej.
6. Prowadzi sprawy związane z przygotowaniem materiałów do przetargu na wykonanie prac leśnych, wykonania planu urzędzenia lasu (w tym dane do referatu nadleśniczego n/t gospodarki leśnej w minionym 10-leciu).
7. Zakres obowiązków i odpowiedzialności zastępców nadleśniczego i stanowisk w Dziale Gospodarki Leśnej oraz leśniczych i podleśniczych określają szczegółowe zakresy czynności.
8. Realizuje Politykę Komunikacyjną PGL LP.
9. Administrowanie i prowadzenie nadzoru nad systemem elektronicznego zarządzania dokumentacją (EZD).
10. Przyjmowanie zgłoszeń strony społecznej ws. lasów cennych przyrodniczo i ważnych społecznie.

Leśnictwo (ZL) kierowane jest przez leśniczego.

1. Do zadań leśniczego należy całokształt spraw związanych z prowadzeniem gospodarki leśnej na terenie swego leśnictwa, za którą ponosi pełną odpowiedzialność. Wykonuje również zadania związane z ochroną przed szkodnictwem leśnym i jego zwalczaniem, zgodnie z zarządzeniem nr 46 DGLP z dnia 06.06.2015 r., korzystając z uprawnień strażnika leśnego określonych w ustawie o lasach.
2. Leśniczy oraz podleśniczy odpowiadają materialnie za powierzone mienie.
3. Leśniczy wykonuje swoje zadania przy pomocy podleśniczego oraz innych pracowników przydzielonych do pracy w leśnictwie np. instruktora technicznego, stażysty.
4. Leśniczy czynnie uczestniczy w procesie tworzenia planu urzędzenia lasu dla Nadleśnictwa Rozwadów, zwłaszcza w opiniowaniu i uzgodnieniu z wykonawcą zapisów z prac terenowych oraz wprowadzeniu niezbędnych korekt.

5. W czasie nieobecności leśniczego zastępuje go podleśniczy lub osoba wyznaczona przez nadleśniczego. Przekazanie leśnictwa na czas nieobecności leśniczego powinno odbywać się na podstawie łącznego powierzenia mienia, uregulowanego umową o współodpowiedzialności, zawartą na piśmie przez pracodawcę, leśniczego i podleśniczego, określającą zakres odpowiedzialności poszczególnych pracowników. Zasady określające zastępstwa w leśnictwach Nadleśnictwa Rozwadów reguluje odrębne zarządzenie wydane przez Nadleśniczego Nadleśnictwa Rozwadów.
6. Podleśniczy oraz inni pracownicy (np. instruktorzy techniczni), przydzieleni do leśnictwa, podlegają bezpośrednio leśniczemu.
7. Leśniczy współpracuje z firmami usługowymi (ZUL) w zakresie realizacji i wykonania powierzonych zadań gospodarczych.
8. Leśniczy realizuje zadania operacyjne (obronne) nałożone na nadleśnictwo.
9. Szczegółowy zakres obowiązków i odpowiedzialności służbowej leśniczego oraz podległych jemu pracowników, określają stosowne zakresy czynności.

Leśnictwo Szkółki (ZS) – leśniczy szkółkarz.

1. Na terenie powierzonej mu jednostki, wykonuje czynności techniczno-produkcyjne, administracyjne oraz ponosi odpowiedzialność za właściwe wykonanie przydzielonych mu zadań i ochronę powierzonego majątku.
2. Leśniczy szkółkarz organizuje całokształt prac szkółkarskich w tym szczególnie pełną produkcję niezbędnego materiału sadzeniowego podstawowych gatunków lasotwórczych.
3. Organizuje, zleca i koordynuje zbiór nasion i szyszek z bazy nasiennej Nadleśnictwa Rozwadów.
4. Odpowiada za przechowywanie nasion i sadzonek z zachowaniem zasady rotacji.
5. Prowadzi dokumentację dotyczącą szkółkarstwa i nasiennictwa zgodnie z obowiązującymi w tym zakresie przepisami.
6. Prowadzi niezbędną dokumentację obrotu nasion i sadzonek.
7. W czasie nieobecności leśniczego szkółkarza zastępuje go Leśniczy L-ctwa Zaosie lub osoba wyznaczona przez nadleśniczego.
8. Szczegółowy zakres obowiązków i odpowiedzialności określa zakres czynności.

Podleśniczy (ZP)

1. Podleśniczy przydzielony do leśnictwa podlega bezpośrednio leśniczemu. Wykonuje czynności techniczno – produkcyjne, administracyjne i ochronne mające na celu realizację zadań ustalonych dla leśnictwa. Zastępuje leśniczego w czasie nieobecności.
2. Podleśniczy odpowiada za wykonywanie przez siebie zadań w zakresie zwalczania szkodnictwa leśnego, które określają odpowiednie zapisy w ustawie o lasach i aktualnie obowiązującej instrukcji ochrony lasu przed szkodnictwem.
3. Szczegółowy zakres obowiązków i odpowiedzialności służbowej podleśniczego określa jego zakres czynności.

§ 9

1. **Główny księgowy (K)** wykonuje zadania i ponosi odpowiedzialność za całość spraw dotyczącą gospodarki finansowo-księgowej nadleśnictwa w zakresie: księgowości, finansów, planowania finansowo-gospodarczego, analiz, sprawozdawczości oraz organizuje i sprawuje kontrolę wewnętrzną dokumentów

- finansowo księgowych, a także opracowuje regulamin kontroli wewnętrznej i obiegu dokumentów w nadleśnictwie.
2. W szczególności do obowiązków głównego księgowego należy terminowe egzekwowanie należności i regulowanie zobowiązań.
 3. Główny księgowy jest odpowiedzialny za opracowanie, wdrożenie i aktualizację schematu obiegu dokumentów oraz opracowanie i aktualizację regulaminu przeprowadzania inwentaryzacji rocznej.
 4. Czynności nadzorczo - kontrolne wykonuje zgodnie z ustawą z dnia 29 września 1994 r. o rachunkowości - dokonuje kontroli wewnętrznej operacji gospodarczych nadleśnictwa stanowiących przedmiot księgowania.
 5. Pisma i inne dokumenty dotyczące spraw działu finansowo-księgowego są parafowane przez głównego księgowego lub osoby zastępujące go i podpisywane przez nadleśniczego lub zastępcę nadleśniczego.
 6. Dokumenty i pisma przedkładane głównemu księgowemu do kontroli powinny być parafowane przez kierownika komórki organizacyjnej, gdzie sprawa jest załatwiana.
 7. Współuczestniczy w opracowaniu planu finansowo-gospodarczego Nadleśnictwa Rozwadów.
 8. W realizacji wyznaczonego zakresu obowiązków główny księgowy ma prawo żądać od innych służb i komórek organizacyjnych nadleśnictwa:
 - udzielenia w formie ustnej lub pisemnej niezbędnych informacji i wyjaśnień,
 - udostępnienia do wglądu dokumentów i wyliczeń będących dodatkowym źródłem informacji,
 - usunięcia w wyznaczonym terminie nieprawidłowości dotyczących:
 - przyjmowania, wystawiania, obiegu i kontroli dokumentów,
 - systemu kontroli wewnętrznej,
 - systemu wewnętrznej informacji ekonomicznej.
 9. Główny księgowy oraz dział finansowo-księgowy w zakresie zwalczania szkodnictwa leśnego i ochrony mienia:
 - prowadzi we współpracy z radcą prawnym windykację należności zasądzonych prawomocnymi wyrokami sądów.

Dział Finansowo – Księgowy (KF) kierowany przez głównego księgowego.

Do zadań działu w szczególności należy:

1. Prowadzenie ewidencji i formalno-rachunkowej kontroli dokumentów, sporządzanie planów finansowych, analiz i sprawozdawczości, rozliczanie działalności gospodarczej i administracyjnej oraz terminowe egzekwowanie wszelkich należności i regulowanie zobowiązań.
2. Sporządzanie list płac, rozliczanie składek na ubezpieczenia społeczne i podatek dochodowy od osób fizycznych oraz przygotowywanie stosownych deklaracji dla Urzędów Skarbowych i ZUS.
3. Zakres obowiązków i odpowiedzialności głównego księgowego i stanowisk w Dziale Finansowo-Księgowym określają szczegółowe zakresy czynności.

§ 10

Sekretarz (S)- kieruje Działem Administracyjno-Gospodarczym i jest odpowiedzialny za całokształt spraw związanych z pełną obsługą administracyjną nadleśnictwa, w szczególności:

1. Odpowiada za procedury zamówień zgodnie z art. 52 ust. 2 ustawy z dnia 11

września 2019 roku Prawo zamówień publicznych (tekst jedn. Dz. U. z 2024 r. poz. 1320 z późn. zm.) oraz gromadzenie wszelkiej dokumentacji w tej sprawie.

2. Nadzoruje pracę sekretariatu i prowadzenie archiwum zakładowego.
3. Realizuje zadania operacyjne (obronne) nałożone na nadleśnictwo.
4. Sekretarz swoje obowiązki wykonuje przy pomocy podległych sobie pracowników
5. Sekretarz oraz pracownicy działu administracyjno-gospodarczego w zakresie ochrony mienia i zwalczania szkodnictwa leśnego, w szczególności odpowiadają za zabezpieczenie obiektów budynkowych nadleśnictwa, zwłaszcza przed kradzieżami i dewastacją.

Dział Administracyjno–Gospodarczy (SA) - kierowany przez sekretarza. Do zadań Działu w szczególności należy realizacja zadań wynikających z całokształtu zagadnień obejmujących pełną obsługę administracyjną nadleśnictwa:

1. Prowadzenie spraw związanych z sekretariatem nadleśnictwa.
2. Prowadzenie magazynu głównego nadleśnictwa.
3. Koordynacja spraw dotyczących instrukcji kancelaryjnej i archiwalnej.
4. Zaopatrzenie, zakupy.
5. Remonty oraz budowa środków trwałych infrastruktury nadleśnictwa.
6. Transport i jego ewidencja.
7. Umowy dzierżaw i najmu mieszkań, budynków i budowli.
8. Podatek od nieruchomości.
9. Organizacja i realizacja zamówień publicznych.
10. Prowadzenie archiwum zakładowego.
11. Prowadzenie spraw związanych z inwentaryzacją składników majątkowych nadleśnictwa.
12. Administrowanie i prowadzenie nadzoru nad systemem elektronicznego zarządzania dokumentacją (EZD)
13. Prowadzenie nadzoru technicznego nad systemem elektronicznego zarządzania dokumentacją (EZD).

Zakres obowiązków i odpowiedzialności sekretarza i stanowisk w Dziale Administracyjno-Gospodarczym określają szczegółowe zakresy czynności.

§ 11

Specjalista ds. pracowniczych (NK) - prowadzi całokształt spraw pracowniczych w rozumieniu Kodeksu pracy, PUZP dla pracowników PGL LP oraz innych unormowań prawnych obowiązujących w tym zakresie, w szczególności:

1. Prowadzenie dokumentacji w sprawach związanych ze stosunkiem pracy, przechowywanie i aktualizowanie akt osobowych pracowników oraz ochrona danych w nich zawartych.
2. Kontrola merytoryczna dokumentacji płacowej nadleśnictwa.
3. Rejestrowanie i wyrejestrowanie pracowników i członków rodzin z ubezpieczenia w ZUS.
4. Przygotowanie i przechowywanie w aktach osobowych dokumentacji płacowych pracowników.
5. Powadzenie spraw związanych z ubezpieczeniami, szkoleniami i podnoszeniem kwalifikacji zawodowych pracowników.
6. Opracowywanie, wdrażanie i aktualizacja regulaminów: organizacyjnego, pracy, Zakładowego Funduszu Świadczeń Socjalnych oraz ścisła realizacja wytycznych

nadleśniczego w zakresie polityki kadrowej.

7. Prowadzenie całokształtu spraw pracowniczych i socjalnych.

Zakres obowiązków i odpowiedzialności specjalisty ds. pracowniczych określa szczegółowy zakres czynności.

§ 12

Komendant Posterunku Straży Leśnej (NS)

1. Na bieżąco kieruje posterunkiem Straży Leśnej, opracowuje okresowe (tygodniowe) plany pracy strażników leśnych, sprawozdania z prowadzonych działań. Komendant Posterunku Straży Leśnej, przy wykonywaniu zadań i czynności, korzysta z uprawnień, o których mowa w art. 45 – 47 ustawy o lasach oraz zgodnie z zarządzeniem nr 52 DGLP z dnia 09.09.2004 r.
2. Według w/w zarządzenia prowadzi ewidencję szkodnictwa leśnego Nadleśnictwa Rozwadów oraz sprawy związane z rejestracją przestępstw i ich sprawców w Krajowym Centrum Informacji Kryminalnej „KCIK.”
3. Zamawia i rozlicza bloczki mandatowe zgodnie z obowiązującym prawem.
4. Prowadzi magazyn broni służbowej.
5. Prowadzi sprawy niejawne.
6. Komendant Straży Leśnej prowadzi w nadleśnictwie sprawy niejawne, w tym oddział kancelarii niejawnej oraz sprawy z zakresu obronności. Podlega w ww. zakresie bezpośrednio Nadleśniczemu. Koordynuje i realizuje zadania operacyjne (obronne) nałożone na nadleśnictwo, ustalone w opracowanych planach obronnych. Organizuje i prowadzi szkolenia z zakresu obronności. Wdraża postanowienia wynikające z aktów prawnych, podwyższenia gotowości obronnej państwa i nadleśnictwa w ramach systemu stałych dyżurów, w tym organizuje stały dyżur w nadleśnictwie. Ponadto komendant sprawuje nadzór nad przestrzeganiem przez pracowników nadleśnictwa tajemnicy służbowej. Szczegółowy zakres i obowiązki w zakresie prowadzenia spraw związanych z obronnością kraju i kancelarią niejawną, zawarty jest w odrębnych instrukcjach, zarządzeniach, rozporządzeniach i wytycznych.

Posterunek Straży Leśnej (NS)

Obszarem działania posterunku jest zasięg terytorialny nadleśnictwa.

1. Do obowiązków strażnika leśnego należy zapobieganie i zwalczanie przestępstw i wykroczeń w zakresie szkodnictwa leśnego, ochrona składników mienia nadleśnictwa oraz prowadzenie magazynu broni.
2. Przy wykonywaniu zadań i czynności, strażnik leśny korzysta z uprawnień, o których mowa w art. 45 – 47 ustawy o lasach.
3. Strażnicy leśni prowadzą sprawy związane z rejestracją przestępstw i ich sprawców w Krajowym Centrum Informacji Kryminalnej (KCIK).
4. Strażnik leśny niezwłocznie reaguje na wszelkie przejawy szkodnictwa leśnego zgodnie z zarządzeniem nr 46 DGLP z dnia 06.06.2015 r.
5. Bierze udział w akcjach zabezpieczenia p.poż nadleśnictwa na podstawie odrębnych zarządzeń.
6. Zakres obowiązków i odpowiedzialności komendanta posterunku straży leśnej oraz strażników leśnych określają szczegółowe zakresy czynności.
7. Strażnik leśny wyznaczony przez Nadleśniczego Nadleśnictwa Rozwadów pełni funkcję pełnomocnika ds. UODO, który podejmuje działania zmierzające do zapewnienia przestrzegania przepisów o ochronie danych osobowych w związku z zapobieganiem i zwalczaniem przestępczości związanej z przetwarzaniem tych danych, prowadzi wymaganą prawem i uregulowaniami

wewnętrzny dokumentację oraz realizuje wszystkie zadania przewidziane dla pełnomocnika ds. UODO w Polityce bezpieczeństwa danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości w PGL Lasy Państwowe wprowadzonej do użytku służbowego w Nadleśnictwie. Służbowo podlega bezpośrednio Nadleśniczemu.

§ 13

Inżynier nadzoru (NN1, NN2)

1. W Nadleśnictwie Rozwadów zatrudnia się dwóch inżynierów nadzoru (**NN1, NN2**), którym przydziela się odpowiednio po jednej grupie leśnictw. Pierwszą grupę stanowią leśnictwa o kodach 01,03,04,09,10,11 zaś drugą leśnictwa o kodach 02,05,06,07,08.
2. Inżynierowie nadzoru (**NN1, NN2**) prowadzą kontrolę funkcjonalną zarówno w biurze nadleśnictwa jak i przydzielonych leśnictwach, w zakresie ustalonym przez nadleśniczego, opartą na kryteriach legalności, celowości, gospodarności i rzetelności oraz odpowiadają przed nadleśniczym za skuteczność tej kontroli.
3. Inżynierowie nadzoru współpracują z zastępcą nadleśniczego w sprawach dotyczących planowania gospodarczego, koordynacji i realizacji prac gospodarczych oraz aktualizacji Leśnej Mapy Numerycznej (LMN) i opisów taksacyjnych w Systemie Informatycznym Lasów Państwowych (SILP).
4. Inżynierowie nadzoru w kontaktach z leśniczymi są organem doradczym, nadzorującym oraz kontrolującym bieżące prace.
5. Inżynierowie nadzoru prowadzą sprawy związane z inicjowaniem lub wdrażaniem innowacji.
6. Inżynierowie nadzoru uczestniczą w opracowaniu planu urządzenia lasu dla Nadleśnictwa Rozwadów, zwłaszcza w uzgodnieniu prac terenowych oraz biorą udział w komisjach dotyczących ustaleń zakresu i realizacji planu.
7. Inżynierowie nadzoru kontrolują warunki pracy i przestrzeganie przepisów bhp przy pracach leśnych.
8. Inżynierowie nadzoru realizują zadania operacyjne (obronne) nałożone na nadleśnictwo.
9. Inżynierowie nadzoru odpowiadają za wykonywanie przez siebie zadań w zakresie zwalczania szkodnictwa leśnego, które określają odpowiednie zapisy w ustawie o lasach i aktualnie obowiązującej Instrukcji ochrony lasu przed szkodnictwem.
10. Inżynierowie nadzoru uczestniczą czynnie w rozpatrywaniu reklamacji ilościowego i jakościowego surowca drzewnego.
11. Szczegółowe zakresy obowiązków i odpowiedzialności służbowej inżynierów nadzoru określają ich zakresy czynności oraz regulamin kontroli wewnętrznej Nadleśnictwa Rozwadów.
12. Inżyniera nadzoru w razie konieczności zastępuje drugi inżynier nadzoru lub osoba wyznaczona przez nadleśniczego.
13. Inżynierowie nadzoru realizują Politykę Komunikacyjną PGL LP.

Rozdział IV Czynności wspólne

§ 14

Wszystkie komórki organizacyjne nadleśnictwa zobowiązane są do współpracy, udzielania sobie wzajemnie pomocy oraz uzgadniania stanowisk przed przedstawieniem ich do akceptacji nadleśniczemu.

Do zadań wspólnych komórek organizacyjnych należy:

1. Współpraca z komórką wiodącą przy sporządzaniu planu finansowo-gospodarczego.
2. Stałe podnoszenie kwalifikacji zawodowych pracowników poprzez śledzenie na bieżąco nowatorskich rozwiązań, nowych technik pracy oraz współpraca z ośrodkami naukowymi w zakresie swojego działania,
3. Współdziałanie w prowadzeniu szkoleń i doradztwa zawodowego.
4. Sporządzanie sprawozdawczości statystycznej i informacji wewnętrznej w zakresie swojego działania.
5. Obsługa modułów funkcjonowania SILP w zakresie merytorycznego działania komórki organizacyjnej.
6. Przygotowanie, aktualizacja informacji publicznych przeznaczonych do umieszczenia na stronie Biuletynu Informacji Publicznej i stronie internetowej Nadleśnictwa Rozwadów w zakresie merytorycznego działania komórki organizacyjnej.

§ 15

Do zadań kierowników komórek organizacyjnych należy między innymi:

1. Ustalanie szczegółowych zakresów czynności podległym pracownikom oraz ich bieżące aktualizowanie, które po zatwierdzeniu przez nadleśniczego, przyjmują do realizacji pracownicy potwierdzając otrzymanie datą i własnoręcznym podpisem.
2. Organizowanie pracy podległym pracownikom poprzez rozdzielanie równomierne zadań, udzielanie wskazówek dotyczących sposobu ich realizacji, jak też terminowego i zgodnego z obowiązującymi przepisami wykonania przydzielonych zadań.
3. Zapewnienie bezpieczeństwa danych, przestrzegania dyscypliny pracy oraz przepisów o zabezpieczeniu informacji niejawnych i tajemnicy służbowej przez podległych pracowników.
4. Samodzielne wykonywanie w niezbędnym zakresie, zadań o szczególnym stopniu złożoności i pilności oraz parafowanie pism i dokumentów opracowanych przez podwładnych.
5. Działania na rzecz podnoszenia kwalifikacji pracowników komórek organizacyjnych.
6. Wykonywanie innych zadań zleconych przez przełożonego.

§ 16

Do obowiązków wszystkich pracowników nadleśnictwa, w zakresie swojego działania, należy:

1. Postępowanie zgodne z obowiązującymi przepisami, zasadami i instrukcjami oraz terminowe załatwianie przydzielonych spraw.
2. Szczegółowa znajomość i przestrzeganie przepisów prawnych z zakresu swojego działania.
3. Zapewnienie zgodności danych z dokumentów analogowych z danymi zawartymi w bazie danych SILP.
4. Przestrzeganie zasad ochrony danych zgromadzonych w SILP oraz ich zabezpieczenie przed dostępem osób nieuprawnionych oraz informowanie przełożonych o wszystkich zauważonych przypadkach naruszenia tych zasad.
5. Bieżące informowanie przełożonego o występujących nieprawidłowościach i opóźnieniach w realizacji zadań oraz inicjowanie lub wnoszenie usprawnień w działalności nadleśnictwa.

6. Ochrona majątku zarządzanego przez nadleśnictwo.
7. Realizowanie zadań z zakresu ochrony mienia i ochrony lasów przed szkodnictwem w zakresie swojego działania, zgodnie z zarządzeniem nr 46 Dyrektora Generalnego Lasów Państwowych z dnia 06 czerwca 2015 roku; za niedopełnienie obowiązków służbowych w zakresie reagowania na przypadki szkodnictwa leśnego pracownicy ponoszą odpowiedzialność służbową.
8. Przestrzeganie zasad bhp i przepisów przeciwpożarowych.
9. Przestrzeganie przepisów o ochronie informacji niejawnych i tajemnicy przedsiębiorcy.
10. Przestrzeganie zasad Instrukcji kancelaryjnej i archiwalnej,
11. Współpraca ze specjalistą ds. pracowniczych w zakresie ochrony danych osobowych.
12. Współpraca z Działem Gospodarki Leśnej oraz Działem Administracyjno-Gospodarczym nadleśnictwa, odpowiedzialnym za zamówienia publiczne w zakresie konieczności zastosowania ustawy o zamówieniach publicznych (w zakresie działania określonego działu lub stanowiska).
13. Wykonywanie wyznaczonych zadań obronnych w zakresie swojego działania, koordynowanych przez komendanta posterunku straży leśnej.
14. Przygotowywanie informacji i materiałów na cele obsługi mediów i innych działań promocyjno-informatycznych.
15. Wykonywanie innych czynności tematycznie związanych z zakresem działania, wynikających z aktów normatywnych lub poleceń przełożonego, w tym wspólne uzgadnianie z pracownikami innych działów projektów dokumentów lub rozwiązań organizacyjnych.

Rozdział V

Zasady funkcjonowania nadleśnictwa

§ 17

Nadleśnictwo funkcjonuje wg następujących zasad:

1. Każdy pracownik nadleśnictwa podlega bezpośrednio tylko jednemu przełożonemu (wg. kompetencji), od którego otrzymuje polecenia służbowe i przed którym odpowiada za ich właściwe wykonywanie.
2. Pracownik, który otrzyma polecenie od przełożonego wyższego szczebla powinien polecenie to wykonać, zawiadamiając o tym (w miarę możliwości) jeszcze przed jego wykonaniem swojego bezpośredniego przełożonego.
3. W przypadku otrzymania polecenia sprzecznego z obowiązującymi przepisami, pracownikowi przysługuje prawo żądania potwierdzenia go na piśmie. Podobnego potwierdzenia pracownik może żądać od innego pracownika nadleśnictwa, który pośredniczy w przekazywaniu polecenia przełożonego lub wydaje polecenie z jego upoważnienia.
4. W przypadku czasowego oddelegowania pracownika do pracy w innej komórce organizacyjnej nadleśnictwa lub do innej jednostki, pozostaje on w zależności służbowej w zakresie pełnionych funkcji służbowych od przełożonego tej komórki lub jednostki, do której został oddelegowany.
5. Z czynności związanych z przekazaniem – przejściem stanowiska pracy, w związku ze zmianami osobowymi, należy sporządzić protokół zdawczo-odbiorczy, podpisany przez przekazującego, przejmującego oraz właściwego przełożonego (lub osobę przez niego upoważnioną), bądź komisyjnie, jeśli komisja została powołana oddzielnym zarządzeniem nadleśniczego. Dotyczy to stanowisk: nadleśniczego, zastępcy nadleśniczego, głównego księgowego, inżyniera nadzoru, sekretarza, specjalisty ds. pracowniczych, komendanta

- posterunku straży leśnej i leśniczego, lub na polecenie nadleśniczego, innych pracowników odpowiedzialnych materialnie.
6. Przed rozwiązaniem stosunku pracy z pracownikiem nadleśnictwa jest on zobowiązany do rozliczenia się z powierzonego mu majątku, uregulowania wszelkich zobowiązań oraz przedłożenia karty obiegowej. Karty obiegowe wydaje do wypełnienia oraz przechowuje w aktach osobowych specjalista ds. pracowniczych.
 7. Umowy o zakazie konkurencji w czasie trwania stosunku pracy zawiera się z pracownikami zatrudnionymi na stanowiskach: nadleśniczego, zastępcy nadleśniczego, głównego księgowego, inżyniera nadzoru, leśniczego (zgodnie z Zarządzeniem nr 10 Dyrektora Generalnego L.P. z dnia 29 stycznia 2003r.).

§ 18

Do składania oświadczeń woli w zakresie działania nadleśnictwa uprawnieni są:

1. Nadleśniczy.
2. Zastępcy nadleśniczego, główny księgowy i radca prawny na podstawie i w zakresie udzielonych im przez nadleśniczego pełnomocnictw. Kopie udzielonych pełnomocnictw, przechowywane są przez pracownika ds. pracowniczych.

§ 19

Korespondencja wychodząca na zewnątrz podpisywana jest jednoosobowo przez nadleśniczego lub osobę zastępującą z wyjątkiem:

1. pism i dokumentów, które z mocy przepisów wymagają podpisów dwóch uprawnionych osób (zmiany w rzeczowym lub pieniężnym stanie składników majątkowych, w stanie dokumentacji lub sprawozdawczości, w zakresie planowania i ewidencji finansowej);
2. korespondencji, z której wynikają zobowiązania majątkowe i która powinna być podpisana także przez głównego księgowego;

§ 20

Projekty pism wychodzących i innych opracowań przedkładanych nadleśniczemu do podpisu, parafowane są przez pracownika sporządzającego oraz przez jego bezpośredniego przełożonego, zgodnie z obowiązującą instrukcją systemu EZD.

§ 21

Zasady funkcjonowania SILP

Zasady funkcjonowania SILP oraz serwisów informatycznych działających w domenie Lasów Państwowych, obejmują kompleksowe współdziałanie pracowników, komórek i jednostek organizacyjnych LP przy zastosowaniu technik komputerowych będących na wyposażeniu tych jednostek.

1. Za prawidłowe funkcjonowanie SILP oraz serwisów informatycznych w nadleśnictwie odpowiada nadleśniczy. Realizuje on swoje obowiązki w tym zakresie w oparciu o strukturę organizacyjną nadleśnictwa w tym poprzez powołanych administratorów systemu (administratorzy powołani są odrębnym zarządzeniem).
2. Każdy pracownik, w którego zakresie działania znajdują się zagadnienia objęte SILP oraz serwisami informatycznymi (a będący ich użytkownikiem) posiada dostęp do ich modułów związanych z obowiązującym zakresem czynności i jest zobowiązany do:

- 1) opanowania umiejętności posługiwania się systemem przynajmniej w zakresie swego działania,
 - 2) prawidłowego i rzetelnego wprowadzania danych do systemu (przy pomocy informatycznych nośników informacji lub ręcznie) oraz ochrony i przetwarzania danych osobowych,
 - 3) terminowego wprowadzania dokumentów do SILP lub innych serwisów informatycznych działających w domenie Lasów Państwowych,
 - 4) zgłaszania w „Systemie Zgłaszania Błędów” lub do administratorów systemu wszelkich zauważonych błędów i nieprawidłowości w funkcjonowaniu SILP i innych serwisów informatycznych,
 - 5) zapoznania się i stosowania „Zasad funkcjonowania systemu informatycznego w Lasach Państwowych” zawartych w zarządzeniu nr 35 Dyrektora Generalnego Lasów Państwowych z dnia 18 maja 2026 r. w sprawie zasad funkcjonowania i zasad bezpieczeństwa systemu informatycznego w Państwowym Gospodarstwie Leśnym Lasy Państwowe, (znak: EI.0413.3.2026).
3. Bezpośredni przełożony użytkownika SILP i innych serwisów informatycznych odpowiada za:
- 1) egzekwowanie znajomości programu użytkowego zgodnego z zakresem czynności podległych pracowników,
 - 2) poprawności formalno-merytorycznej dokumentów wprowadzonych do SILP i innych serwisów informatycznych
 - 3) zgodności danych w dokumencie z danymi wprowadzonymi do systemów informatycznych (np. EZD),
 - 4) terminowości wprowadzania dokumentów do systemów informatycznych,
 - 5) do każdego modułu funkcjonalnego SILP jest opracowywana instrukcja użytkownika SILP.

§ 22

1. Zasady funkcjonowania zintegrowanego systemu informatycznego w LP określone są w Załączniku nr 1 do Zarządzenia nr 35 Dyrektora Generalnego Lasów Państwowych z dnia 18 maja 2026 r. w sprawie zasad funkcjonowania i zasad bezpieczeństwa systemu informatycznego w Państwowym Gospodarstwie Leśnym Lasy Państwowe (znak: EI.0413.3.2026), który stanowi załącznik nr 4 do regulaminu organizacyjnego Nadleśnictwa Rozwadów.
2. Zasady bezpiecznej eksploatacji zasobów informatycznych LP określone są w Załączniku nr 2 do Zarządzenia nr 35 Dyrektora Generalnego Lasów Państwowych z dnia 18 maja 2026 r. w sprawie zasad funkcjonowania i zasad bezpieczeństwa systemu informatycznego w Państwowym Gospodarstwie Leśnym Lasy Państwowe (znak: EI.0413.3.2026), który stanowi załącznik nr 5 do regulaminu organizacyjnego Nadleśnictwa Rozwadów. Do załącznika nr 5 dołącza się również regulamin użytkownika systemu poczty elektronicznej LP oraz urządzenia uwierzytelniania użytkowników LP (wprowadzone na podstawie Załącznika nr 2 do Zarządzenia nr 35 Dyrektora Generalnego Lasów Państwowych z dnia 18 maja 2026 r. w sprawie zasad funkcjonowania i zasad bezpieczeństwa systemu informatycznego w Państwowym Gospodarstwie Leśnym Lasy Państwowe).
3. Zasady dostępu do danych w SILP są zawarte w Załączniku nr 3 do Zarządzenia nr 35 Dyrektora Generalnego Lasów Państwowych z dnia 18 maja 2026 r. w sprawie zasad funkcjonowania i zasad bezpieczeństwa systemu informatycznego w Państwowym Gospodarstwie Leśnym Lasy Państwowe, (znak: EI.0413.3.2026), który stanowi załącznik nr 6 do regulaminu organizacyjnego Nadleśnictwa Rozwadów.
4. W systemie Elektronicznego Zarządzania Dokumentacją Nadleśnictwa Rozwadów

dopuszcza się posługiwanie/podpisywanie dokumentów zewnętrznych podpisem kwalifikowanym wydanym przez certyfikowanego dostawcę usług zaufania. Podpisem kwalifikowanym mogą posługiwać się wszyscy pracownicy Nadleśnictwa Rozwadów według swoich kompetencji i którym pracodawca zakupił taki podpis.

§ 23

Ochrona Danych

1. W zakresie ochrony danych osobowych w Nadleśnictwie Rozwadów stosuje się:
 - a) Rozporządzenie Parlamentu Europejskiego Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) zwane „RODO”;
 - b) Ustawę z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. 2019 r. poz. 1781 z późn.zm.) zwaną „UODO”.
 - c) Ustawę z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125 z późn. zm.) zwane dalej jako: „UDODO”.
 - d) Politykę Ochrony Danych Osobowych w Nadleśnictwie Rozwadów.
2. Nadzór nad przestrzeganiem bezpieczeństwa danych osobowych w Nadleśnictwie Rozwadów może pełnić firma zewnętrzna na podstawie umowy cywilnoprawnej.
3. Podmiot prowadzący nadzór nad ochroną danych osobowych wskazany w pkt 2 obowiązany jest do dostosowania procesów przetwarzania danych osobowych, systemów informatycznych oraz dokumentacji do wymagań RODO, wprowadzenia zmian do istniejącej dokumentacji dotyczącej przetwarzania danych osobowych, zapewnienia odpowiednich środków technicznych i organizacyjnych, przeprowadzenia szkoleń dla pracowników Administratora Danych, konsultacji telefonicznych/e-mail w zakresie ochrony danych osobowych.

§ 24

Obsługa prawna

1. Obsługa prawna w Nadleśnictwie sprawowana jest przez radców prawnych wykonujących te czynności na podstawie umowy, która określa zakres przedmiotowy zlecenia.
2. Zasięgnięcia opinii prawnej, przed podpisaniem dokumentu przez nadleśniczego, wymagają m.in. sprawy:
 1. wydanie aktu prawnego o charakterze ogólnym,
 2. indywidualne, skomplikowane pod względem prawnym,
 3. zawarcie lub rozwiązanie umowy długoterminowej, porozumienia bądź zobowiązania,
 4. rozwiązania z pracownikiem umowy o pracę bez okresu wypowiedzenia,
 5. odmowy uznania zgłoszonych roszczeń,
 6. związane z postępowaniem przed organami orzekającymi w sprawach cywilnych,
 7. zawarcie ugody w sprawach majątkowych
 8. inne, które w ocenie nadleśniczego lub jego zastępcy powinny uzyskać parafę radcy prawnego

§ 25

Zasady zastępstw

Nadleśniczego zastępuje w czasie jego nieobecności zastępca nadleśniczego, wg. kolejności Z1 następnie Z2, a w przypadku nieobecności zastępców nadleśniczego główny księgowy lub wyznaczony przez nadleśniczego inny pracownik.

1. Zakres zastępstwa ustala nadleśniczy, który każdorazowo zawiadamia zastępcę nadleśniczego lub głównego księgowego lub innego wyznaczonego przez siebie pracownika o przewidywanej swojej nieobecności i powierza mu zastępstwo. Wyznaczonemu pracownikowi zastępstwo powierzane jest ustnie lub na piśmie. Osoba zastępująca pełni powierzoną funkcję wyłącznie w czasie nieobecności nadleśniczego.
2. Jeżeli nadleśniczy nie może pełnić obowiązków służbowych i nie może określić zakresu zastępstwa, zakres zastępstwa pełnionego przez zastępcę nadleśniczego obejmuje wszystkie zadania i kompetencje nadleśniczego. Zastępca nadleśniczego ponosi w tym przypadku całkowitą odpowiedzialność za decyzje podjęte w czasie pełnienia tego zastępstwa.
3. W czasie urlopu lub innych nieobecności pracownicy nadleśnictwa zastępują lub są zastępowani zgodnie z zapisami zawartymi w zakresach czynności.

§ 26

Skargi i wnioski

Nadleśniczy lub wyznaczony przez niego zastępca, przyjmuje interesantów w sprawach skarg i wniosków w każdy wtorek w godz. 13⁰⁰ – 15³⁰ lub w dzień następny w przypadku, gdy wtorek jest dniem wolnym od pracy w godzinach od 13⁰⁰ do 15³⁰. Informacja o dniach i godzinach przyjęć w sprawach skarg i wniosków wywieszona jest na tablicy ogłoszeń jak również na tablicach informacyjnych w kancelariach leśnictw.

1. Ewidencję przyjęć interesantów w sprawie skarg i wniosków prowadzi sekretariat nadleśnictwa.
2. Szczegółowy tryb rozpatrywania skarg i wniosków określa zarządzenie wewnętrzne w sprawie organizacji, przyjmowania i rozpatrywania skarg i wniosków w Nadleśnictwie Rozwadów.

§ 27

Staże w nadleśnictwie

1. W nadleśnictwie zatrudniani są absolwenci wyższych i średnich szkół na czas określony, zwany stażem. Staż dla absolwentów szkół leśnych odbywa się zgodnie z Zarządzeniem Dyrektora Generalnego Lasów Państwowych nr 59 z dnia 07 września 2012 roku.
2. W Nadleśnictwie Rozwadów organizowane są również praktyki zawodowe dla uczniów szkół średnich lub wyższych.

§ 28

1. Czas oraz zasady dyscypliny pracy w nadleśnictwie określa Regulamin pracy nadleśnictwa.
2. Tok i zakres czynności kancelaryjnych regulują instrukcje: kancelaryjna, obiegu dokumentów, instrukcja obsługi systemu EZD PUW i inne przepisy.
3. Postępowanie w sprawach ochrony informacji niejawnych regulują odrębne przepisy i instrukcje.

§ 29

Kontrola wewnętrzna

1. Cel, zakres i formy sprawowania kontroli wewnętrznej oraz zadania w tym zakresie poszczególnych działów i stanowisk pracy określa regulamin kontroli wewnętrznej, opracowany i uaktualniany przez głównego księgowego, a zatwierdzany przez nadleśniczego. Regulamin ten określa szczegółowe zadania i obowiązki w zakresie funkcjonalnej kontroli wewnętrznej poszczególnych działów, pracowników działów i stanowisk pracy
2. Obieg dokumentów, ich sporządzanie, kontrola oraz zatwierdzanie i przechowywanie w nadleśnictwie określone są w dokumencie „Schemat obiegu dokumentów” stanowiącym załącznik do regulaminu kontroli wewnętrznej.

Rozdział VI

Tryb pracy z uwzględnieniem obiegu informacji

§ 30

1. W nadleśnictwie Rozwadów czynności kancelaryjne, w tym przyjmowanie, dekretowanie, przekazywanie, prowadzenie spraw, akceptowanie, podpisywanie, udostępnianie pism i dokumentów wykonywane są w systemie elektronicznego zarządzania dokumentacją (EZD), który na podstawie Decyzji nr 104 Dyrektora Regionalnej Dyrekcji Lasów Państwowych z dnia 09.12.2020 r. w sprawie wprowadzenia elektronicznego zarządzania dokumentacją w biurze nadleśnictwa Rozwadów, od dnia 04.01.2021 r. jest podstawowym sposobem dokumentowania przebiegu załatwiania i rozstrzygania spraw w biurze nadleśnictwa.
2. Szczegółowe zasady funkcjonowania systemu EZD, a także procedury obiegu spraw i postępowania z dokumentacją określa odrębne zarządzenie Nadleśniczego w sprawie zasad postępowania z dokumentacją i wykonywania czynności kancelaryjnych w systemie elektronicznego zarządzania dokumentacją, w biurze nadleśnictwa Rozwadów sporządzone w oparciu o obowiązującą Instrukcję Kancelaryjną.

Rozdział VII

Postanowienia końcowe

§ 31

W sprawach nieuregulowanych niniejszym regulaminem organizacyjnym mają zastosowanie przepisy prawa powszechnie obowiązujące, a w szczególności: Kodeksu pracy, Kodeksu cywilnego, Kodeksu postępowania administracyjnego, a także przepisy wewnątrzbranżowe, w tym: ustawa z dnia 28 września 1991 roku o lasach oraz przepisami wykonawczymi, Statut PGL LP, PUZP, zarządzenia i decyzje Dyrektora Generalnego Lasów Państwowych, Dyrektora RDLP w Lublinie.

1. Nadleśnictwo Rozwadów jest przewidziane do militaryzacji i po jej ogłoszeniu wchodzi w skład jednostki zmilitaryzowanej – RDLP Lublin. Od tej chwili obowiązuje zarządzenie Nadleśniczego Nadleśnictwa Rozwadów w sprawie zmian do regulaminu organizacyjnego nadleśnictwa po objęciu militaryzacją.
2. Nadleśnictwo Rozwadów, jako jednostka organizacyjna wykonująca zadania na rzecz obronności i bezpieczeństwa państwa jest jednostką przewidzianą do militaryzacji.

§ 32

Załącznikami do Regulaminu Organizacyjnego są:

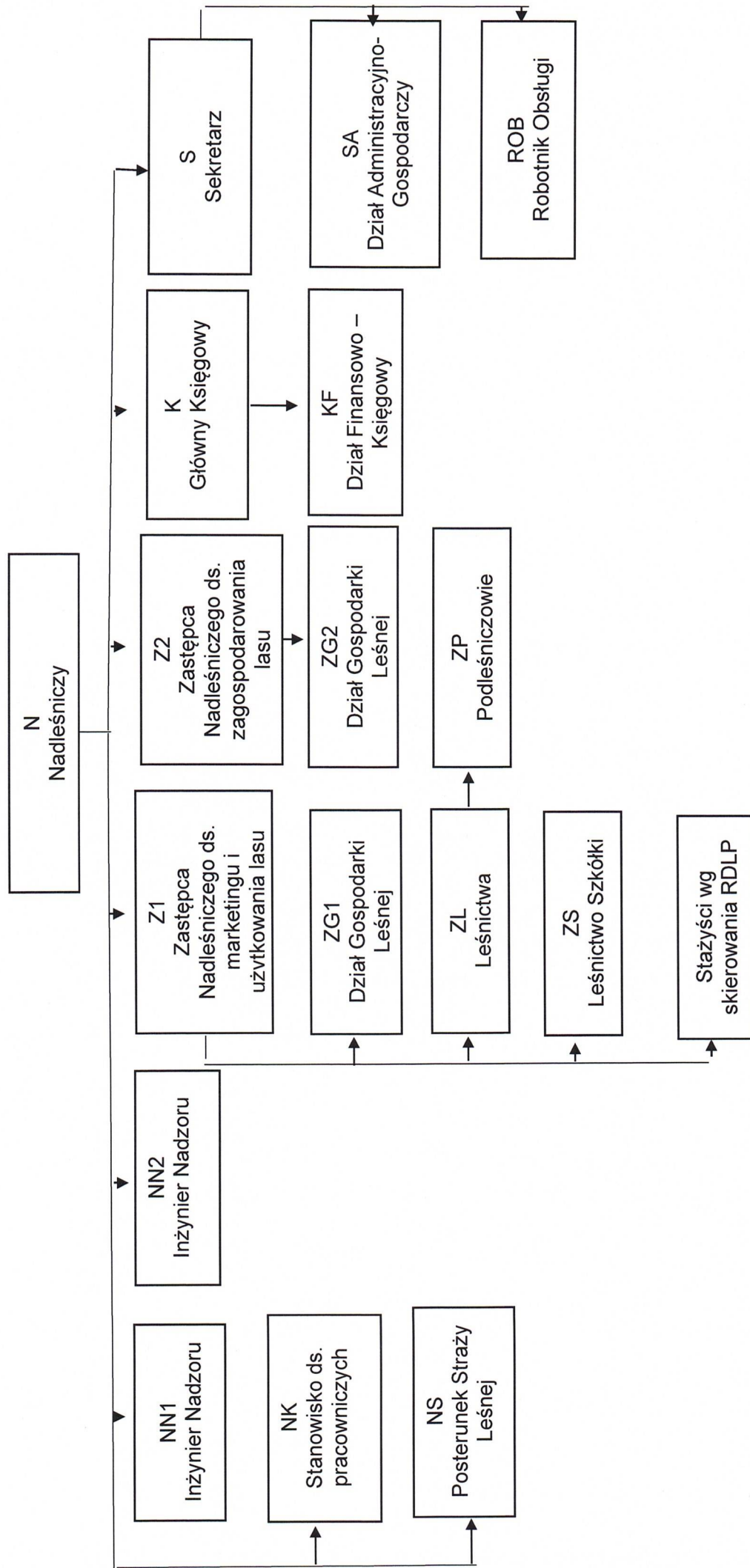
- a. schemat organizacyjny nadleśnictwa (zał. nr 1),
- b. wykaz leśnictw (zał. nr 2),
- c. wykaz imienny pracowników nadleśnictwa upoważnionych do stosowania w SILP funkcji „GLOBAL” (zał. nr 3),
- d. zasady funkcjonowania zintegrowanego systemu informatycznego w LP (zał. nr 4),
- e. zasady bezpiecznej eksploatacji zasobów informatycznych LP, regulamin użytkownika systemu poczty elektronicznej LP oraz urządzenia uwierzytelniania użytkowników LP (zał. nr 5),
- f. zasady dostępu do danych w SILP (zał. nr 6),

Stalowa Wola, 22.06.2026.r.

Niniejszy Regulamin zatwierdzam

NADLEŚNICZY
Nadleśnictwa Rozwadów
mgr inż. Wojciech Chołpa

SCHEMAT STRUKTURY ORGANIZACYJNEJ NADLEŚNICTWA ROZWADÓW



NADLEŚNICZY
Nadleśnictwa Rozwadów
mgr inż. Wojciech Chęłpa

**Wykaz leśnictw z docelową obsadą stanowisk
robotniczych i nierobotniczych**

Lp.	Leśnictwo	Obsada	
		leśniczy	podleśniczy
1.	Burdze	1	1
2.	Ciemny Kąt	1	2
3.	Charzewice	1	1
4.	Moskale	1	1
5.	Zaosie	1	1
6.	Zapolednik	1	2
7.	Żupawa	1	1
8.	Huta Deręgowska	1	1
9.	Katy	1	1
10.	Pysznicza	1	2
11.	Szkółki	1	-
Razem		11	13

Stalowa Wola, 22.06.2026 r.

NADLEŚNICZY
Nadleśnictwa Rozwadów
mgr inż. Wojciech Chęłpa

WYKAZ OSÓB UPOWAŻNIONYCH DO STOSOWANIA FUNKCJI „GLOBAL”

1. Jędral Radosław
2. Ciba Mariusz
3. Dul Małgorzata
4. Dul Krzysztof
5. Hara Łukasz
6. Kawęcka Anna
7. Serafin Miłosz
8. Kłosowski Artur
9. Kumięga Barbara
10. Myszka Patrycja
11. Nowak Anna
12. Paleń Łukasz
13. Pucuła Ewa
14. Smogorzewska Paulina
15. Wołoszyn Malwina
16. Zawiślak Marta
17. Zarzeczna- Pistor Magdalena
18. Krasowska Barbara

Wyżej wymienione osoby upoważnione są do stosowania funkcji „GLOBAL” zgodnie z przyznanymi uprawnieniami w SILP, stosownie do ustalonego indywidualnie dla każdego pracownika zakresu czynności.

Data: 22.06.2026 r.

NADLEŚNICZY

NADLEŚNICZY
Nadleśnictwa Rozwadów
mgr inż. Wojciech Chelpa

ZASADY FUNKCJONOWANIA ZINTEGROWANEGO SYSTEMU INFORMATYCZNEGO W LASACH PAŃSTWOWYCH

§ 1

Terminy użyte w tekście

1. **Lasy Państwowe, PGL LP, LP** – Państwowe Gospodarstwo Leśne Lasy Państwowe.
2. **DGLP** – Dyrekcja Generalna Lasów Państwowych.
3. **rdLP** – regionalne dyrekcje Lasów Państwowych.
4. **SILP** – Zintegrowany System Informatyczny Lasów Państwowych, zbiór elementów, którego funkcją jest przetwarzanie, przechowywanie i przesyłanie danych w PGL LP przy użyciu zasobów informatycznych LP.
5. **System LAS** – system i podstawowa aplikacja biznesowa LP.
6. **SZKZ** – System Zarządzania Kodami Źródłowymi SILP.
7. **SZBM** – narzędzie udostępnione poprzez przeglądarkę internetową pod nazwą „System Zgłaszania Błędów i Modyfikacji SILP”.
8. **WAN LP** – sieć rozległa Lasów Państwowych, komputerowa sieć modelu TCP/IP służąca do przesyłania danych pomiędzy jednostkami LP.
9. **Sieć LP** – wszystkie sieci transmisji danych będące własnością bądź zarządzane przez LP.
10. **Dostęp zdalny VPN** – dostęp do wewnętrznych zasobów SILP z sieci Internet za pośrednictwem szyfrowanych połączeń IPsec lub SSL.
11. **WI DGLP** – Wydział Informatyki Dyrekcji Generalnej Lasów Państwowych.
12. **ZCI** – Zespół do spraw Cyberbezpieczeństwa w WI DGLP, odpowiedzialny za nadzór nad bezpieczeństwem SILP.
13. **SZBI** – System Zarządzania Bezpieczeństwem Informacji, zestaw zasad, procesów, procedur, struktur organizacyjnych i zasobów wykorzystywanych do ochrony bezpieczeństwa informacji SILP.
14. **ZILP** – Zakład Informatyki Lasów Państwowych.
15. **WI** – komórki organizacyjne rdLP właściwe do spraw informatyki oraz administracji SILP w jednostkach nadzorowanych.

16. **Administrator SILP** – pracownik wyznaczony przez kierownika jednostki LP, posiadający rozszerzone uprawnienia do zarządzania powierzonymi zasobami SILP, odpowiedzialny za ich utrzymanie, bezpieczeństwo i ciągłość działania.
17. **Użytkownik SILP** – pracownik jednostki LP w okresie pozostawania w stosunku zatrudnienia lub inna osoba fizyczna wykonująca prace na podstawie umowy o dzieło, umowy zlecenia lub innej umowy cywilnoprawnej w okresie obowiązywania umowy, których zakresy obowiązków wymagają dostępu do SILP.
18. **Instruktor regionalny SILP** – wyznaczony przez dyrektora rdLP pracownik biura RDLP lub jednostki nadzorowanej, który świadczy pomoc oraz prowadzi szkolenia w określonym zakresie funkcjonalnym SILP.
19. **Koordynator regionalny SZBM** – Instruktor regionalny SILP lub wyznaczony przez dyrektora rdLP pracownik biura RDLP, który koordynuje zgłoszenia w systemie SZBM wprowadzane przez pracowników jednostek własnej RDLP.
20. **Koordynator centralny SZBM** – wyznaczony przez Dyrektora Generalnego LP pracownik LP, który koordynuje zgłoszenia w systemie SZBM w przypisanym zakresie merytorycznym.
21. **AD** – Active Directory usługa katalogowa, katalog użytkowników i komputerów pracujących w sieci LP, zdefiniowana w osobnym dokumencie „Projekt usług katalogowych PGL LP”.
22. **Dane stanowiące tajemnicę przedsiębiorstwa SILP** – dane stanowiące tajemnicę przedsiębiorstwa, zgodnie z klasyfikacją danych określoną szczegółowo w odrębnym zarządzeniu Dyrektora Generalnego Lasów Państwowych.
23. **PKI LP** – infrastruktura klucza publicznego Lasów Państwowych utrzymywana w ramach wewnętrznych zasobów SILP.
24. **Stacja robocza** – stacjonarny lub przenośny komputer klasy PC wraz z oprogramowaniem systemowym i aplikacjami, stanowiący podstawowe narzędzie pracy użytkowników w SILP.

§ 2

System Informatyczny Lasów Państwowych

1. System Informatyczny Lasów Państwowych, stanowi zbiór elementów wzajemnie współpracujących, których funkcją jest przetwarzanie danych w PGL LP przy użyciu:
 - 1) sprzętu,
 - 2) oprogramowania,
 - 3) elementów organizacyjnych,
 - 4) technik informacyjnych.

2. Podstawą prawidłowego funkcjonowania SILP, na każdym szczeblu organizacyjnym, jest:
 - 1) spójna polityka dotycząca wykorzystania jednolitej platformy sprzętowej, systemowej i programowej,
 - 2) wspólne zasady gromadzenia, przetwarzania i wymiany informacji,
 - 3) kompleksowe współdziałanie pracowników, komórek i jednostek organizacyjnych LP.
3. Nadzór nad prawidłowym funkcjonowaniem SILP sprawują Kierownicy jednostek organizacyjnych, w szczególności w zakresie:
 - 1) przestrzegania zasad bezpieczeństwa,
 - 2) wdrażania zmian SILP,
 - 3) szkolenia pracowników.

§ 3

Informatyka w Lasach Państwowych

1. W celu zabezpieczenia realizacji zadań utrzymania i rozwoju SILP:
 - 1) Dyrektor Generalny Lasów Państwowych powołuje:
 - a) WI w DGLP,
 - b) Zespół ds. Cyberbezpieczeństwa – wyodrębnioną strukturę w ramach Wydziału Informatyki DGLP
 - c) ZILP,
 - d) zespoły zadaniowe – wg potrzeb.
 - 2) Dyrektorzy regionalnych dyrekcji Lasów Państwowych powołują:
 - a) WI w rdLP,
 - b) Instruktorów regionalnych SILP i/lub koordynatorów SZBM,
 - c) zespoły zadaniowe – wg potrzeb.
2. Kierownicy pozostałych jednostek organizacyjnych ujmują w strukturze organizacyjnej kierowanej przez siebie jednostki stanowisko lub stanowiska administratorów SILP.
3. Szczegółowe zakresy zadań wydziałów informatyki oraz administratorów SILP są określone w regulaminach organizacyjnych jednostek organizacyjnych.
4. Szczegółowe zadania ZILP precyzuje odrębne zarządzenie Dyrektora Generalnego LP.
5. Szczegółowe zakresy zadań Instruktorów regionalnych SILP określają odrębne uregulowania stanowione przez dyrektorów rdLP.

6. Instruktorzy regionalni SILP i koordynatorzy SZBM otrzymują dodatkowe wynagrodzenie, a ramowe kryteria ich wynagradzania ustala Dyrektor Generalny LP.
7. Administratorzy SILP zobowiązani są posiadać stosowny certyfikat uprawniający do pełnienia funkcji administratora SILP. W uzasadnionych sytuacjach dopuszcza się czasowe pełnienie obowiązków administratora SILP bez przedmiotowego certyfikatu. Wymóg posiadania stosownego certyfikatu nie dotyczy administratorów SILP w WI, WI DGLP oraz ZILP.

§ 4

Zadania komórek organizacyjnych rdLP i DGLP, w zakresie wdrażania i eksploatacji SILP

1. Kierowników komórek organizacyjnych rdLP i DGLP czyni się odpowiedzialnymi za znajomość zasad funkcjonowania i wykorzystania systemu informatycznego przez podległych pracowników, co najmniej w zakresie czynności określonych dla danego stanowiska w komórce.
2. Kierowników komórek organizacyjnych DGLP zobowiązuje się do współpracy z prowadzącymi szkolenia dla Instruktorów regionalnych SILP, w zakresie merytorycznej kompetencji danej komórki.
3. Kierowników komórek organizacyjnych rdLP zobowiązuje się do organizowania szkoleń użytkowników SILP w zakresie merytorycznej kompetencji danej komórki.
4. Kierownicy merytorycznych komórek organizacyjnych rdLP nadzorują proces wdrażania nowych funkcjonalności i zmian w SILP w jednostkach podległych w zakresie działania komórki organizacyjnej.

§ 5

Zasady działania w zakresie użytkowania SILP

1. Pracownicy jednostek organizacyjnych Lasów Państwowych, w których zakresie działania znajdują się zagadnienia objęte SILP są zobowiązani do:
 - 1) opanowania umiejętności posługiwania się systemem w zakresie swego działania,
 - 2) prawidłowego i rzetelnego wprowadzania danych do systemu,
 - 3) zgłaszania wszelkich zauważonych błędów i nieprawidłowości w funkcjonowaniu SILP,

- 4) przestrzegania zasad i dbania o zachowanie bezpieczeństwa SILP i przetwarzanych danych.
2. Bezpośredni przełożony użytkownika odpowiada za:
 - 1) stały nadzór nad prawidłowością posiadanych przez pracownika uprawnień w systemie, niezbędnych do prawidłowej realizacji zadań wynikających z zakresu czynności,
 - 2) sprawowanie nadzoru nad działaniami wymienionymi w ust. 1,
 - 3) prawidłowe wykorzystanie przez pracowników modułów funkcjonalnych SILP w zakresie merytorycznego działania komórki organizacyjnej,
 - 4) egzekwowanie przestrzegania zasad ochrony informacji przetwarzanych w systemach teleinformatycznych przez podległych pracowników.

§ 6

Błędy i modyfikacje SILP

1. Błędy i propozycje modyfikacji SILP może zgłosić każda jednostka organizacyjna Lasów Państwowych lub użytkownik SILP.
2. Zgłoszenie błędów i propozycji modyfikacji odbywa się za pośrednictwem SZBM, lub w uzasadnionych przypadkach na pisemny wniosek skierowany drogą służbową.

§ 7

Zgłoszenia błędów w SZBM

1. Zgłoszenia wprowadzone do SZBM podlegają weryfikacji przez koordynatorów regionalnych, stanowiących pierwszą linię wsparcia dla użytkowników.
2. Obsługą zgłoszeń o charakterze merytorycznym lub technicznym wykraczającym poza możliwości rozwiązania na poziomie koordynatorów regionalnych SZBM, zajmują się koordynatorzy centralni SZBM.
3. Koordynatorzy centralni SZBM dokonują oceny zgłoszeń pod względem merytorycznym, kwalifikując zgłoszenie do właściwego zakresu merytorycznego SILP i w przypadku uznania ich zasadności zatwierdzają do realizacji.
4. Koordynatorzy centralni SZBM przed zatwierdzeniem zgłoszenia mogą wymagać dodatkowych informacji od zgłaszającego lub przekazać zgłoszenie do konsultacji do DGLP.

5. Kompletnie zgłoszenia błędów zatwierdzone przez koordynatorów centralnych SZBM są podstawą do przekazania tych zgłoszeń do podmiotu konserwującego dany zakres SILP, w celu podjęcia działań zmierzających do usunięcia błędu.
6. Tryb postępowania w zakresie sposobu i terminów realizacji zatwierdzonych zgłoszeń błędów wynika z odrębnych ustaleń z podmiotem konserwującym dany zakres SILP.

§ 8

Modyfikacje w SILP

1. Koordynacją modyfikacji SILP zajmuje się WI w DGLP. W uzgodnieniu z wydziałami merytorycznymi WI w DGLP opracowuje zlecenia modyfikacji do ZILP wraz z określeniem terminów realizacji.
2. ZILP dokonuje zleconych modyfikacji SILP lub wdraża nowe elementy SILP. Dopuszcza się zlecenie wykonania modyfikacji lub wdrożenia nowych elementów SILP podmiotom zewnętrznym, konserwującym poszczególne elementy SILP w ramach zawartych umów lub innym podmiotom wyłonionym na podstawie odrębnych procedur.
3. W przypadku braku możliwości realizacji modyfikacji w terminie oczekiwanym w zleceniu DGLP, priorytety realizacji modyfikacji ustalają w trybie roboczym członkowie ścisłego kierownictwa DGLP na wniosek naczelnika WI w DGLP.
4. Zmiany w systemie LAS wynikające z usunięcia błędów lub modyfikacji przekazywane są przez Wykonawców w postaci kodów źródłowych, w formacie wymaganym przez SZKZ, wraz dokumentacją techniczną, analityczną i instrukcją użytkownika.
5. Kody źródłowe podlegają weryfikacji w SZKZ pod względem ich poprawności.
6. Po pozytywnym wyniku weryfikacji następuje kompilacja kodów źródłowych do wersji wykonywalnej i przekazanie oprogramowania do testów w ZILP oraz w jednostkach testowych LP powoływanych odrębnymi zarządzeniami Dyrektora Generalnego Lasów Państwowych.
7. Integralną częścią procesu testowania jest ocena przedłożonej dokumentacji wymienionej w ust. 4. Ocena dokumentacji realizowana jest przez ZILP, jednostki testowe i zespoły zadaniowe powołane przez Dyrektora Generalnego Lasów Państwowych.
8. Pozytywny wynik testów oprogramowania oraz pozytywna ocena dokumentacji jest podstawą przekazania modyfikacji do wdrożenia w jednostkach LP.

§ 9

Wdrażanie zmian w systemie LAS

1. Za dystrybucję i udostępnienie nowych wersji oprogramowania aplikacji LAS odpowiada Dyrektor ZILP.
2. Pakiety instalacyjne zawierające nowe wersje oprogramowania są udostępniane za pomocą SZKZ.
3. Udostępnienie autoryzowanego pakietu instalacyjnego, za pomocą SZKZ, jest jednoznaczne z poleceniem jego instalacji i wdrożenia na wszystkich szczeblach organizacyjnych.
4. Dyrektor ZILP odpowiada za dostosowanie i wdrożenie modyfikacji interfejsów, do dedykowanych aplikacji użytkowanych przez zakłady LP (krajowe i regionalne), niezbędnych do zachowania integralności z systemem LAS.
5. ZILP jest uprawniony do samodzielnego wdrożenia aktualizacji oprogramowania LAS na podstawie polecenia wydanego przez Dyrektora Generalnego Lasów Państwowych, bez konieczności uzyskiwania dodatkowych zgód od kierowników pozostałych jednostek LP.

§ 10

Wsparcie użytkowników w procesie wdrażania i eksploatacji SILP

1. Usługi wsparcia użytkowników w procesie wdrażania i eksploatacji SILP świadczą zgodnie z właściwym zakresem merytorycznym:
 - 1) pracownicy wydziałów DGLP w odniesieniu do wszystkich pracowników jednostek LP,
 - 2) pracownicy wydziałów rdLP w stosunku do pracowników biura rdLP i jednostek nadzorowanych przez rdLP,
 - 3) regionalni instruktorzy SILP w stosunku do pracowników biura rdLP i jednostek nadzorowanych przez rdLP,
 - 4) członkowie zespołów zadaniowych powołanych przez Dyrektora Generalnego Lasów Państwowych w zakresie określonym przez zarządzenie, w odniesieniu do wszystkich pracowników jednostek LP,
 - 5) koordynatorzy regionalni SZBM w odniesieniu do pracowników biura rdLP i jednostek nadzorowanych,
 - 6) koordynatorzy centralni SZBM w odniesieniu do wszystkich pracowników jednostek LP,
 - 7) ZILP w odniesieniu do wszystkich pracowników jednostek LP.

2. Usługi wsparcia zdefiniowane w ust. 1. mogą być realizowane za zgodą i na wniosek poprzez bezpośredni dostęp do systemów i danych jednostki zgłaszającej problem.

§ 11

Instrukcje użytkownika

1. Do każdego modułu funkcjonalnego SILP jest opracowywana instrukcja użytkownika.
2. Instrukcje użytkownika opracowuje ZILP na podstawie materiałów własnych lub dokumentacji przekazywanych przez wykonawców.
3. Instrukcje są udostępniane dla użytkowników SILP w bazie wiedzy o systemie informatycznym LP.
4. ZILP zobowiązany jest do dokonywania integracji instrukcji SILP z instrukcjami przekazanymi przez wykonawców. W okresie do czasu jej publikacji dopuszcza się wykorzystanie przez użytkowników instrukcji przygotowanej przez podmiot wykonujący modyfikację.

ZASADY BEZPIECZNEJ EKSPLOATACJI ZASOBÓW INFORMATYCZNYCH LASÓW PAŃSTWOWYCH

§ 1 Zasady ogólne

1. Dane przetwarzane w SILP podlegają ochronie z uwagi na obowiązujące przepisy prawa, w szczególności ustawy o ochronie danych osobowych oraz ustawy o ochronie informacji niejawnych.
2. Zachowanie bezpieczeństwa SILP i bezpieczeństwa danych w nim przetwarzanych jest wspólnym obowiązkiem wszystkich pracowników LP.
3. SILP służy jedynie do wykonywania zadań służbowych.
4. Dostęp do wewnętrznych zasobów SILP jest przyznawany użytkownikom SILP:
 - 1) po złożeniu przez użytkownika oświadczenia stanowiącego załącznik nr 4 do zarządzenia „Wzór oświadczenia pracownika”,
 - 2) jedynie do zasobów niezbędnych do świadczenia pracy.
5. Dostęp do SILP dla użytkowników z podmiotów zewnętrznych może być przydzielony jedynie w przypadku, gdy z podmiotem została podpisana umowa wymagająca takiego dostępu.
6. Dostęp do zasobów i danych SILP jednostki organizacyjnej LP posiadają jej pracownicy, zgodnie z uprawnieniami zatwierdzonymi przez kierownika tej jednostki.
7. Zabronione jest wykorzystywanie dostępu do przydzielonych zasobów SILP w celach sprzecznych z obowiązującymi przepisami prawa lub regulacjami wewnętrznymi LP.
8. Zabronione jest umożliwianie osobom nieuprawnionym dostępu do SILP.
9. Zabronione jest ujawnianie osobom nieuprawnionym: danych SILP stanowiących tajemnice przedsiębiorstwa, danych uwierzytelniania w SILP, zasad działania i funkcjonowania SILP.
10. Zabronione jest podejmowanie prób przełamywania zabezpieczeń systemów teleinformatycznych, z wykluczeniem skanów podatności oraz testów penetracyjnych systemów SILP wykonywanych przez pracowników Komórki ds. Cyberbezpieczeństwa w Wydziale Informatyki DGLP.

11. Informacje, dokumenty, korespondencja i pozostałe dane przetwarzane w SILP są własnością Lasów Państwowych. Przełożeni mają prawo zażądać udostępnienia ich treści. Dane te należy chronić przed utratą i nieuprawnionym dostępem oraz regularnie przeprowadzać ich archiwizację. Ochroną przed nieuprawnionym dostępem należy objąć również wydruki z SILP.
12. Dane SILP stanowiące tajemnicę przedsiębiorstwa i inne dane, które mogą mieć wpływ na działanie i bezpieczeństwo PGL LP oraz urządzenia do ich przetwarzania, podlegają szczególnej ochronie. Użytkownik SILP jest zobowiązany do ochrony danych i urządzeń przed:
 - 1) zniszczeniem i uszkodzeniami mechanicznymi;
 - 2) kradzieżą;
 - 3) wpływami oddziaływań elektrostatycznych, elektromagnetycznych i elektrycznych;
 - 4) dostępem osób nieuprawnionych.
13. Dane SILP stanowiące tajemnicę przedsiębiorstwa i inne dane, które mogą mieć wpływ na działanie i bezpieczeństwo PGL LP, zapisane na nośnikach elektronicznych wynoszonych poza siedzibę jednostki LP, muszą być zaszyfrowane.
14. Dane SILP stanowiące tajemnicę przedsiębiorstwa i inne dane, które mogą mieć wpływ na działanie i bezpieczeństwo PGL LP, mogą być przechowywane i przetwarzane w publicznej chmurze obliczeniowej jedynie w przypadku spełnienia wymagań określonych w dokumencie „Polityka bezpieczeństwa przetwarzania danych LP w publicznej chmurze obliczeniowej” zatwierdzanym przez naczelnika WI DGLP.
15. Sprzęt elektroniczny przekazywany do serwisu musi być pozbawiony danych SILP poprzez trwałe ich usunięcie lub usunięcie nośników. W przypadku braku możliwości usunięcia danych lub nośników dopuszcza się przekazanie sprzętu do serwisu z danymi, które są zaszyfrowane.
16. W przypadku likwidacji nośników lub sprzętu z nośnikami zawierającymi dane SILP, należy trwale usunąć dane w sposób uniemożliwiający ich odtworzenie.
17. Wszystkie urządzenia służące do przetwarzania, przechowywania i przesyłania danych SILP muszą mieć instalowane na bieżąco, udostępniane przez producentów, aktualizacje krytyczne i aktualizacje bezpieczeństwa:
 - 1) oprogramowania sprzętowego;
 - 2) sterowników urządzeń w systemach operacyjnych;
 - 3) systemów operacyjnych;
 - 4) aplikacji.

18. Zabronione jest korzystanie z urządzeń i oprogramowania, które utraciły wsparcie producenta i nie otrzymują aktualizacji krytycznych i aktualizacji bezpieczeństwa.
19. Dopuszcza się czasowe odstąpienie od aktualizacji, w szczególnych przypadkach, w których aktualizacje powodują brak możliwości użytkowania oprogramowania stosowanego w LP.
20. Sieć komputerowa w jednostkach organizacyjnych LP opiera się o model zgodny z „Projektem usług katalogowych PGL LP” zatwierdzonym przez naczelnika WI DGLP.
21. Za utrzymanie, konserwację i prawidłowe działanie systemów informatycznych odpowiadają administratorzy SILP.
22. Wszelkie prace związane z utrzymaniem i konserwacją SILP prowadzone są przez administratorów SILP lub za ich wiedzą i zgodą.

§ 2

Bezpieczeństwo serwerów i systemów sieciowych SILP

1. Podstawową metodą uwierzytelniania użytkowników i administratorów w systemach wewnętrznych zasobów SILP jest uwierzytelnianie przy pomocy certyfikatu korporacyjnego PKI LP zapisanego na dedykowanym urządzeniu kryptograficznym. Szczegółowe zasady korzystania z urządzeń kryptograficznych zostały określone w § 14.
2. Wewnętrzne zasoby SILP mogą uwierzytelniać użytkowników SILP przy pomocy mechanizmów jednokrotnego logowania (ang. Single Sign-On) zintegrowanych z systemem usług katalogowych AD.
3. Jeżeli powyższe sposoby uwierzytelniania nie są możliwe, dopuszcza się uwierzytelnianie w oparciu o system usług katalogowych AD.
4. Dopuszcza się zakładanie lokalnych kont uprzywilejowanych i uwierzytelnianie za ich pomocą administratorów SILP w krytycznych, ze względu na działanie SILP, elementach infrastruktury.
5. Dopuszcza się zakładanie lokalnych kont uprzywilejowanych i uwierzytelnianie za ich pomocą administratorów SILP w systemach stanowiących SZBI.
6. Dopuszcza się zakładanie lokalnych kont w systemach SILP w przypadku konieczności autoryzacji usług, w szczególności kopii bezpieczeństwa, skanowania i druku. Konta te nie mogą być używane do logowania użytkowników lub administratorów SILP.

7. Użycie innych zasad uwierzytelniania wymaga zatwierdzenia przez naczelnika WI DGLP na wniosek WI.
8. Hasła kont lokalnych w systemach SILP podlegają zasadom tworzenia haseł określonym w „Projekcie usług katalogowych PGL LP”. W przypadkach, w których techniczne ograniczenia systemu uniemożliwiają zastosowanie zdefiniowanych w projekcie zasad, hasła należy tworzyć zgodnie z wymaganiami:
 - 1) hasło nie może zawierać identyfikatorów (loginów);
 - 2) hasło nie może zawierać imienia, nazwiska lub innych nazw własnych;
 - 3) hasło nie może zawierać informacji takich jak daty, numery pesel, numery telefonu;
 - 4) hasło nie może się składać z samych cyfr lub samych liter;
 - 5) w przypadku gdy system umożliwia użycie znaków specjalnych w haśle, hasło powinno zawierać znaki specjalne;
 - 6) hasło powinno mieć długość co najmniej 10 znaków. W przypadku gdy, z powodu ograniczeń systemu, nie można stworzyć hasła o żądanej długości, hasło powinno mieć największą możliwą długość;
 - 7) hasło nie może zawierać ciągów (co najmniej 3 znaki) tworzonych z kolejnych cyfr, liter alfabetu, klawiszy klawiatury.
9. Dostęp administracyjny do systemów SILP za pośrednictwem sieci należy realizować z użyciem połączeń szyfrowanych zapewniających poufność i integralność przesyłanych danych. W sytuacjach awaryjnych dopuszcza się nieszyfrowany dostęp do zdalnych urządzeń lub systemów sieciowych w celu usunięcia awarii. Po usunięciu awarii należy zmienić użyte hasła za pośrednictwem połączenia szyfrowanego.
10. Zabroniony jest dostęp administracyjny do systemów SILP w celach innych niż prace związane z administracją, utrzymaniem lub diagnostyką działania systemów SILP.
11. Użytkownicy SILP posiadają jedynie konta z uprawnieniami ograniczonymi wyłącznie do zakresu niezbędnego wykonywania obowiązków służbowych.
12. Konta o rozszerzonych uprawnieniach administracyjnych posiadają jedynie administratorzy SILP oraz członkowie stałych zespołów zadaniowych, w których zakresie są czynności administracyjne SILP. Z kont administracyjnych tylko w celu wykonywania czynności administracyjnych.
13. Proces uwierzytelniania użytkowników w systemach SILP za pośrednictwem sieci należy realizować z użyciem połączeń szyfrowanych zapewniających poufność i integralność przesyłanych danych.
14. W przypadku realizacji dostępu do produkcyjnych systemów SILP za pomocą protokołów szyfrowanych SSL/TLS/IPsec uwierzytelnienie serwera odbywa się przy

użyciu certyfikatów wystawionych i potwierdzonych przez PKI LP lub za pomocą certyfikatów kwalifikowanych.

15. Systemy serwerowe SILP muszą posiadać włączoną i aktualną ochronę przed złośliwym oprogramowaniem:

- 1) oprogramowanie ochronne musi posiadać aktualną bazę sygnatur zagrożeń aktualizowaną co najmniej raz na dobę, w sposób automatyczny;
- 2) oprogramowanie ochronne musi pracować w trybie skanowania plików w czasie rzeczywistym;
- 3) przynajmniej raz na miesiąc musi być wykonywane pełne skanowanie systemu w sposób automatyczny.

16. Dopuszcza się brak uruchomionej ochrony przed złośliwym oprogramowaniem w przypadku, gdy oprogramowanie ochrony:

- 1) powoduje brak możliwości użytkownika oprogramowania stosowanego w LP;
- 2) producenta oprogramowania stosowanego w LP zaleca wyłączenie takiej ochrony;
- 3) system serwerowy SILP nie ma możliwości uruchomienia oprogramowania ochrony.

17. Aktualizacje systemów serwerowych SILP pracujących z systemami MS Windows muszą być wykonywane za pośrednictwem serwera MS Windows Server Update Services umieszczonego w wewnętrznych zasobach SILP w sieci WAN LP. W przypadku instalacji aktualizacji wymagającej restartu systemu, administrator SILP niezwłocznie wykona restart.

18. Zabronione jest podłączanie do sieci LAN PC interfejsów zarządzających serwerów, systemów i urządzeń sieciowych SILP.

19. Serwery, systemy i urządzenia sieciowe muszą być zabezpieczone przed:

- 1) uszkodzeniami mechanicznymi;
- 2) kradzieżą;
- 3) pożarem;
- 4) zanikiem zasilania;
- 5) wpływami oddziaływań elektrostatycznych, elektromagnetycznych i elektrycznych;
- 6) innymi negatywnymi czynnikami środowiskowymi;
- 7) dostępem osób niepowołanych.

20. Systemy SILP muszą rejestrować i przechowywać przez co najmniej 6 miesięcy lub przekazywać do zewnętrznego dziennika zdarzeń, który przechowuje dane w analogicznym okresie:

- 1) informacje o wszystkich próbach dostępu użytkowników SILP;
- 2) informacje o wszystkich próbach dostępu administratorów SILP;
- 3) informacje o błędach w działaniu systemów i usług;

- 4) informacje o wszystkich próbach dostępu do udziałów i usług sieciowych.
21. Systemy SILP mogą mieć uruchomione jedynie usługi i oprogramowanie zgodne z przeznaczeniem systemów.
22. Instalowanie oraz usuwanie oprogramowania mogą wykonywać jedynie uprawniony administrator SILP lub firma zewnętrzna świadcząca serwis.
23. Instalacja i używanie oprogramowania w systemach SILP są dopuszczone wyłącznie po spełnieniu wymagań:
 - 1) posiadanie wymaganej przez producenta lub autora oprogramowania licencji;
 - 2) pochodzenie oprogramowania z autoryzowanych źródeł:
 - a) zewnętrznych repozytoriów sieciowych autoryzowanych przez producenta i uwierzytelnionych przy użyciu certyfikatów kwalifikowanych;
 - b) oryginalnych nośników producenta;
 - c) wewnętrznych repozytoriów sieciowych SILP uwierzytelnionych przy użyciu certyfikatów wystawionych i potwierdzonych przez PKI LP;
 - 3) brak negatywnego wpływu na stabilność pracy i bezpieczeństwo SILP.

§ 3

Bezpieczeństwo stacji roboczych

1. Zasady ogólne:
 - 1) podstawowym systemem uwierzytelniania użytkowników i administratorów na stacjach roboczych SILP jest uwierzytelnianie certyfikatem korporacyjnym PKI LP zapisanym na dedykowanym urządzeniu kryptograficznym. Szczegółowe zasady korzystania z urządzeń kryptograficznych zostały określone w § 14. Jeżeli powyższy sposób uwierzytelniania nie jest możliwy, dopuszcza się uwierzytelnianie w oparciu o system usług katalogowych AD;
 - 2) dopuszcza się uwierzytelnienie w oparciu o lokalne konto administratora SILP w systemie stacji roboczej. Konto może być użyte jedynie w sytuacjach awaryjnych, gdy inne metody uwierzytelnienia nie są możliwe;
 - 3) użycie innych zasad uwierzytelniania na stacjach roboczych SILP wymaga zatwierdzenia przez naczelnika WI DGLP na wniosek WI;
 - 4) zabronione jest użycie tego samego hasła do więcej niż jednego konta;
 - 5) zabrania się używania w Internecie haseł identycznych z używanymi w SILP;
 - 6) każdy z użytkowników jest odpowiedzialny za operacje w systemach informatycznych wykonane z użyciem jego identyfikatora;
 - 7) odchodząc od stacji roboczej użytkownik musi ją zablokować lub wylogować się;
 - 8) przeglądarki internetowe muszą mieć wyłączoną opcję zapamiętywania identyfikatorów i haseł;
 - 9) PIN do kart kryptograficznych musi zawierać minimum 6 znaków.

2. Podstawowym systemem operacyjnym stacji roboczej użytkownika SILP jest system MS Windows. Wykorzystanie innego systemu stacji roboczej do pracy użytkownika SILP wymaga udokumentowanej zgody WI DGLP, z wyłączeniem stanowiska leśniczego dla którego określone zostały odrębne zasady.
3. Aktualizacje stacji roboczych pracujących z systemami MS Windows muszą być wykonywane za pośrednictwem serwera MS Windows Server Update Services umieszczonego w wewnętrznych zasobach SILP. W przypadku instalacji aktualizacji wymagającej restartu systemu, administrator lub użytkownik SILP niezwłocznie wykona restart.
4. Ochrona przed złośliwym oprogramowaniem stacji roboczych:
 - 1) każda stacja robocza musi posiadać aktywną ochronę przez dedykowane oprogramowanie połączone do konsoli administracyjnej, zapewniającej monitoring stanu stacji oraz spójność polityk bezpieczeństwa;
 - 2) oprogramowanie ochrony stacji musi pracować w trybie ciągłym zapewniając ochronę w czasie rzeczywistym;
 - 3) użytkownik SILP nie może posiadać uprawnień do wyłączenia i deinstalacji programu ochrony stacji;
 - 4) program ochrony stacji może wyłączyć lub dokonać jego deinstalacji jedynie administrator SILP, na czas przeprowadzania czynności administracyjnych, wymagających takiego postępowania.
5. Instalacja oprogramowania:
 - 1) instalowanie i usuwanie oprogramowania może wykonywać jedynie administrator SILP lub firma zewnętrzna świadcząca serwis techniczny;
 - 2) instalacja i używanie oprogramowania są dopuszczone wyłącznie po spełnieniu wymagań:
 - a) posiadanie wymaganej przez producenta lub autora oprogramowania licencji;
 - b) pochodzenie oprogramowania z autoryzowanych źródeł:
 - (1) zewnętrznych repozytoriów sieciowych autoryzowanych przez producenta i uwierzytelnionych przy użyciu certyfikatów kwalifikowanych;
 - (2) oryginalnych nośników producenta;
 - (3) wewnętrznych repozytoriów sieciowych SILP uwierzytelnionych przy użyciu certyfikatów wystawionych i potwierdzonych przez PKI LP;
 - c) brak negatywnego wpływu na stabilność pracy i bezpieczeństwo SILP.
 - 3) administrator SILP zobowiązany jest do nadzorowania zgodności instalowanego oprogramowania z posiadanymi licencjami;
 - 4) zakupy oprogramowania muszą być dokonywane za wiedzą administratora SILP danej jednostki.
6. Stanowisko leśniczego:
 - 1) podstawowym systemem pracy na stanowisku leśniczego jest system KNX udostępniany przez WI DGLP. Używanie innego systemu do pracy na stanowisku

leśniczego wymaga zgody dyrektora właściwej regionalnej dyrekcji Lasów Państwowych.

- 2) podstawowym sposobem łączności ze stanowiska leśniczego do sieci WAN LP są połączenia SSL VPN realizowane za pośrednictwem wskazanego przez WI DGLP serwisu dostępowego w domenie lasy.gov.pl.

§ 4

Usługa katalogowa Active Directory

1. W sieci WAN LP funkcjonuje usługa katalogowa Active Directory (AD).
2. Usługa katalogowa AD jest podstawowym katalogiem użytkowników, administratorów SILP oraz stacji roboczych z systemem MS Windows.
3. Struktura usługi katalogowej AD odwzorowuje strukturę organizacji i podległości jednostek LP.
4. Struktura logiczna katalogu Active Directory zawiera pojedynczą domenę Active Directory. Jako nazwa przestrzeni Active Directory przyjęta jest domena ad.lasy.gov.pl.
5. Każdy użytkownik SILP musi być zarejestrowany w usłudze katalogowej AD.
6. Usługa katalogowa AD wymusza używanie indywidualnych identyfikatorów użytkowników i administratorów SILP umożliwiając ich jednoznaczną identyfikację.
7. Usługa katalogowa AD umożliwia użytkownikom i administratorom SILP samodzielną zmianę ich haseł.
8. Usługa katalogowa AD wymusza użycie haseł odpowiedniej jakości oraz okresową wymianę haseł przez użytkowników i administratorów SILP.
9. Szczegółowe zasady funkcjonowania usługi katalogowej AD określa osobny dokument „Projekt usług katalogowych PGL LP” zatwierdzany przez naczelnika WI DGLP.

§ 5

Kopie bezpieczeństwa

1. Kopie zapasowe danych ze stacji roboczych:
 - 1) za kopie danych ze stacji roboczych odpowiedzialni są użytkownicy stacji roboczych;
 - 2) w przypadku uruchomienia serwera kopii bezpieczeństwa w danej jednostce LP odpowiedzialność za tworzenie i przechowywanie kopii regulują wytyczne właściwych WI.

2. Kopie zapasowe danych systemów sieciowych i serwerowych SILP:
 - 1) wszystkie produkcyjne systemy sieciowe i serwerowe SILP objęte są wymogiem tworzenia ich kopii zapasowych;
 - 2) osobą odpowiedzialną za tworzenie kopii i utrzymanie spisu wykonanych kopii systemów oraz utworzenie i aktualizowanie procedury odtworzenia systemu przy użyciu kopii zapasowej jest:
 - a) administrator SILP odpowiedzialny za dany system – w przypadku, gdy system nie jest objęty zewnętrznym oprogramowaniem odpowiedzialnym za jego kopię,
 - b) administrator SILP zewnętrznego systemu kopii - w przypadku, gdy system jest objęty zewnętrznym oprogramowaniem odpowiedzialnym za jego kopię;
 - 3) za testowe odtworzenie z kopii zapasowej i weryfikację poprawności działania po odtworzeniu systemu SILP odpowiedzialny jest jego administrator.
3. Kopie bezpieczeństwa systemu LAS:
 - 1) administrator SILP odpowiedzialny za System LAS tworzy kopie i utrzymuje rejestr kopii bezpieczeństwa;
 - 2) administrator SILP odpowiedzialny za System LAS tworzy i aktualizuje procedurę odtworzenia systemu z kopii bezpieczeństwa.
4. Szczegółowe zasady wykonywania kopii bezpieczeństwa określa osobny dokument „Polityka kopii zapasowych SILP” zatwierdzany przez naczelnika WI DGLP.

§ 6

Praca w sieci Lasów Państwowych

1. Zasady ogólne:
 - 1) stacje robocze podłączone do sieci LP nie mogą mieć włączonych innych połączeń transmisji danych;
 - 2) dopuszcza się dostęp zdalny do wewnętrznych zasobów SILP za pośrednictwem wbudowanych mechanizmów VPN centralnego systemu EMM w PGL LP.
 - 3) dopuszcza się dostęp zdalny VPN z sieci Internet do wewnętrznych zasobów SILP. Warunki i sposób dostępu zostały określone w § 9;
 - 4) zabrania się fizycznego podłączenia do sieci LP komputerów nie będących własnością Lasów Państwowych, bez zgody właściwych WI;
 - 5) w przypadku wykrycia lub pojawienia się znanej podatności powodującej zagrożenie bezpieczeństwa danych stacji roboczej, serwera lub systemu sieciowego z wykorzystaniem sieci teleinformatycznej, ZCI może zablokować cały ruch kierowany do/z danego systemu;
 - 6) w przypadku pojawienia się w sieci LP ruchu zaburzającego prawidłowe działanie SILP lub świadczącego o infekcji stacji roboczej, serwera lub systemu sieciowego SILP, ZCI może zablokować cały ruch do/z danego źródła.

2. Adresacja urządzeń w sieci LP:

- 1) zasady adresacji wszystkich urządzeń w sieci LP ustala i reguluje osobny dokument „Zasady adresacji IP w sieci LP”, tworzony oraz aktualizowany przez ZCI i zatwierdzany przez naczelnika WI DGLP;
- 2) w każdej sieci LAN PC musi być dostępny serwer DHCP przyznający adresacje dla stacji roboczych;
- 3) w sieci WAN LP zabronione jest używanie translacji i maskowania adresów IP, w szczególności NAT, PAT, Proxy;
- 4) ZCI prowadzi rejestr adresów i sieci IP używanych w WAN LP oraz publicznych adresów IP używanych przez LP w sieci Internet.

3. Dozwolony ruch w sieci WAN LP:

- 1) ruch wewnątrz sieci WAN LP podlega ograniczeniom w celu ochrony zasobów SILP przed nieuprawnionym dostępem;
- 2) polityki dla ruchu dozwolonego wewnątrz sieci WAN LP ustala i reguluje osobny dokument „Polityka dla ruchu w sieci WAN LP”, tworzony oraz aktualizowany przez ZCI i zatwierdzany przez naczelnika WI DGLP;
- 3) zmiany polityk dla ruchu w sieci WAN LP wprowadzane są przez WI DGLP na wniosek od właściwych WI;
- 4) polityki dla ruchu w sieci WAN LP realizowane są na znajdujących się w jednostkach urządzeniach będących własnością LP. Za implementację polityk na urządzeniach w sieci WAN LP odpowiada WI DGLP.

4. Sieci bezprzewodowe Wi-Fi:

- 1) sieci LAN jednostek LP mogą być budowane w oparciu o bezprzewodowe sieci komputerowe Wi-Fi;
- 2) szczegółowy opis tworzenia sieci LAN jednostek LP w oparciu o bezprzewodowe sieci komputerowe określa osobny dokument „Zasady budowy lokalnych sieci bezprzewodowych w jednostkach PGL LP”, tworzony oraz aktualizowany przez ZCI i zatwierdzany przez naczelnika WI DGLP;
- 3) sieci bezprzewodowe muszą używać szyfrowania zgodnego z wymaganiami określonymi w dokumencie „Zasady budowy lokalnych sieci bezprzewodowych w jednostkach PGL LP”;
- 4) za pośrednictwem sieci bezprzewodowych można realizować dostęp użytkowników SILP do sieci LP przy spełnieniu wymagań:
 - a) uwierzytelnianie dostępu zostanie wykonane w oparciu o certyfikat wystawiony przez PKI LP;
 - b) do uwierzytelniania dostępu wykorzystany jest standard IEEE 802.1X;
 - c) po uwierzytelnieniu użytkownik SILP otrzyma za pośrednictwem DHCP adresację sieci LAN jednostki i dostęp do sieci LP identyczny, jak stacje z dostępem przewodowym;
- 5) za pośrednictwem sieci bezprzewodowych można realizować dostęp gościnny do Internetu z urządzeń nie będących własnością LP, przy spełnieniu wymagań:

- a) uwierzytelnianie dostępu odbywa się za pośrednictwem portalu dla dostępu gościnnego i musi zapewniać jednoznaczne powiązanie urządzenia z tożsamością gościa lub jego numerem telefonu;
- b) dostęp będzie możliwy jedynie po akceptacji przez gościa regulaminu określającego zasady dostępu;
- c) ruch z sieci dostępu gościnnego musi być izolowany w sieci WAN LP i przesyłany tunelem pomiędzy brzegowym urządzeniem sieciowym jednostki LP a urządzeniem terminującym w centralnym węźle sieciowym.

§ 7

Zasady funkcjonowania i użytkowania systemu poczty elektronicznej

1. System poczty elektronicznej LP obsługuje skrzynki poczty elektronicznej w domenach i subdomenach będących własnością Lasów Państwowych.
2. Konta pocztowe w domenie lasy.gov.pl i jej subdomenach mogą posiadać:
 - 1) pracownicy jednostek organizacyjnych Lasów Państwowych;
 - 2) pozostali użytkownicy SILP.
3. Każdy uprawniony do posiadania konta pocztowego posiada tylko jedno imienne konto pocztowe w systemie poczty elektronicznej LP, we właściwej domenie, zgodnie z „Projektem usług katalogowych PGL LP”.
4. Zabronione jest udostępnianie przez użytkowników konta pocztowego lub danych dostępowych do konta pocztowego osobom nieupoważnionym.
5. W systemie poczty Lasów Państwowych funkcjonują tylko imienne konta pocztowe oraz nieimienne konta specjalne tworzone za zgodą naczelnika WI DGLP.
6. Użytkownicy poczty elektronicznej LP posiadający dedykowane urządzenie kryptograficzne muszą posiadać certyfikaty wydane przez PKI LP umożliwiające podpisywanie, szyfrowanie, deszyfrowanie, jednoznaczne potwierdzenie autentyczności wysyłanej oraz odbieranej poczty.
7. Informacja o służbowym adresie e-mail jest jawna i jest powszechnie dostępna, w tym na łamach witryny internetowej BIP Lasów Państwowych. Dotyczy to również adresów e-mail nadanych dla jednostek organizacyjnych Lasów Państwowych.
8. Użytkownicy kont pocztowych zawartych w domenie LP muszą przestrzegać „Regulaminu użytkowania systemu poczty elektronicznej LP”.
9. Aktualny „Regulamin użytkowania systemu poczty elektronicznej LP” publikowany jest pod adresem <https://mail.lasy.gov.pl/regulamin>.

10. Regulamin zatwierdza naczelnik WI DGLP. Wszelkie zmiany Regulaminu zaczynają obowiązywać z momentem ich opublikowania. Użytkownicy są informowani o zmianach Regulaminu poprzez wiadomość poczty elektronicznej.
11. W przypadku naruszenia przez użytkownika „Regulaminu użytkowania systemu poczty elektronicznej LP”, administrator SILP systemu poczty elektronicznej LP ma prawo natychmiastowego zablokowania konta pocztowego.

§ 8

Praca w sieci Internet i styk z Internetem

1. Dostęp do sieci Internet z sieci WAN LP realizowany jest jedynie za pośrednictwem węzłów centralnych w Centrum Podstawowym i Centrum Zapasowym. Zabrania się łączenia sieci LAN jednostek organizacyjnych LP z zewnętrznymi sieciami komputerowymi, inaczej niż za pośrednictwem węzłów centralnych.
2. Ruch na styku sieci WAN LP i Internet podlega ograniczeniom. Polityki dla ruchu na styku sieci WAN LP i Internet ustala i reguluje osobny dokument „Polityka dla ruchu na styku sieci WAN LP i Internet”, tworzony oraz aktualizowany przez ZCI i zatwierdzany przez naczelnika WI DGLP.
3. Na styku sieci WAN LP i Internet ruch szyfrowany może podlegać inspekcji. Użytkownik SILP może za pośrednictwem właściwych WI wnioskować o wykluczenie adresów podlegających inspekcji ruchu szyfrowanego. Szczegółowe zasady działania inspekcji opisuje dokument „Zasady inspekcji ruchu szyfrowanego” zatwierdzany przez naczelnika WI DGLP.
4. Zabronione jest używanie oprogramowania służącego do anonimizacji ruchu sieciowego, w szczególności wykorzystującego technologie Proxy, TOR lub zewnętrzne usługi VPN.
5. Polityki dla ruchu na styku sieci WAN LP i Internet realizowane są na centralnych systemach zabezpieczeń sieciowych będących własnością PGL LP.
3. Zabronione jest wykorzystanie usług umożliwiających zdalny dostęp z sieci Internet do wewnętrznych zasobów SILP z wyjątkiem:
 - 1) sesji serwisowych dla firm zewnętrznych nadzorowanych przez pracowników służb informatycznych, po uprzednim uzyskaniu zgody WI;
 - 2) dostępu za pomocą dedykowanych systemów VPN LP autoryzowanych przez WI DGLP.

§ 9 Dostęp zdalny VPN do zasobów SILP

1. Dostęp zdalny VPN do SILP jest przyznawany pracownikom Lasów Państwowych wyłącznie na czas pozostawania w stosunku zatrudnienia.
2. Każdy pracownik LP ma prawo posiadać dostęp zdalny VPN do SILP, z uprawnieniami jakie posiada w sieci LAN PC własnej jednostki organizacyjnej, po otrzymaniu pisemnej zgody kierownika swojej jednostki i przekazaniu stosownego wniosku do WI odpowiedzialnych za utworzenie dostępu z zachowaniem drogi służbowej.
3. Dostęp zdalny VPN do SILP dla pracowników Lasów Państwowych jest dozwolony jedynie z urzędzeń będących własnością Lasów Państwowych.
4. Dostęp zdalny VPN do SILP dla osób fizycznych wykonujących prace na podstawie umowy o dzieło, umowy zlecenia lub innej umowy cywilnoprawnej jest przyznawany jedynie do zasobów niezbędnych do wykonania prac określonych w umowie. Dostęp ten jest przyznawany jedynie na czas wykonywania prac określonych w umowie.
5. Dostęp zdalny VPN do SILP dla pracowników podmiotów zewnętrznych do zasobów SILP może być przydzielony jedynie w przypadku, gdy została podpisana umowa wymagająca takiego dostępu, przy spełnieniu następujących warunków:
 - 1) dostęp może być przydzielony jedynie na czas obowiązywania umowy;
 - 2) dostęp może być przydzielony wyłącznie do zasobów niezbędnych do wykonania prac określonych w umowie;
 - 3) podmiot zewnętrzny podpisze oświadczenie o zasadach udzielenia dostępu i zachowania poufności.
6. Dostęp zdalny VPN do SILP jest realizowany przy spełnieniu następujących warunków:
 - 1) uwierzytelnianie i autoryzacja następują w oparciu o certyfikat wystawiony przez PKI LP lub imienne konta AD założone zgodnie z „Projektem usług katalogowych PGL LP”;
 - 2) dostęp zapewnia poufność i integralność przesyłanych danych oraz wzajemne uwierzytelnienie obu stron połączenia;
 - 3) tunel VPN jest terminowany na centralnym koncentratorze VPN.
7. W przypadku konieczności utrzymania stałego dostępu przez firmy lub instytucje zewnętrzne do zasobów SILP, może zostać przydzielony zdalny dostęp VPN nieimienny typu site-to-site. Dostęp zostanie przydzielony na zatwierdzony przez naczelnika WI DGLP wniosek od WI. Szczegóły techniczne takiego połączenia ustala i realizuje ZCI. Dostęp może być przydzielony jedynie w przypadku, gdy z firmą zewnętrzną została podpisana umowa wymagająca takiego dostępu, przy spełnieniu następujących warunków:

- 1) dostęp będzie możliwy jedynie na czas obowiązywania umowy;
 - 2) firma zewnętrzna podpisze oświadczenie o zasadach udzielenia dostępu i zachowaniu poufności.
8. Stały dostęp zdalny VPN typu site-to-site może zostać wykonany za pośrednictwem sieci Internet w jednostkach LP nie posiadających łącza do sieci WAN LP. Podłączenie zostaje wykonane na wniosek kierownika jednostki do naczelnika WI DGLP. Wniosek musi być potwierdzony przez nadrzędny dla jednostki WI. Dostęp realizowany jest przy spełnieniu następujących warunków:
- 1) dostęp zdalny VPN typu site-to-site dla jednostek LP musi zapewniać poufność i integralność przesyłanych danych oraz wzajemne uwierzytelnienie obu stron połączenia;
 - 2) tunel VPN po stronie lokalizacji zdalnej LP terminowany jest na dedykowanym urządzeniu szyfrującym, po stronie sieci LP tunel terminowany jest w Centrum Podstawowym przetwarzania danych w DGLP;
 - 3) warunkiem do podłączenia jednostki zdalnej, jest instalacja w lokalizacji łącza internetowego ze stałą, publiczną adresacją IP, przy czym co najmniej jeden publiczny adres IP musi być dostępny do adresacji interfejsu urządzenia terminującego tunel VPN. Sieć LAN tak podłączonej lokalizacji zdalnej, powinna posiadać adresację przydzieloną przez ZCI;
 - 4) cały ruch z sieci lokalnej podłączonej lokalizacji zdalnej kierowany jest do tunelu VPN;
 - 5) polityki dostępu z sieci lokalizacji zdalnej do sieci WAN LP i do sieci Internet implementowane i realizowane są na centralnym koncentratorze VPN;
 - 6) szczegółowe parametry i konfiguracje tunelu dostępu zdalnego VPN ustala i wykonuje ZCI;
 - 7) w przypadku wykorzystywania tunelu VPN w lokalizacji zdalnej zarówno na potrzeby pracowników biurowych LP i sal szkoleniowych, wymagana jest separacja sieci LAN biura i sal szkoleniowych za pomocą osobnego przełącznika lub przy użyciu przełącznika zarządzanego i osobnych sieci VLAN;
 - 8) sieci LAN części biurowej i sal szkoleniowych powinny posiadać niezależne adresacje IP przydzielone przez ZCI;
 - 9) dopuszczone jest wykorzystanie zainstalowanego na potrzeby VPN łącza internetowego, również jako łącze dostępowe do sieci Internet dla części hotelowej w lokalizacji. W takim wypadku ruch z części hotelowej do sieci Internet nie jest kierowany przez tunel VPN i wychodzi bezpośrednio do Internetu. Takie podłączenie do łącza części hotelowej ośrodków może zostać wykonane pod warunkami:
 - a) separacji sieci LAN dla części hotelowej za pomocą osobnego przełącznika lub przy użyciu przełącznika zarządzanego i osobnego VLAN,
 - b) posiadania na łączu dodatkowego stałego publicznego adresu IP, innego niż używany do terminowania tunelu VPN, na który będą translowane połączenia wychodzące do sieci Internet;

10)w przypadku wynajmu sal na szkolenia inne niż wewnętrzne szkolenia LP, wymagane jest przełączenie sieci sali szkoleniowej do LAN lub VLAN części hotelowej lub sieci bezprzewodowej dla dostępu gościnnego.

§ 10

Dostęp do wewnętrznych zasobów SILP z sieci LAN dla podmiotów zewnętrznych

1. Dostęp do wewnętrznych zasobów SILP dla pracowników podmiotów zewnętrznych może być przydzielony jedynie w przypadku, gdy została podpisana Umowa wymagająca takiego dostępu.
2. Dostęp może być przydzielony wyłącznie do zasobów niezbędnych do wykonania prac określonych w umowie.
3. Dostęp może być przydzielony wyłącznie na czas obowiązywania umowy.
4. Podmiot zewnętrzny jest zobowiązany do złożenia oświadczenie o zasadach udzielenia dostępu i zachowaniu poufności.
5. Uwierzytelnianie i autoryzacja dostępu następują w oparciu o certyfikat wystawiony przez PKI LP lub imienne konta AD założone zgodnie z „Projektem usług katalogowych PGL LP”.
6. W przypadku gdy, dostęp do wewnętrznych zasobów SILP dla pracowników podmiotów zewnętrznych dotyczy prowadzenia czynności wynikających z obowiązujących umów serwisowych, może być on realizowany jedynie za zgodą pracowników służb informatycznych, w trybie nadzorowanych sesji dostępowych. W takim przypadku, niniejszy ustęp ma charakter wyłączny, a pozostałe ustępy nie obowiązują.

§ 11

Internetowe i Intranetowe usługi SILP

1. W sieci LP funkcjonują obligatoryjnie następujące usługi:
 - 1) System Las;
 - 2) Usługa katalogowa AD – każdy użytkownik pracujący w sieci LP musi być zarejestrowany w usłudze katalogowej, jest to konieczne do uzyskania przez niego dostępu do usług i urządzeń zgodnie z posiadanymi uprawnieniami;
 - 3) PKI LP – infrastruktura klucza publicznego Lasów Państwowych utrzymywana w ramach wewnętrznych zasobów SILP;
 - 4) Poczta elektroniczna – każdy pracownik LP zarejestrowany w usłudze katalogowej musi posiadać imienne konto pocztowe;
 - 5) Portal pracowniczy;
 - 6) Portal leśno-drzewny;

- 7) Portal leśnik+;
 - 8) Elektroniczne Zarządzanie Dokumentacją - system elektronicznego obiegu dokumentów;
 - 9) Centralny system zarządzania urządzeniami mobilnymi klasy EMM;
 - 10) System Zgłaszania Błędów i Modyfikacji;
 - 11) Centralny system telefonii IP;
 - 12) Serwis dystrybucji poprawek i aktualizacji systemów firmy Microsoft.
2. Za prawidłowe funkcjonowanie serwerów usług internetowych i intranetowych LP odpowiedzialne są WI utrzymujące dany serwer oraz usługę.
 3. Zasady funkcjonowania i korzystania z usług internetowych i intranetowych LP regulują osobne dokumenty techniczne.

§ 12

Urządzenia mobilne

1. Urządzenia mobilne będące własnością jednostek LP podlegają następującym wymaganiom:
 - 1) urządzenie powinno pochodzić z autoryzowanego, na terenie Polski lub Unii Europejskiej, kanału dystrybucji;
 - 2) urządzenie powinno mieć zapewnione połączenie do Internetu realizowane przez transmisję danych komórkowych;
 - 3) instalacja aplikacji oraz aktualizacje mogą być przeprowadzane tylko z oficjalnych źródeł dystrybucji producenta systemu operacyjnego lub ze sklepu korporacyjnego LP;
 - 4) jeżeli system urządzenia posiada możliwość instalacji ochrony antywirusowej lub monitorującej i reagującej na zagrożenia, uruchomienie jej jest obowiązkowe dla urządzeń przetwarzających dane firmowe i/lub posiadające dostęp do zasobów firmowych, uruchomienie takiej ochrony jest rekomendowane dla pozostałych urządzeń;
 - 5) służbowe karty SIM zainstalowane w urządzeniu muszą być zabezpieczone kodem PIN;
 - 6) urządzenie musi mieć włączoną aktywną kontrolę dostępu;
 - 7) lokalizacja urządzenia może być prowadzona jedynie za wiedzą i zgodą użytkownika;
 - 8) szczegółowe wytyczne dotyczące konfiguracji urządzenia i oprogramowania są określone w dokumencie pn. „Polityka bezpieczeństwa dla urządzeń mobilnych w PGL LP” zatwierdzanym przez naczelnika WI DGLP.
2. Urządzenia mobilne będące własnością PGL LP, wykorzystywane do przechowywania i przetwarzania danych służbowych oraz łączenia się z zasobami LP, dodatkowo podlegają następującym wymaganiom:

- 1) urządzenie musi spełniać obowiązującą rekomendację określoną przez WI DGLP;
- 2) urządzenie musi pracować pod aktywną kontrolą centralnego systemu zarządzania urządzeniami mobilnymi w PGL LP;
- 3) dostęp z urządzenia do sieci WAN LP realizowany jest wyłącznie przez szyfrowane kanały VPN zestawiane przez centralny system zarządzania urządzeniami mobilnymi w PGL LP;
- 4) przestrzeń pamięci urządzenia i kart przechowujących dane SILP, stanowiące tajemnice przedsiębiorstwa, muszą być zaszyfrowane;
- 5) potencjalnie niebezpieczne aplikacje lub bezpodstawnie żądające zwiększonych uprawnień mogą zostać usunięte przez Administratora SILP;
- 6) w przypadku utraty urządzenia lub naruszenia polityki bezpieczeństwa informatycznego LP Administrator SILP może usunąć dostęp do zasobów korporacyjnych lub/i wszystkich danych z urządzenia;
- 7) szczegółowe wytyczne dotyczące konfiguracji urządzenia i oprogramowania oraz rekomendacje są określone w dokumencie pn. „Polityka bezpieczeństwa dla urządzeń mobilnych w PGL LP” zatwierdzanym przez Naczelnika WI DGLP.

§ 13

System telefonii IP w jednostkach LP

1. Telefony IP w sieci LP są obsługiwane przez centralny system zarządzający telefonią.
2. Telefony IP oraz terminale wideo w jednostkach organizacyjnych LP powinny znajdować się w wydzielonej sieci VLAN o ID 200.
3. Katalogi użytkowników systemów telefonii IP i wideokonferencji są synchronizowane z usługą katalogową Active Directory.
4. Nr telefonu IP użytkownika SILP wprowadzany jest w Active Directory zgodnie ze schematem opisu pól określonym w Projekcie usług katalogowych PGL LP.
5. Szczegółowe wytyczne dotyczące konfiguracji i planów numeracyjnych są określone w dokumencie „Projekt funkcjonowania systemu telefonii IP” zatwierdzanym przez Naczelnika WI DGLP

§ 14

Urządzenia uwierzytelnienia użytkowników LP

1. Użytkownicy SILP jednostek organizacyjnych Lasów Państwowych, z wyłączeniem użytkowników stanowiska leśniczego, muszą posiadać i wykorzystywać certyfikaty wystawione przez PKI LP służące do:

- 1) uwierzytelniania użytkownika - w szczególności do weryfikacji jego tożsamości w systemach SILP;
 - 2) elektronicznego podpisywania dokumentów - w celu zapewnienia integralności oraz niezaprzeczalności dokumentów;
 - 3) szyfrowania - w celu zapewnienia poufności i zabezpieczenia danych SILP przed nieuprawnionym dostępem.
2. Urządzenia kryptograficzne służące do przechowywania certyfikatów oraz ich szczegółowe parametry techniczne, zostały określone w dokumencie „Urządzenia uwierzytelniania użytkowników LP” zatwierdzanym przez naczelnika WI DGLP.
 3. Użytkownik SILP dysponujący urządzeniem przechowującym certyfikaty ma obowiązek zabezpieczyć je przed zgubieniem, zniszczeniem i użyciem przez osoby trzecie.
 4. W przypadku zgubienia, zniszczenia lub nieuprawnionego użycia urządzenia kryptograficznego, użytkownik jest zobowiązany niezwłocznie poinformować administratora SILP.
 5. Pracownicy korzystający z uwierzytelnienia przy pomocy systemów zbliżeniowych muszą korzystać z urządzeń zbliżeniowych o parametrach określonych w dokumencie „Urządzenia uwierzytelniania użytkowników LP” zatwierdzanym przez naczelnika WI DGLP.

Regulamin użytkowania systemu poczty elektronicznej LP

wprowadzony na podstawie Załącznika nr 2 do Zarządzenia nr 35 Dyrektora Generalnego Lasów Państwowych z dnia 18 maja 2026 r. w sprawie zasad funkcjonowania i zasad bezpieczeństwa systemu informatycznego w Państwowym Gospodarstwie Leśnym Lasy Państwowe.

Data	Autor	Wersja	Opis zmian
2017-12-29	OI.C	1.0	Pierwsza wersja dokumentu
2018-04-13	OI.C	1.1	Aktualizacja: zasady dostępu do systemu poczty z sieci Internet, zabronione przekierowanie poczty poza system poczty LP
2026-05-26	EI, ZILP	1.2	Ujednoczenie zapisów; dodanie obligatoryjnych adresów grup dystrybucyjnych

I. Zasady użytkowania systemu poczty elektronicznej LP

1. Za utrzymanie i prawidłowe funkcjonowanie systemu poczty LP odpowiada Zakład Informatyki Lasów Państwowych.
2. System poczty jest utrzymywany z wykorzystaniem infrastruktury własnej LP.
3. Założenie lub usunięcie konta w systemie poczty LP odbywa się na polecenie kierownika jednostki przez właściwego administratora domeny pocztowej.
4. Adres e-mail użytkownika poczty tworzony jest na podstawie nazwy logowania użytkownika w usługach katalogowych LP zgodnie z konwencją <imię>.<nazwisko>.
 - 4.1. Adres pocztowy użytkownika musi być unikalny w ramach domeny RDLP/Zakładu o zasięgu krajowym.
 - 4.2. Adres pocztowy nie może zawierać polskich znaków diakrytycznych.
5. Konto pocztowe tworzy się w ramach organizacji we właściwej domenie zgodnie z „Projektem Usług Katalogowych PGL LP”:
 - 5.1. nazwa_logowania_użytkownika@nazwa_RDLP.lasy.gov.pl, dla pracowników rdLP i jednostek podległych,
 - 5.2. nazwa_logowania_użytkownika@nazwa_zakładu.lasy.gov.pl, dla pracowników zakładów o zasięgu krajowym,
 - 5.3. nazwa_logowania_użytkownika@lasy.gov.pl, dla pracowników DGLP.
6. Każdy użytkownik systemu poczty LP może posiadać certyfikaty PKI LP umożliwiające podpisywanie i szyfrowanie wiadomości elektronicznych gwarantujące integralność i poufność przesyłanych danych.
7. Korespondencja poczty elektronicznej zawierająca dane SILP stanowiące tajemnice przedsiębiorstwa lub dane wrażliwe musi być zaszyfrowana. W przypadku braku możliwości zaszyfrowania korespondencji certyfikatem korporacyjnym, nadawca jest zobowiązany do zaszyfrowania informacji innymi dostępnymi metodami.
8. Użytkownik systemu poczty LP w celu potwierdzenia autentyczności i integralności korespondencji e-mail jest zobowiązany podpisywać wiadomości certyfikatem korporacyjnym.
9. W systemie poczty LP funkcjonują aliasy adresów kont poczty elektronicznej. Użytkownik może wnioskować do właściwego administratora domeny pocztowej o nadanie aliasu do swojej skrzynki pocztowej.
10. Grupy pocztowe tworzone są w oparciu o schematy organizacyjne jednostek LP z wykorzystaniem tabel nr 1, 2 i 3.
11. Wiadomości wysyłane w odpowiedzi na pocztę wysłaną do grupy pocztowej będą

Regulamin użytkownika systemu poczty elektronicznej LP

korzystać z imiennego adresu poczty elektronicznej konta osoby odpowiadającej.

12. Grupy pocztowe tworzą i zarządzają nimi właściwi administratorzy SILP domeny pocztowej. Administratorzy dodają i usuwają użytkowników z grup pocztowych na podstawie decyzji kierownika jednostki lub właściwego kierownika komórki organizacyjnej.
13. Na czas absencji w pracy trwającej ponad 1 dzień użytkownik SILP powinien włączyć automatyczne powiadomienia systemu poczty elektronicznej o nieobecności lub skorzystać z funkcji „Ustaw auto odpowiedź w mailu” w panelu „Absencje i delegacje” w SILPWeb.
14. Użytkownik przed rozpoczęciem korzystania z konta ma obowiązek zapoznania się z treścią Regulaminu użytkownika systemu poczty elektronicznej LP. Korzystanie z systemu pocztowego LP oznacza akceptację warunków regulaminu.
15. Użytkownik jest zobowiązany do wykorzystywania poczty elektronicznej wyłącznie do celów służbowych.
16. Użytkownik poczty LP ma obowiązek ochrony danych logowania oraz certyfikatu podpisywania i szyfrowania i nie może udostępniać ich osobom trzecim w żadnej formie.
17. Przed wysłaniem wiadomości użytkownik musi zweryfikować czy wpisane adresy e-mail odbiorców są poprawne oraz czy załączone są właściwe pliki.
18. W przypadku wysłania wiadomości zawierającej dane osobowe do nieuprawnionego odbiorcy, użytkownik jest zobowiązany niezwłocznie poinformować o tym fakcie właściwego Inspektora Ochrony Danych Osobowych.
19. Użytkownik powinien stosować podpis treści wiadomości zgodny ze wzorem określonym w dokumencie „Księga Identyfikacji Wizualnej LP”.
20. Pojemność konta systemu poczty LP wynosi 2 GB. W uzasadnionych przypadkach, użytkownik ma możliwość wnioskowania o podniesienie wielkości konta do maksymalnej pojemności 10 GB. Odpowiedni wniosek należy złożyć do właściwego administratora systemu pocztowego.
21. Wielkość pojedynczej wiadomości wraz z załącznikami podlega ograniczeniom i nie może przekroczyć 30MB.
22. Z konta systemu poczty LP można korzystać przy pomocy:
 - 22.1. Dedykowanego serwisu WWW utrzymywanego przez ZILP.
 - 22.2. Programów klientów pocztowych obsługujących protokoły SMTP, POP3, IMAP lub dedykowanych rozwiązań Microsoft MAPI/HTTP oraz EWS, przy spełnieniu wymagań:
 - 22.2.1. Obszar pamięci, w którym program pocztowy przechowuje lokalnie pliki poczty jest zaszyfrowany.

Regulamin użytkownika systemu poczty elektronicznej LP

- 22.2. 2. Połączenia do systemu poczty są szyfrowane. W przypadku braku możliwości takiej konfiguracji dopuszcza się połączenia nieszyfrowane, dla usług (np. skaner) pod warunkiem, że nie są w nich przesyłane dane SILP stanowiące tajemnice przedsiębiorstwa.
- 22.3. Programów klientów pocztowych dla urządzeń mobilnych za pośrednictwem wbudowanych mechanizmów VPN centralnego systemu EMM w PGL LP.
23. Dostęp dla użytkowników systemu poczty LP z sieci Internet jest możliwy jedynie za pośrednictwem bezpiecznego kanału VPN.
24. Użytkownicy SILP muszą używać połączeń szyfrowanych w komunikacji z systemem poczty LP.
25. Zabrania się wykonywania konfiguracji ustawień w celu automatycznego przekazywania lub przechowywania wiadomości poczty elektronicznej poza SILP.
26. Jeżeli użytkownik nie logował się do konta pocztowego przez 365 kolejnych dni, administrator SILP ma prawo do usunięcia skrzynki oraz wszystkich znajdujących się w niej wiadomości.
27. Stosowane w systemie poczty LP techniki zabezpieczenia kont i korespondencji służą zapewnieniu jak najwyższego poziomu bezpieczeństwa, jednak ze względów technicznych nie mogą gwarantować w pełni tajemnicy składowanych i przesyłanych informacji.
28. System poczty LP jest zabezpieczony przez system ochrony przed spamem, phishingiem, złośliwym oprogramowaniem.
- 28.1. Wiadomości e-mail przesłane przez nadawców spoza organizacji są oznaczone znacznikiem [EXTERNAL] dodawanym do tematu wiadomości.
- 28.2. Wiadomości oznaczone jako potencjalnie niebezpieczne lub spam mogą zostać automatycznie zablokowane przez system ochrony.
- 28.3. Informacje o zablokowanych wiadomościach użytkownik otrzymuje w dwóch zbiorczych raportach w ciągu dnia. Raporty są wysyłane z adresu e-mail kwarantanna@lasy.gov.pl.
- 28.4. W przypadku zablokowanych wiadomości, które nie zostały zawarte w raportach należy skorzystać z portalu znajdującego się pod adresem <https://kwarantanna.lasy.gov.pl>. Logowanie do portalu odbywa się za pośrednictwem adresu e-mail użytkownika oraz hasła domenowego.
- 28.5. Decyzję o dostarczeniu lub odrzuceniu wiadomości z kwarantanny podejmuje jej adresat.
- 28.6. W przypadku nieuzasadnionego zablokowania nadawcy wiadomości e-mail przez zabezpieczenia serwera, należy ten fakt zgłosić do WI lub za pośrednictwem SZBM.

Regulamin użytkownika systemu poczty elektronicznej LP

29. W przypadku otrzymania wiadomości e-mail z nieznanego źródła, zawierającej podejrzaną treść lub załącznik, użytkownik zobowiązany jest do:
- 29.1. Zachowania szczególnej ostrożności, nieotwierania odnośników i załączników.
 - 29.2. Poinformowania o możliwym incydencie administratora SILP jednostki, WI lub bezpośrednio ZCI przesyłając przedmiotową wiadomość jako załącznik na adres incydent@las.gov.pl.
 - 29.3. Wiadomości spam, które nie zostały wykryte przez system ochrony poczty LP należy przesyłać na adres tojestspam@las.gov.pl
30. Użytkownik zobowiązuje się do wykorzystywania konta zgodnie z obowiązującymi przepisami prawa, normami społecznymi i obyczajowymi, postanowieniami niniejszego regulaminu, a w szczególności do:
- 30.1. działania w sposób nienaruszający praw innych użytkowników;
 - 30.2. niepodejmowania działań mających na celu odczytanie haseł innych użytkowników;
 - 30.3. niepodejmowania działań mających na celu odczytanie wiadomości, których nie jest adresatem;
 - 30.4. nieudostępniania konta poczty LP osobom trzecim;
 - 30.5. nierozsyłania z konta niechcianej przez odbiorców korespondencji, w szczególności spamu, niezamówionych treści o charakterze reklamowym, informacyjnym, łańcuszków internetowych.
31. Użytkownik ponosi odpowiedzialność za treść i zawartość wiadomości elektronicznych wysłanych za pośrednictwem swojego konta pocztowego.
32. Z uwagi na konieczność zapewnienia organizacji pracy umożliwiającej pełne wykorzystanie czasu pracy oraz właściwego użytkownika udostępnionych pracownikowi narzędzi pracy, pracodawca może wprowadzić kontrolę i monitoring służbowej poczty elektronicznej pracownika.
33. Lasy Państwowe nie ponoszą odpowiedzialności za:
- 33.1. Sposób w jaki użytkownicy korzystają z kont pocztowych ani za jakiegokolwiek wynikłe z tego skutki.
 - 33.2. Treść wiadomości wysłanych oraz przyjmowanych przez użytkowników.
 - 33.3. Skutki wynikłe z wejścia w posiadanie przez osoby trzecie hasła użytkownika, niezależnie od przyczyny, która to spowodowała (np. udostępnienie hasła osobie trzeciej przez użytkownika, złamanie hasła przez osobę trzecią).
 - 33.4. Udostępnianie hasła i danych osobom upoważnionym na podstawie właściwych przepisów prawa.

Regulamin użytkownika systemu poczty elektronicznej LP

34. Lasy Państwowe zastrzegają sobie prawo, a użytkownik to prawo akceptuje, do:
- 34.1. Natychmiastowego zablokowania konta użytkownika bez uprzedzenia, w przypadku naruszenia przez użytkownika niniejszego regulaminu.
 - 34.2. Zablokowania konta użytkownika bez uprzedzenia, w przypadku podejrzenia wycieku danych.
 - 34.3. Zablokowania na serwerach Systemu Poczтового LP nadawców wiadomości lub całych domen i adresów IP w razie naruszenia dóbr użytkowników LP przez nadawców wiadomości z zewnątrz, w wypadku narażenia systemu poczty LP na straty lub niestabilność lub w razie naruszenia Regulaminu,
 - 34.4. Uruchamiania oprogramowania przetwarzającego wiadomości przychodzące do systemu pocztowego w celu klasyfikacji wiadomości (np. jako *spam*, *phishing* lub *malware*) na podstawie ich treści.
 - 34.5. Uruchamiania oprogramowania zapobiegającego na podstawie analizy treści wiadomości wyciekowi danych stanowiących tajemnice przedsiębiorstwa.
 - 34.6. Usuwania z wiadomości poczty elektronicznej treści niebezpiecznych, w szczególności takich jak złośliwe oprogramowanie czy odnośniki do niebezpiecznych stron o niskiej reputacji.
 - 34.7. Wprowadzenia ograniczeń ilości i wielkości wiadomości przyjmowanych oraz przechowywanych przez system pocztowy. Ograniczenie powyższe dotyczyć może konkretnych skrzynek poczty elektronicznej.
 - 34.8. Usunięcia konfiguracji automatycznego przekazywania wiadomości poczty elektronicznej poza SILP.
 - 34.9. Zmian konfiguracji konta pocztowego w celu uzyskania stanu zgodności z Regulaminem.
35. Lasy Państwowe zobowiązują się, iż nie będą udostępniać zebranych danych osobom trzecim. Wyjątki od tej zasady mogą być spowodowane wyłącznie postanowieniem uprawnionych organów państwowych.
36. Wszelkie uwagi i problemy techniczne w działaniu Systemu Poczтового LP należy zgłaszać do właściwego administratora systemu pocztowego.

Regulamin użytkowania systemu poczty elektronicznej LP

Tabela nr 1 Wymagane adresy w domenie lasy.gov.pl

Adres bez domeny	Przykładowy adres	Uwagi	Upewnienia do wysyłania wiadomości
dglp	dglp@las.gov.pl	Osoba (osoby) odpowiedzialna za obsługę sekretariatu Dyrektora Generalnego	bez ograniczeń
sekretariate	sekretariate@las.gov.pl	Osoba (osoby) odpowiedzialna za obsługę sekretariatu Zastępcy Dyrektora Generalnego ds. Ekonomicznych	bez ograniczeń
sekretariatZ	sekretariatZ@las.gov.pl	Osoba (osoby) odpowiedzialna za obsługę sekretariatu Zastępcy Dyrektora Generalnego ds. Zrównoważonej Gospodarki Leśnej	bez ograniczeń
gabinet.dg	gabinet.dg@las.gov.pl	Gabinet Dyrektora Generalnego	bez ograniczeń
kommunikacja	kommunikacja@las.gov.pl	Wydział Komunikacji Strategicznej	bez ograniczeń
inspekcja.lp	inspekcja.lp@las.gov.pl	Inspekcja Lasów Państwowych	bez ograniczeń
inspektorat.sl	inspektorat.sl@las.gov.pl	Inspektorat Straży Leśnej	bez ograniczeń
kadry	kadry@las.gov.pl	Wydział Zarządzania Zasobami Ludzkimi	bez ograniczeń
obronosc	obronosc@las.gov.pl	Zespół ds. Obronności i Ochrony Informacji Niejawnych	bez ograniczeń
hodowla	hodowla@las.gov.pl	Wydział Hodowli Lasu	bez ograniczeń
ochrona	ochrona@las.gov.pl	Wydział Ochrony Lasu	bez ograniczeń

Regulamin użytkowania systemu poczty elektronicznej LP

urzadzanie	urzadzanie@lasy.gov.pl	Wydział Urządzenia Lasu	bez ograniczeń
ochrona przyrody	ochrona.przyrody@lasy.gov.pl	Wydział Ochrony Przyrody	bez ograniczeń
wsfl	wsfl@lasy.gov.pl	Wydział Społecznych Funkcji Lasu	bez ograniczeń
marketing	marketing@lasy.gov.pl	Wydział Gospodarki Drewnem	bez ograniczeń
lowiectwo	lowiectwo@lasy.gov.pl	Zespół ds. łowiectwa	bez ograniczeń
stan.posiadania	stan.posiadania@lasy.gov.pl	Wydział Stanu Posiadania	bez ograniczeń
bhp	bhp@lasy.gov.pl	Stanowisko ds. Bezpieczeństwa i Higieny Pracy	bez ograniczeń
finanse	finanse@lasy.gov.pl	Wydział Księgowości	bez ograniczeń
planowanie	planowanie@lasy.gov.pl	Wydział Analiz Ekonomicznych i Planowania	bez ograniczeń
innowacje	innowacje@lasy.gov.pl	Wydział Organizacji i Rozwoju	bez ograniczeń
infrastruktura	infrastruktura@lasy.gov.pl	Wydział Infrastruktury i Zamówień Publicznych	bez ograniczeń
informatyka	informatyka@lasy.gov.pl	Wydział Informatyki	bez ograniczeń

Regulamin użytkownika systemu poczty elektronicznej LP

administracja	administracja@las.gov.pl	Wydział Administracji	bez ograniczeń
sd	sd@las.gov.pl	Staż Dyżur	bez ograniczeń
palp	palp@las.gov.pl	Punkt Alarmowy Lasów Państwowych	bez ograniczeń
administracja	administracja@las.gov.pl	Wydział Administracji	bez ograniczeń
rzecznik	rzecznik@las.gov.pl	Rzecznik Prasowy	bez ograniczeń
rdlp	rdlp@las.gov.pl	Wszystkie rdlp, w liście zawarte minimum 1 adres każdej RDLP rdlp@warszawa.las.gov.pl itd.	tylko zdefiniowane adresy
rdlp.dyrektor	rdlp.dyrektor@las.gov.pl	Wszyscy dyrektorzy rdlp oraz kierownicy jednostek o zasięgu krajowym.	tylko zdefiniowane adresy
rdlp.zastepca.e	rdlp.zastepca.e@las.gov.pl	Zastępcy Dyrektorów rdlp ds. ekonomicznych	tylko zdefiniowane adresy
rdlp.zastepca.z	rdlp.zastepca.z@las.gov.pl	Zastępcy Dyrektorów rdlp ds. Gospodarki Leśnej	tylko zdefiniowane adresy
rdlp.kadry	rdlp.kadry@las.gov.pl	Wydział Organizacji i Kadry rdlp	tylko z adresów w domenach *las.gov.pl
rdlp.kontrola	rdlp.kontrola@las.gov.pl	Wydział Kontroli i Audytu Wewnętrznego rdlp	tylko z adresów w domenach *las.gov.pl
rdlp.obronnosc	rdlp.obronnosc@las.gov.pl	Stanowiska / Zespoły ds. Obronności i Ochrony Mienia rdlp	tylko z adresów w domenach *las.gov.pl

Regulamin użytkowania systemu poczty elektronicznej LP

rdlp.rzecznik	rdlp.rzecznik@las.gov.pl	Rzecznicy Prasowi / Zespoły ds. Promocji i Mediów rdLP	tylko z adresów w domenach *las.gov.pl
rdlp.zagospodarowanie	rdlp.zagospodarowanie@las.gov.pl	Wydziały Gospodarowania Ekosystemami rdLP	tylko z adresów w domenach *las.gov.pl
rdlp.ochrona	rdlp.ochrona@las.gov.pl	Wydziały Ochrony Ekosystemów rdLP	tylko z adresów w domenach *las.gov.pl
rdlp.zasoby	rdlp.zasoby@las.gov.pl	Wydziały Zarządzania Zasobami Leśnymi rdLP	tylko z adresów w domenach *las.gov.pl
rdlp.infrastruktura	rdlp.infrastruktura@las.gov.pl	Wydziały Infrastruktury Leśnej rdLP	tylko z adresów w domenach *las.gov.pl
rdlp.finance	rdlp.finance@las.gov.pl	Wydziały Księgowości rdLP	tylko z adresów w domenach *las.gov.pl
rdlp.planowanie	rdlp.planowanie@las.gov.pl	Wydziały / Zespoły Analiz i Planowania rdLP	tylko z adresów w domenach *las.gov.pl
rdlp.marketing	rdlp.marketing@las.gov.pl	Wydziały Gospodarki Drewnem rdLP	tylko z adresów w domenach *las.gov.pl
rdlp.administracja	rdlp.administracja@las.gov.pl	Wydziały Administracji rdLP	tylko z adresów w domenach *las.gov.pl
rdlp.informatyka	rdlp.informatyka@las.gov.pl	Wydziały / Zespoły Informatyki rdLP	tylko z adresów w domenach *las.gov.pl
rdlp.projekty	rdlp.projekty@las.gov.pl	Zespoły / Stanowiska ds. Koordynacji Wdrażania Projektów Rozwojowych	tylko z adresów w domenach *las.gov.pl
rdlp.sd	rdlp.sd@las.gov.pl	Wszystkie Stale dyżury rdLP	tylko zdefiniowane adresy
zaklady.informatyka	zaklady.informatyka@las.gov.pl	Osoby odpowiedzialne za obsługę informatyczną zakładów	tylko z adresów w domenach *las.gov.pl

Regulamin użytkownika systemu poczty elektronicznej LP

zaklady.finance	zaklady.finance@las.gov.pl	Osoby odpowiedzialne za księgowości w zakładach	tylko z adresów w domenach *las.gov.pl
zaklady.sd	zaklady.sd@las.gov.pl	Osoby odpowiedzialne za Staty Dyżur w Zakładach	tylko zdefiniowane adresy
nadleśnictwa	nadleśnictwa@las.gov.pl	Wszystkie Nadleśnictwa	tylko zdefiniowane adresy
nadleśniczy	nadleśniczy@las.gov.pl	Wszyscy Nadleśniczowie	tylko zdefiniowane adresy
uzytkownicy	uzytkownicy@las.gov.pl	Wszyscy użytkownicy systemu poczty w domenie las.gov.pl	tylko zdefiniowane adresy
komunikaty.ezd	komunikaty.ezd@las.gov.pl	Wszyscy administratorzy i koordynatorzy EZD	tylko zdefiniowane adresy

Tabela nr 2 Wymagane adresy w domach rdLP

Adres bez domeny	Przykładowy adres	Uwagi	Uprawnienia do wysyłania wiadomości
rdlp	rdlp@warszawa.las.gov.pl	Osoba (osoby) odpowiedzialna za obsługę korespondencji przychodzącej do RDLP	bez ograniczeń
kadry	kadry@warszawa.las.gov.pl	Wydział Organizacji i Kadry	bez ograniczeń
kontrola	kontrola@warszawa.las.gov.pl	Wydział Kontroli i Audytu Wewnętrznego	bez ograniczeń
obronnosc	obronnosc@warszawa.las.gov.pl	Stanowisko / Zespół ds. Obronności i Ochrony Mienia	bez ograniczeń
rzecznik	rzecznik@warszawa.las.gov.pl	Rzecznik Prasowy / Zespół ds. Promocji i Mediów	bez ograniczeń

Regulamin użytkowania systemu poczty elektronicznej LP

sd	sd@warszawa.lasy.gov.pl	Staty Dyżur	bez ograniczeń
nadleśnictwa.sd	nadleśnictwa.sd@warszawa.lasy.gov.pl	Osoby odpowiedzialne za Staty Dyżur w Nadleśnictwach	tylko zdefiniowane adresy
palp	palp@warszawa.lasy.gov.pl	Punkt Alarmowy Lasów Państwowych	bez ograniczeń
zagospodarowanie	zagospodarowanie@warszawa.lasy.gov.pl	Wydział Gospodarowania Ekosystemami	bez ograniczeń
ochrona	ochrona@warszawa.lasy.gov.pl	Wydział Ochrony Ekosystemów	bez ograniczeń
zasoby	zasoby@warszawa.lasy.gov.pl	Wydział Zarządzania Zasobami Leśnymi	bez ograniczeń
infrastruktura	infrastruktura@warszawa.lasy.gov.pl	Wydział Infrastruktury	bez ograniczeń
finanse	finanse@warszawa.lasy.gov.pl	Wydział Księgowości	bez ograniczeń
planowanie	planowanie@warszawa.lasy.gov.pl	Wydział / Zespół Analiz i Planowania	bez ograniczeń
marketing	marketing@warszawa.lasy.gov.pl	Wydział Gospodarki Drewnem	bez ograniczeń
administracja	administracja@warszawa.lasy.gov.pl	Wydział Administracji	bez ograniczeń
informatyka	informatyka@warszawa.lasy.gov.pl	Wydział / Zespół Informatyki	bez ograniczeń

Regulamin użytkownika systemu poczty elektronicznej LP

projekty	projekty@warszawa.lasy.gov.pl	Zespół / Stanowisko ds. Koordynacji Wdrażania Projektów Rozwojowych	bez ograniczeń
pad	pad.warszawa.lasy.gov.pl	Punkt alarmowo dyspozycyjny	bez ograniczeń
nazwa_jednostki_lp	chojnow@warszawa.lasy.gov.pl	Adres kierownika jednostki lub osoby (osób) upoważnionej do obsługi korespondencji przychodzącej do jednostki.	bez ograniczeń
sd.nazwa_ki_lp	sd.chojnow@warszawa.lasy.gov.pl	Staty Dyżur w nadleśnictwie	bez ograniczeń
pad.nazwa_jednostki_lp	pad.chojnow@warszawa.lasy.gov.pl	Punkt Alarmowo Dyspozycyjny w nadleśnictwie	bez ograniczeń
administratorzy	administratorzy@warszawa.lasy.gov.pl	W liście zawarte adresy administratorów SILP w jednostkach RDLP	tylko z adresów w domenach *.lasy.gov.pl
uzytkownicy	uzytkownicy@warszawa.lasy.gov.pl	Wszyscy użytkownicy systemu poczty w domenie RDLP	tylko zdefiniowane adresy
ezd	ezd@warszawa.lasy.gov.pl	Wszyscy administratorzy i koordynatorzy EZD w domenie RDLP	bez ograniczeń
ezd.rdlp	ezd.rdlp@warszawa.lasy.gov.pl	Administratorzy i koordynatorzy EZD w biurze RDLP	bez ograniczeń
ezd.nazwa_jednostki_lp	ezd.chojnow@warszawa.lasy.gov.pl	Administratorzy i koordynatorzy EZD w jednostkach	bez ograniczeń

Tabela nr 3 Wymagane adresy w domenach zakładów o zasięgu krajowym

Adres bez domeny	Przykładowy adres	Uwagi	Uprawnienia do wysyłania wiadomości
biuro	biuro@zilp.lasy.gov.pl	Osoba (osoby) odpowiedzialna za obsługę korespondencji przychodzącej do zakładu	bez ograniczeń

Regulamin użytkownika systemu poczty elektronicznej LP

informatyka	informatyka@zilp.lasy.gov.pl	Osoba (osoby) odpowiedzialna za obsługę informatyczną zakładu	bez ograniczeń
finanse	finanse@zilp.lasy.gov.pl	Osoba (osoby) odpowiedzialna za księgowość w zakładzie	bez ograniczeń
uzytkownicy	uzytkownicy@zilp.lasy.gov.pl	Wszyscy użytkownicy systemu poczty w domenie zakładu	tylko zdefiniowane adresy
pk	pk@zilp.lasy.gov.pl	Punkt kontaktowy	bez ograniczeń
Ezd	ezd@zilp.lasy.gov.pl	Administratorzy i koordynatorzy EZD w domenie zakładu	bez ograniczeń

Urządzenia uwierzytelniania użytkowników LP

wprowadzony na podstawie Załącznika nr 2 do Zarządzenia nr 35 Dyrektora Generalnego Lasów Państwowych z dnia 18 maja 2026 r. w sprawie zasad funkcjonowania i zasad bezpieczeństwa systemu informatycznego w Państwowym Gospodarstwie Leśnym Lasy Państwowe.

Data	Autor	Wersja	Opis zmian
2026-05-26	EI.C	1.0	Pierwsza wersja dokumentu

Urządzenia uwierzytelniania użytkowników LP

1. Urządzenia kryptograficzne służące przechowywaniu materiału kryptograficznego w tym certyfikatów użytkownika wystawionych przez PKI LP. Wymagania minimalne dla urządzenia (karty lub inne nośniki):
 - a. musi umożliwiać zarządzanie cyklem życia Karty z poziomu HID® ActivID™ Credential Management System w wersji minimum: 6.4;
 - b. musi współpracować z oprogramowaniem pośredniczącym HID® ActivClient, w tym szczególnie w zakresie CryptoAPI jak i PKCS#11;
 - c. wsparcie dla PKCS#11 w środowiskach: Windows10, Windows11 (obsługa systemów operacyjnych 32/64-bit). Mac, Linux;
 - d. wsparcie następujących algorytmów kryptograficznych i szyfrujących: 3TDES: 3 keys (CBC and ECB) (legacy only), AES: (128-, 192-, 256-bit) (CBC and ECB); RSA: (2048-, 3072-, 4096-bit); ECC: (P-256, P-384 bits); HMAC-SHA1, HMAC-SHA2 (256-, 512-bit);
 - e. System operacyjny karty musi być zgodny ze specyfikacją JavaCard wersji 3.0.5 lub wyższej;
 - f. Interfejs stykowy musi spełniać jeden z poniższych warunków: I. musi być zgodny z normą ISO 7816-3 (T=0 and T=1)
II. USB 2.0 min. 12Mbps, posiadać dotykowy interfejs potwierdzający obecność użytkownika, dwukolorowy wskaźnik statusu urządzenia
 - g. Certyfikację Common Criteria EAL 6+ , FIPS 140-3 poziom 3
 - h. Gwarantowany okres przechowywania danych w pamięci nieulotnej karty – min. 25 lat;
 - i. Karta musi posiadać co najmniej 16 dostępnych „slotów” na klucze PKI oraz 24 „sloty” na klucze PIV;
 - j. Karta ma zapewniać wsparcie dla polityki haseł (pinów):
 - I. Możliwość współdzielenia pin pomiędzy PKI, FIDO and OATH
 - II. Konfigurowalna minimalna i maksymalna długość PIN użytkownika
 - III. Konfigurowalna ilość wprowadzenia błędnych PIN przed zablokowaniem karty,
 - IV. Możliwość wymuszenia PIN tylko numerycznego
 - V. Możliwość ustawienia PIN alfanumerycznego
 - k. Jeżeli urządzenie jest kartą to wymiary nie mogą przekraczać 54 x 85.7 x 0.84 mm;
 - l. Jeżeli urządzenie jest kartą to musi być możliwość nadruku zarówno w technologii Direct to Card DTC jak i w technologii retransferowej;
 - m. Jeżeli urządzeniem jest kartą musi zostać spersonalizowane tj. musi być na urządzeniu widoczna nazwa użytkownika i logo Lasów Państwowych.

Urządzenia uwierzytelniania użytkowników LP

2. Urządzenia do autoryzacji dla systemów zbliżeniowych:

Urządzenie musi spełniać jeden z poniższych punktów:

a. Urządzenie z obsługą:

I. Seos 8K, Mifare Classic, MIFARE DESFire (z wsteczną kompatybilnością z EV2/EV1), dla częstotliwości 13.56MHz; II. HID Prox, dla częstotliwości 125KHz;

III. musi być zgodna z normą ISO 14443 dla interfejsu bezstykowego;

b. Zgodność z ISO 14443 dla interfejsu bezstykowego z NFC (T=CL)

3. Urządzenie uwierzytelniania może być pojedyncze - jednocześnie spełniające funkcjonalność wymienione w pkt. 1 i w pkt. 2 (urządzenie/karta dualna)

ZASADY DOSTĘPU DO DANYCH W SYSTEMIE INFORMATYCZNYM LASÓW PAŃSTWOWYCH

§ 1

Reguły ogólne

1. Zasady stosuje się jedynie w przypadku dostępu do danych SILP, które wymagają kontroli dostępu. Zasady nie dotyczą danych dostępnych publicznie.
2. Przez dostęp do danych SILP rozumie się proces składający się z kolejnych etapów:
 - 1) uwierzytelnienia - potwierdzenia tożsamości podmiotu, który chce uzyskać dostęp do danych;
 - 2) autoryzacji podmiotu i nadanie uprawnień do danych - weryfikacji uprawnień oraz przyznanie dostępu do określonych danych zgodnie z przypisaną podmiotowi rolą lub zakresem;
 - 3) przetwarzania danych zgodnie z nadanymi uprawnieniami.
3. Dostęp do danych SILP przyznawany jest wyłącznie zidentyfikowanym i uprawnionym podmiotom, zgodnie z ich rolą oraz zakresem obowiązków.
4. Przetwarzanie danych osobowych szczegółowo reguluje odrębne zarządzenie Dyrektora Generalnego LP w sprawie wprowadzenia zasad korzystania z danych osobowych przetwarzanych w Systemie Informatycznym Lasów Państwowych.

§ 2

Dostęp dla użytkowników SILP

1. Dostęp do danych SILP może być realizowany w dwóch trybach:
 - 1) dostępu stałego - przyznawany na czas nieokreślony;
 - 2) dostępu tymczasowego - przyznawany na czas określony do realizacji konkretnego zadania, po którego zakończeniu uprawnienia są automatycznie wycofywane lub wygasają.
2. Dostęp stały do danych SILP może być przyznawany dla:

- 1) Użytkowników SILP zatrudnionych na czas nieokreślony w jednostce LP wyłącznie na podstawie udokumentowanej dyspozycji kierownika jednostki lub bezpośredniego przełożonego określającej:
 - a) wskazane zasoby danych danej jednostki,
 - b) zakres uprawnień dostępu do danych;
 - 2) Osób zatrudnionych w jednostce nadrzędnej, w ramach sprawowania nadzoru, na podstawie udokumentowanej dyspozycji kierownika jednostki nadrzędnej, określającej wskazane zasoby danych jednostek podległych;
 - 3) Instruktorów regionalnych SILP wyznaczonych przez dyrektora rdLP, jedynie w określonym zakresie funkcjonalnym SILP niezbędnym do świadczenia pomocy.
 - 4) Członków stałych zespołów zadaniowych powołanych zarządzeniem Dyrektora Generalnego Lasów Państwowych w zakresie niezbędnym do realizacji zleconych zadań;
 - 5) Pracowników PGL LP wskazanych w aktach regulacji wewnętrznej Dyrektora Generalnego Lasów Państwowych w zakresie niezbędnym do realizacji powierzonych zadań.
3. Dostęp tymczasowy do danych SILP może być realizowany dla:
- 1) osób zatrudnionych w jednostce na czas określony;
 - 2) pracowników ILP zgodnie z zarządzeniem Dyrektora Generalnego Lasów Państwowych w sprawie kontroli instytucjonalnej w Państwowym Gospodarstwie Leśnym Lasy Państwowe;
 - 3) członków doraźnych zespołów zadaniowych powołanych zarządzeniem lub decyzją, w zakresie i na czas niezbędny do realizacji zleconych zadań.
4. Rozwiązanie stosunku pracy z pracownikiem posiadającym dostęp do danych SILP, skutkuje niezwłocznym odebraniem uprawnień dostępu. Zgodnie z przyjętą w danej jednostce organizacyjnej LP procedurą realizowane jest:
- 1) odebranie uprawnień dostępu do danych, poprzez zablokowanie kont użytkownika w systemach oraz dezaktywację konta domenowego;
 - 2) odebranie środków technicznych IT umożliwiających dostęp do SILP.
5. Zmiana stanowiska pracy lub zakresu obowiązków użytkownika SILP posiadającego dostęp do danych SILP wymaga niezwłocznej aktualizacji zakresu uprawnień dostępu, zgodnie z procedurą przyjętą w danej jednostce organizacyjnej LP.
6. Komórka właściwa ds. kadrowych niezwłocznie informuje WI lub administratora SILP jednostki o nawiązaniu lub rozwiązaniu stosunku pracy z użytkownikiem SILP.
7. Komórka właściwa ds. kadrowych niezwłocznie informuje WI lub administratora SILP jednostki o zmianie stanowiska użytkownika SILP wewnątrz struktury organizacyjnej lub o zmianie jego zakresu obowiązków.

§ 3

Dostęp dla administratorów SILP

1. Administratorzy SILP są uprawnieni do dostępu do danych jednostek, w których są zatrudnieni oraz do danych jednostek nadzorowanych lub innych jednostek na rzecz których świadczą usługi informatyczne.
2. Administratorzy SILP są uprawnieni do dostępu do danych w trybie uprzywilejowanym z rozszerzonym zakresem uprawnień.
3. Czynności administracyjne powodujące zmiany danych systemu LAS danej jednostki mogą być realizowane przez administratora SILP wyłącznie za akceptacją głównego księgowego jednostki.
4. Administratorzy SILP nadają i odbierają dostępy użytkownikom SILP zgodnie z udokumentowanymi poleceniami kierowników jednostek.

§ 4

Dostęp dla podmiotów zewnętrznych

1. Dostęp do danych SILP dla podmiotu zewnętrznego jest realizowany na podstawie umowy, porozumienia lub innego zobowiązania cywilno-prawnego pomiędzy jednostką organizacyjną LP a podmiotem zewnętrznym. Zobowiązanie musi określać, osoby uzyskujące dostęp, okres oraz zasoby do których podmiot zewnętrzny ma uzyskać prawo dostępu.
2. Dostęp przyznawany jedynie do zasobów niezbędnych do wykonania prac określonych w zobowiązaniu.
3. Dostęp jest przyznawany jedynie na czas wykonywania prac określonych w zobowiązaniu.

§ 5

Dostęp dla podmiotów edukacyjnych

1. Dostęp do danych SILP dla podmiotu edukacyjnego jest realizowany na podstawie porozumienia pomiędzy podmiotem edukacyjnym a jednostką organizacyjną LP.
2. Dla podmiotów edukacyjnych dane SILP są udostępniane w dedykowanym środowisku edukacyjnym zarządzanym przez ZILP.

3. ZILP nadaje dostęp administracyjny dla osoby uprawnionej z danego podmiotu edukacyjnego, która nadaje dostępy i uprawnienia użytkownikom lokalnym.
4. Na potrzeby szkoleń, nauki zawodu, testów rozwojowych lub w celu realizacji tematów badawczych, administrator SILP na polecenie kierownika jednostki może wykonać i udostępnić podmiotowi z którym zawarto porozumienie, kopię danych przygotowaną w sposób uniemożliwiający identyfikację danych osobowych adresowych i płacowo kadrowych.

§ 6

Dostęp dla systemów zewnętrznych

1. Dostęp do danych SILP przez systemy zewnętrzne może być realizowany wyłącznie na polecenie i za zgodą Dyrekcji Generalnej Lasów Państwowych.
2. Autoryzacja dostępu pomiędzy systemami musi odbywać się z wykorzystaniem zaufanych certyfikatów instalowanych na serwerach.

§ 7

Rozliczalność dostępu

1. Każda czynności nadania lub zmiany nadanych dostępu i uprawnień musi być zapisana do dziennika zdarzeń z jednoznaczną identyfikacją czasu oraz podmiotu wprowadzającego zmianę.
2. Dziennik zdarzeń musi przechowywać informację o czynnościach określonych w pkt. 1 przez okres co najmniej 3 lat.
3. Każda czynność przetwarzania danych zgodnie z nadanymi uprawnieniami musi być zapisana do dziennika zdarzeń z jednoznaczną identyfikacją czasu oraz podmiotu przetwarzającego.
4. Dziennik zdarzeń musi przechowywać informację o czynnościach określonych w pkt. 3 przez okres co najmniej 6 miesięcy.