Zał. Nr 5
do Regulaminu Organizacyjnego

„Wyciąg z zasad funkcjonowania i zasad bezpieczeństwa systemu informatycznego w Lasach Państwowych"

I. Zasady funkcjonowania Systemu Informatycznego w Lasach Państwowych

§ 1.
Terminy użyte w tekście

1. Lasy Państwowe, LP – Państwowe Gospodarstwo Leśne Lasy Państwowe.
2. DGLP – Dyrekcja Generalna Lasów Państwowych.
3. RDLP – regionalne dyrekcje Lasów Państwowych.
4. ILP – Inspekcja Lasów Państwowych.
5. SILP – Zintegrowany System Informatyczny Lasów Państwowych, zbiór elementów, którego funkcją jest przetwarzanie, przechowywanie i przesyłanie danych w PGL LP przy użyciu zasobów informatycznych LP.
6. Publiczne zasoby SILP – zbiór elementów SILP dostępnych publicznie z sieci Internet. Zasoby umieszczone są w dedykowanym i wydzielonym fragmencie sieci, odseparowanym technicznie od sieci wewnętrznej LP.
7. Wewnętrzne zasoby SILP – zbiór wszystkich elementów SILP z wyłączeniem Publicznych zasobów SILP.
8. System LAS – system i podstawowa aplikacja biznesowa LP.
9. BO – Business Objects i zdefiniowany w nim świat obiektów – stanowiąca oprogramowanie do analizy i tworzenia raportów z danych zapisanych w bazach SILP.
10. SZKZ – System Zarzadzania Kodami Źródłowymi SILP.
11. SZBM – narzędzie udostępnione poprzez przeglądarkę internetową pod nazwą „System Zgłaszania Błędów i Modyfikacji SILP".
12. CP – Centrum Podstawowe przetwarzania danych, zasoby SILP zlokalizowane w serwerowni w budynku biurowym DGLP.
13. CZ – Centrum Zapasowe przetwarzania danych, zasoby SILP zlokalizowane w serwerowni w Sękocinie Starym.
14. WAN LP – sieć rozległa Lasów Państwowych, komputerowa sieć modułu TCP/IP odpowiedzialna za przesyłanie danych pomiędzy jednostkami LP.
15. LAN – sieci lokalne w jednostkach LP.
16. LAN PC – sieci lokalne w jednostkach LP, do których podłączone są stacje robocze.
17. Sieć LP – wszystkie sieci transmisji danych będące własnością bądź zarządzane przez LP.
18. Dostęp zdalny VPN – dostęp do wewnętrznych zasobów SILP z sieci Internet za pośrednictwem szyfrowanych połączeń IPSes lub SSL.
19. Dostęp do SILP – dostęp do zasobów SILP za pośrednictwem konsoli, terminala, sieci LAN, WAN LP z wyłączeniem dostępu zdalnego VPN.
20. AD – Active Directory usługa katalogowa, katalog użytkowników i komputerów pracujących w sieci LP, zdefiniowana osobnym dokumentem „Projekt usług katalogowych PGL LP".
21. WI DGLP – Wydział Informatyki Dyrekcji Generalnej Lasów Państwowych.
22. Bezpieczeństwo informacji, bezpieczeństwo danych – bezpieczeństwo polegające na zachowaniu poufności, integralności i dostępności informacji SILP.
23. ZCI – Zespół w WI DGLP do spraw Cyberbezpieczeństwa Informatycznego, odpowiedzialny za nadzór nad bezpieczeństwem SILP.

24. SZBI – System zarządzania bezpieczeństwem informacji, część SILP oraz systemu zarządzania odnosząca się do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia bezpieczeństwa informacji przez ZCI.
25. ZILP – Zakład Informatyki Lasów Państwowych.
26. WI - komórki organizacyjne RDLP właściwe do spraw informatyki oraz administracji SILP w jednostkach nadzorowanych.
27. Administrator SILP – pracownicy odpowiedzialne za zasoby SILP we własnej jednostce.
28. Użytkownik SILP – pracownik Lasów Państwowych, 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.
29. Koordynator regionalny SZBM – pracownik WI w RDLP, który w swoim zakresie obowiązków ma koordynowanie zgłoszeń błędów przekazanych przez pracowników Nadleśnictw.
30. Koordynator centralny SZBM – wyznaczony pracownik LP, który w swoim zakresie obowiązków ma koordynowanie zgłoszeń błędów SZBM w przypisanym zakresie merytorycznym.
31. PKI LP – infrastruktura klucza publicznego Lasów Państwowych utrzymana w ramach wewnętrznych zasobów SILP.
32. Dane SILP stanowiące tajemnice przedsiębiorstwa – dane stanowiące tajemnicę przedsiębiorstwa zgodnie z klasyfikacją danych określoną przez zarządzenie nr 48 Dyrektora Generalnego Lasów Państwowych z dnia 6 października 2010r.

§ 2.
Zasady ogólne

1. Pod pojęciem Systemu Informatycznego Lasów Państwowych, należy rozumieć zbiór elementów, którego funkcją jest przetwarzanie danych w PGL LP przy użyciu techniki komputerowej, w tym:
   1.1. sprzęt,
   1.2. oprogramowanie,
   1.3. elementy organizacyjne,
   1.4. elementy informacyjne.
2. Przez funkcjonowanie SILP rozumie się kompleksowe współdziałanie pracowników i komórek organizacyjnych nadleśnictwa przy zastosowaniu technik komputerowych będących na wyposażeniu jednostki.
3. Podstawą prawidłowego funkcjonowania SILP są określone, jednolite dla danego poziomu organizacyjnego sprzęt, oprogramowanie, dokumenty źródłowe i wynikowe oraz jednolite zasady gromadzenia, przetwarzania i wymiany informacji.
4. Sprawy związane z przeprowadzeniem wdrożeń, w tym szkoleń, oraz nadzorem nad prawidłowym funkcjonowaniem systemu informacyjnego, są kompetencją Nadleśniczego.
5. W celu zabezpieczenia realizacji zadań, utrzymania i rozwoju SILP:
   5.1. Dyrektor Generalny powołuje:
      5.1.1. WI w DGLP;
      5.1.2. Zespół ds. Cyberbezpieczeństwa – wyodrębniona strukturę w ramach Wydziału Informatyki DGLP;
      5.1.3. ZILP;
      5.1.4. zespoły zadaniowe wg potrzeb.
   5.2. Dyrektor regionalnej dyrekcji LP powołuje:
      5.2.1. WI w RGLP;
      5.2.2. regionalnych instruktorów SILP
      5.2.3. zespoły zadaniowe - wg potrzeb
   5.3. Nadleśniczy, wyznacza spośród pracowników nadleśnictwa administratorów SILP odpowiedzialnych za zabezpieczenie prawidłowego funkcjonowania systemu na poziomie nadleśnictwa

6. Instruktorzy regionalni SILP mogą otrzymywać dodatkowe wynagrodzenie za wykonywanie, poza godzinami pracy, określonych zadań rzeczowych związanych z przygotowaniem szkoleń. Wynagrodzenie jest wypłacane na podstawie stosownej umowy, zawartej z kierownikiem jednostki organizacyjnej PGL LP.
7. Ramowe kryteria wynagrodzenia instruktorów regionalnych SILP ustala Dyrektor Generalny Lasów Państwowych.

§ 3.
Informatyka w Lasach Państwowych

1. Ze względu na zróżnicowanie zakresów zadań w obszarze informatyki w jednostkach organizacyjnych LP wyróżnia się zadania dla:
   1.1. WI DGLP,
      1.1.1. Zespołu ds. Cyberbezpieczeństwa Informatycznego
   1.2. ZILP,
   1.3. Wydziałów Informatyki w RDLP,
   1.4. Administratorów SILP w jednostkach nadzorowanych przez RDLP i zakładach o zasięgu krajowym,
   1.5. Regionalnych Instruktorów SILP.
2. Szczegółowe zakresy zadań wydziałów informatyki oraz administratorów SILP są określone w regulaminach organizacyjnych jednostek organizacyjnych.
3. Szczegółowe zadania ZILP precyzuje odrębne zarządzenie Dyrektora Generalnego LP.
4. Szczegółowe zakresy zadań Regionalnych Instruktorów SILP określają odrębne uregulowania stanowione przez dyrektorów RDLP.

§ 4.
Zadania administratora SILP

1. Do zadań administratora SILP należy w szczególności:
   1.1. aktualizacja oprogramowania aplikacji LAS,
   1.2. administrowanie zasobami, udostępnianie zasobów SILP pracownikom uprawnionym przez nadleśniczego z wykorzystaniem dostępnych w poszczególnych aplikacjach funkcji administratora poprzez:
      1.2.1. zarządzanie użytkownikami poszczególnych aplikacji,
      1.2.2. przygotowanie do akceptacji w SILP Web, autoryzacji uprawnień użytkowników do poszczególnych funkcji aplikacji oraz zasobów baz danych,
      1.2.3. autoryzację uprawnień użytkowników do poszczególnych funkcji aplikacji oraz zasobów baz danych w aplikacjach nieposiadających mechanizmu w SILP Web.
   1.3. zaopatrzenie pracowników w karty kryptograficzne i certyfikaty kwalifikowane. Ewidencje kart i certyfikatów prowadzi specjalista ds. pracowniczych.
   1.4. administrowanie i eksploatacja delegacjami aplikacji posadowionymi na serwerach w jednostkach nadrzędnych w zakresie określonym przez WI w RDLP,
   1.5. administrowanie siecią lokalną, komputerami oraz innym sprzętem komputerowym:
      1.5.1. nadzór nad stanem technicznym sprzętu i sieci lokalnej, wykonywanie okresowych przeglądów i konserwacji urządzeń, co najmniej raz w roku,
      1.5.2. konfiguracja komputerów do pracy w sieci,
      1.5.3. instalacja i bieżąca aktualizacja oprogramowania zainstalowanego na komputerach, w szczególności systemu operacyjnego i programów ochrony antywirusowej,
      1.5.4. nadzorowanie wykorzystania systemów komputerowych w nadleśnictwie z uwzględnieniem zasad bezpieczeństwa oraz ochrony antywirusowej,
      1.5.5. konfigurowanie kont pocztowych na komputerach użytkowników.
   1.6. w zakresie zabezpieczenia funkcjonowania SILP na poziomie leśnictwa
      1.6.1. administrowanie rejestratorem leśniczego oraz innymi urządzeniami komputerowymi

1.6.2. bieżący nadzór nad stanem technicznym sprzętu komputerowego, wykonywanie okresowych przeglądów i konserwacji urządzeń, co najmniej raz w roku,
1.6.3. instalacja i bieżąca konserwacja systemów operacyjnych komputerów z zainstalowanym systemem operacyjnym Microsoft Windows,
1.6.4. instalacja i aktualizacja oprogramowania użytkowego komputerów z zainstalowanym systemem operacyjnym Microsoft Windows,
1.6.5. instalacja i aktualizacja oprogramowania antywirusowego na komputerach z zainstalowanym systemem operacyjnym Microsoft Windows,
1.6.6. konfiguracja parametrów transmisji danych pomiędzy rejestratorem leśniczego i SILP,
1.6.7. konfiguracja urządzeń komputerowych do pracy w sieci,
1.6.8. udzielanie leśniczym instruktażu w zakresie obsługi technicznej urządzeń komputerowych,
1.6.9. konfigurowanie kont pocztowych.

1.7. koordynacja i organizacja procesów zakupu, urządzeń komputerowych, oprogramowania, konserwacji i napraw urządzeń komputerowych,
1.8. prowadzenie dokumentacji pracy administratora w tym
1.8.1. ewidencji protokołów instalacji,
1.8.2. ewidencji dokumentacji legalności oprogramowania,
1.8.3. ewidencji dokumentacji uprawnień dostępu do systemu baz danych,
1.8.4. ewidencji ingerencji z bazy danych oraz protokołów z tych czynności.
1.9. nadzór nad ochroną praw autorskich w odniesieniu do użytkowanego oprogramowania, w tym przeprowadzanie audytu legalności oprogramowania nie rzadziej niż raz w roku

§ 5.

Zadania komórek organizacyjnych RDLP i DGLP w zakresie wdrażania i eksploatacji SILP

1. Kierowników jednostek organizacyjnych RDLP i DGLP czyni się odpowiedzialnymi za znajomość zasad funkcjonowania i wykorzystywania 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.

§ 6.

Organizacja szkoleń SILP

1. Za organizację szkoleń z zakresu SILP odpowiadają:
1.1 WI w DGLP: pracowników biura DGLP, administratorów SILP, instruktorów regionalnych SILP.
1.2 Dyrektorzy RDLP: pracowników biura RDLP, pracowników jednostek nadzorowanych w tym administratorów SILP.
1.3 Dyrektorzy Zakładów o zasięgu krajowym: pracowników zakładów o zasięgu krajowym w tym administratorów SILP

§ 7.

Zasady działania w zakresie użytkowania SILP

1. Pracownicy nadleśnictwa, w których zakresie działania znajdują się zagadnienia objęte SILP są zobowiązani do:
   1.1. opanowania umiejętności posługiwania się systemem przynajmniej w zakresie swojego działania,
   1.2. prawidłowego i rzetelnego wprowadzania danych do systemu ręcznie lub przy pomocy informatycznych nośników informacji,
   1.3. terminowego wprowadzania dokumentów do SILP,
   1.4. zgłaszania wszelkich zauważonych błędów i nieprawidłowości w funkcjonowaniu SILP zgodnie z zasadami z ustalonymi w tym zakresie.
2. Bezpośredni przełożeni pracowników użytkujących system informatyczny są zobowiązani do:
   2.1. egzekwowania znajomości programu użytkowego zgodnego z zakresem czynności podległych pracowników,
   2.2. sprawowania nadzoru nad wykonaniem zadań określonych w pkt.1.1 - 1.4., a w szczególności dokonywanie wyrywkowej oceny:
      2.2.1. poprawności formalno-merytorycznej dokumentów wprowadzonych do SILP,
      2.2.2. zgodności danych w dokumencie z danymi wprowadzonymi do systemu,
      2.2.3. terminowości wprowadzania dokumentów do systemu.

§ 8.

Zgłaszanie błędów i modyfikacji SILP

Błędy i modyfikacje SILP może zgłosić każdy pracownik nadleśnictwa. Zgłaszanie błędów odbywa się za pośrednictwem SZBM (Systemu Zgłaszania Błędów i Modyfikacji), a w uzasadnionych przypadkach na pisemny wniosek skierowany drogą służbową do ZILP z powołaniem się na numer zgłoszenia w SZBIM.

§ 9.

Zgłoszenia błędów w SZBM

1. Wprowadzone do SZBM zgłoszenia podlegają wstępnej weryfikacji przez koordynatorów regionalnych SZBM, który dokonują właściwej kwalifikacji pod katem prawidłowej klasyfikacji w zakresie kategorii błędu lub modyfikacji i właściwego zakresu funkcjonalnego oraz wskazują zgłaszającemu możliwości rozwiązania, o ile leży to w kompetencjach koordynatora regionalnego SZBM.
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. Kompletne 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.

§ 10.

Zarządzanie zmianami w systemie LAS

Przez zarządzanie zmianami rozumie się procesy modyfikacji aplikacji, struktury bazy danych i danych stałych globalnych SILP (DSG) wywołane potrzebą:

1.1. poprawy błędów,
1.2. dostosowania aplikacji do zmian w prawie,
1.3. oprogramowania nowych zakresów funkcjonalnych,
1.4. zmian funkcjonalności modułów,
1.5. likwidacji zbędnych funkcji i modułów.

§ 11.

Modyfikacje w SILP

1. Podstawą do wprowadzenia modyfikacji SILP, w tym zmian DSG, są zgłoszenia w SZBM.
2. Koordynacją modyfikacji SILP zajmuje się WI DGLP. Na podstawie zgłoszeń WI w DGLP opracowuje, w uzgodnieniu z wydziałami merytorycznymi, zlecenia do ZILP wraz z określeniem terminów realizacji.
3. Dyrektor ZILP po otrzymaniu zlecenia Dyrektora Generalnego LP dokonuje modyfikacji SILP lub wykonuje nowe oprogramowanie. Dopuszcza się zlecenie wykonania modyfikacji oprogramowania lub wykonanie nowych elementów SILP podmiotom zewnętrznym, konserwującym poszczególne elementy SILP w ramach zawartych umów lub innym podmiotom wyłonionym na podstawie odrębnych procedur.
4. W przypadku braku możliwości realizacji modyfikacji, o których mowa § 10 ust. 1 w terminie oczekiwanym w zleceniu DGLP, priorytety realizacji modyfikacji ustalają w trybie roboczym członkowie ścisłego kierownictwa DGLP na wniosek naczelnika WI w DGLP.
5. Zmiany w SILP wynikające z usunięcia błędów lub modyfikacji przekazywane są przez Wykonawców w postaci kodów źródłowych, w formacie wymaganym przez SZKZ, wraz z dokumentacją techniczną, analityczną i instrukcją użytkownika (jeśli są wymagane).
6. Kody źródłowe podlegają weryfikacji w SZKZ pod względem ich poprawności.
7. Po pozytywnym wyniku tej weryfikacji następuje kompilacja kodów źródłowych do wersji wykonywalnej realizowana w SZKZ i przekazanie oprogramowania do testów ZILP oraz w jednostkach testowych LP powoływanych odrębnymi zarządzeniami Dyrektora Generalnego Lasów Państwowych.
8. Integralną częścią procesu testowania jest ocena przedłożonej dokumentacji wymienionej w ust. 5. Ocena dokumentacji jest realizowana przez ZILP, jednostki testowe i zespoły zadaniowe powołane przez Dyrektora Generalnego LP.
9. Pozytywny wynik testów oprogramowania oraz pozytywna ocena dokumentacji jest podstawą przekazania modyfikacji do wdrożenia w jednostkach LP.

§ 12.

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 Nadleśnictwa, przez administratora SILP.
4. Za dostosowanie do zmian w LAS specyficznych aplikacji dedykowanych dla zakładów Lasów Państwowych i ich wdrożenie odpowiada Dyrektor ZILP.

§ 13.

Wsparcie użytkowników w procesie wdrażania i eksploatacji SILP

1. Usługi wsparcia użytkowników w procesie wdrażania i eksploatacji SILP świadczą:
   1.1. pracownicy wydziałów DGLP w odniesieniu do wszystkich pracowników jednostek LP,
   1.2. pracownicy wydziałów RDLP w stosunku do pracowników biura RDLP i jednostek nadzorowanych przez RDLP,
   1.3. regionalni instruktorzy SILP w stosunku do pracowników biura RDLP i jednostek nadzorowanych przez RDLP,
   1.4. członkowie zespołów zadaniowych powołanych przez Dyrektora Generalnego Lasów Państwowych w zakresie określonym przez zarządzenie, w odniesieniu do wszystkich pracowników jednostek LP,
   1.5. koordynatorzy regionalni SZBM w odniesieniu do pracowników biura RDLP i jednostek nadzorowanych przez RDLP,
   1.6. koordynatorzy centralni SZBM w odniesieniu do wszystkich pracowników jednostek LP,
   1.7. ZILP w odniesieniu do wszystkich pracowników jednostek LP.
2. Usługi wsparcia użytkowników realizowane są poprzez:
   2.1. SZBM,
   2.2. konsultacje telefoniczne,
   2.3. pocztę elektroniczną,
   2.4. e-learning,
   2.5. wykorzystanie narzędzi udostępnionych w Intranecie, np. tematyczne strony WWW, komunikator elektroniczny, fora dyskusyjne.
3. Usługi wsparcia użytkowników realizowane przez członków zespołów zadaniowych, o których mowa w ust. 1.4 mogą być realizowane za zgodą i na wniosek, poprzez bezpośredni dostęp do danych jednostki zgłaszającej problem.

§ 14.

Instrukcje użytkownika

1. Do każdego modułu funkcjonalnego jest opracowana instrukcja użytkownika.
2. Instrukcje użytkownika opracowuje ZILP na podstawie materiałów własnych lub dokumentacji przekazywanych przez wykonawców.
3. Instrukcje są udostępniane dla użytkowników SILP w sieci WAN
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 modyfikacji.

II. Zasady bezpiecznej eksploatacji zasobów informatycznych Lasów Państwowych

§ 1.

Zasady ogólne

1. Dane przetwarzane w Systemie Informatycznym Lasów Państwowych (SILP) podlegają ochronie z uwagi na obowiązujące przepisy prawa, w szczególności z Ustawy o ochronie danych osobowych oraz Ustawy o ochronie informacji niejawnych.
2. Zachowanie bezpieczeństwa SILP i danych w nim przetwarzanych jest wspólnym obowiązkiem wszystkich pracowników nadleśnictwa.
3. Szczególną ochroną otoczone są dane SILP, stanowiące tajemnice przedsiębiorstwa oraz inne dane, które mogą mieć wpływ na działanie i bezpieczeństwo Nadleśnictwa.
4. SILP służy wyłącznie do wykonywania zadań służbowych.

5. Dostęp do wewnętrznych zasobów SILP jest przyznawany użytkownikom SILP jedynie do zasobów niezbędnych do świadczenia pracy.
6. Dostęp do SILP dla użytkowników z podmiotów zewnętrznych może być przydzielony jedynie w przypadku, gdy z podmiotem została podpisana umowa wymagająca takiego dostępu, przy spełnianiu następujących warunków:
   6.1 dostęp będzie możliwy jedynie na czas obowiązywania umowy.
   6.2 podmiot zewnętrzny podpisze oświadczenie o zasadach udzielania dostępu i zachowania poufności.
7. Dostęp do oprogramowania użytkowego i bazy danych nadleśnictwa posiadają pracownicy nadleśnictwa na podstawie przydzielonych im uprawnień.
8. Zabronione jest wykorzystywanie dostępu do przydzielonych zasobów informatycznych w celach sprzecznych z obowiązującymi przepisami prawa.
9. Zabronione jest umożliwieni osobom nieuprawnionym dostępu do SIPL.
10. Zabronione jest ujawnianie osobom nieuprawnionym: danych SILP stanowiących tajemnice przedsiębiorstwa, danych uwierzytelniania SILP, zasad działania i funkcjonowania SILP.
11. Informacje, dokumenty, korespondencja i pozostałe dane, które są przetwarzane w systemach informatycznych są własnością nadleśnictwa, a nadleśniczy ma prawo żądać 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 tajemnice przedsiębiorstwa i przenośny sprzęt do przetwarzania danych, które są wynoszone poza siedzibę nadleśnictwa, podlegają szczególnej ochronie. Użytkownik SILP jest zobowiązany do ochrony wynoszonych danych i sprzętu przed:
    12.1. zniszczeniem i uszkodzeniami mechanicznymi,
    12.2. kradzieżą,
    12.3. wpływami oddziaływań elektrostatycznych i elektrycznych,
    12.4. dostępem osób niepowołanych.
13. Wynoszenie danych SILP stanowiących tajemnice przedsiębiorstwa poza siedzibę nadleśnictwa wymaga zgody Nadleśniczego.
14. Dane SILP stanowiące tajemnice przedsiębiorstwa na nośnikach elektronicznych wynoszonych poza siedzibę nadleśnictwa muszą być zaszyfrowane.
15. Sprzęt elektroniczny przekazywany do serwisu musi być pozbawiony nośników z zapisanymi danymi SILP stanowiącymi tajemnice przedsiębiorstwa.
16. W przypadku likwidacji nośników zawierających dane SILP należy usunąć te dane w sposób uniemożliwiający ich odtworzenie.
17. Sieć komputerowa w nadleśnictwie opiera się o model zgodny z „Projektem usług katalogowych PGL LP" zatwierdzony przez WI DGLP.
18. Za utrzymanie i prawidłowe działanie systemów informatycznych w nadleśnictwie jest odpowiedzialny administrator SILP, a wszelkie prace związane z systemem informatycznym mogą być przeprowadzane tylko przez niego lub za jego wiedzą.

§ 2.

Bezpieczeństwo serwerów i systemów sieciowych SILP

1. Podstawową metodą uwierzytelniania użytkowników i administratorów w systemach wewnętrznych zasobów SILP jest uwierzytelnianie przy pomocy karty kryptograficznej i certyfikatu PKI LP lub haseł jednorazowych.
2. System wewnętrzny zasobów SILP mogą uwierzytelniać użytkowników SILP przy pomocy mechanizmów jednokrotnego logowania 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 i uwierzytelnianie za ich pomocą administratorów SILP w krytycznych ze względu na działanie SILP, elementach infrastruktury.

5. Dopuszcza się zakładanie kont 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 (np. backup, skaner), konta te nie mogą być użyte do logowania użytkowników i administratorów SILP.
7. Użycie innych zasad uwierzytelniania wymaga zatwierdzenia przez naczelnika WI DGLP na wniosek WI.
8. Hasła kont lokalnych systemów SILP podlegają zasadom tworzenia haseł określonym w projekcie usług katalogowych AD. W przypadku, gdy z powodu ograniczeń systemu, zastosowanie zasad z „Projektu usług katalogowych PGL LP nie jest możliwe, hasła należy tworzyć według zasad:
   8.1. hasło nie może zawierać identyfikatorów (loginów),
   8.2. hasło nie może zawierać imienia, nazwiska lub innych nazw własnych,
   8.3. hasło nie może zawierać informacji takich jak daty, numery pesel, numery telefonu,
   8.4. hasło nie może składać się z samych cyfr lub samych liter,
   8.5. w przypadku gdy system umożliwia użycie znaków specjalnych w haśle, hasło powinno zawierać znaki specjalne,
   8.6. hasło powinno mieć długość co najmniej 10 znaków. w przypadku, gdy z powodów ograniczeń systemu nie można stworzyć hasła o żądanej długości, hasło powinno mieć największą możliwą długość,
   8.7. 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 zobowiązani są do korzystania tylko z kont z ograniczonymi uprawnieniami. Dostęp do kont posiadających uprawnienia administracyjne posiadają tylko administratorzy SILP oraz członkowie stałych zespołów zadaniowych, w których zakresie są czynności administracyjne SILP. Mogą oni korzystać z tych kont tylko na czas wykonywania czynności administracyjnych.
12. Proces uwierzytelniania użytkowników w systemach SILP za pośrednictwem sieci należy realizować z użyciem połączeń szyfrowanych zapewniających poufność i integralność przesyłanych danych.
13. W przypadku realizacji dostępu do systemów SILP za pomocą protokołów szyfrowanych SSL/TLS/IPsec, uwierzytelnianie serwera odbywa się przy użyciu certyfikatów wystawionych i potwierdzonych przez PKI LP.
14. Systemy serwerowe SILP działające pod kontrolą systemów operacyjnych Microsoft Windows muszą posiadać włączoną i aktualną ochronę antywirusową.
15. 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.
16. Aktualizacje systemów serwerowych SILP pracujących z systemami Linux muszą być wykonywane za pośrednictwem dedykowanego systemu dystrybucji uaktualnień zarządzanego przez ZCI. Wymóg ten nie dotyczy systemów Linux stanowiących części systemu LAS.
17. Systemy serwerowe SILP muszą mieć instalowane na bieżąco aktualizacje krytyczne oraz aktualizacje bezpieczeństwa systemów i oprogramowania. W awaryjnych sytuacjach prowadzących do niemożliwości użytkowania dopuszczonego przez LP oprogramowania, dopuszcza się możliwość czasowego wycofania problematycznych poprawek.
18. Zabronione jest podłączanie do sieci LAN PC interfejsów zarządzających serwerów, systemów i urządzeń sieciowych SILP.

19. Serwery, systemy i urządzenia sieciowe oraz dane SILP muszą być zabezpieczone przed:
    19.1. uszkodzeniami mechanicznymi,
    19.2. kradzieżą,
    19.3. pożarem,
    19.4. zanikiem zasilania,
    19.5. wpływami oddziaływań elektrostatycznych i elektrycznych,
    19.6. innymi negatywnymi czynnikami środowiskowymi,
    19.7. dostępem osób niepowołanych.
20. Systemy SILP muszą rejestrować i przechowywać przez co najmniej 3 miesiące lub przekazywać do zewnętrznego dziennika zdarzeń:
    20.1. informacje o wszystkich próbach dostępu użytkowników SILP,
    20.2. informacje o wszystkich próbach dostępu administratorów SILP,
    20.3. informacje o błędach w działaniu systemów i usług,
    20.4. informacje o wszystkich próbach dostępu do działów i usług sieciowych.
21. Systemy SILP mogą mieć uruchomione jedynie usługi i oprogramowanie zgodne z przeznaczeniem systemów.
22. Instalowanie, usuwanie oprogramowania może wykonywać jedynie uprawniony administrator SILP.
23. Zabronione jest instalowanie i używanie oprogramowania bez posiadania wymaganej przez producenta lub autora licencji, pochodzącego z nieznanego źródła, z nośników niesprawdzonych programem antywirusowym, wpływającego negatywnie na pracę SILP.

§ 3.

Bezpieczeństwo stacji roboczych

1. Zasady ogólne
    1.1. Podstawowym systemem uwierzytelniania użytkowników i administratorów na stacjach roboczych SILP jest uwierzytelnianie kartą kryptograficzną i certyfikatem korporacyjnym PKI LP. Jeżeli powyższy sposób uwierzytelniania nie jest możliwy, dopuszcza się uwierzytelnianie w oparciu o system usług katalogowych AD.
    1.2. Dopuszcza się uwierzytelnianie w oparciu o lokalne konto administratora SILP w systemie stacji roboczej. Konto może być użyte jedynie w sytuacjach awaryjnych, gdy inne metody uwierzytelniania nie są możliwe.
    1.3. Użycie innych zasad uwierzytelniania na stacjach roboczych SILP wymaga zatwierdzenia przez naczelnika WI DGLP na wiosek WI.
    1.4. Zabronione jest użycie tego samego hasła do więcej niż jednego konta. Zabrania się używania w Internecie haseł identycznych jak używanych w SILP.
    1.5. Każdy z użytkowników jest odpowiedzialny za operacje w systemach informatycznych wykonywane z użyciem jego identyfikatora.
    1.6. Odchodząc od stacji roboczej użytkownik musi ją zablokować lub wylogować się.
    1.7. Przeglądarki internetowe muszą mieć wyłączoną opcję zapamiętywania identyfikatorów i haseł.
    1.8. PIN do karty kryptograficznej musi zawierać minimum 6 znaków.
2. Aktualizacje
    2.1. Stacje robocze muszą mieć instalowane na bieżąco aktualizacje krytyczne oraz aktualizacje bezpieczeństwa systemów i oprogramowania. W awaryjnych sytuacjach prowadzących do niemożności użytkowania dopuszczonego przez LP oprogramowania, dopuszcza się możliwość czasowego wycofania problematycznych poprawek.
    2.2. 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 sieci WAN LP.
3. Ochrona antywirusowa stacji roboczych z systemem Windows.
    3.1. każda stacja robocza podłączona do sieci WAN LP musi posiadać aktywne oprogramowanie antywirusowe podłączone do dedykowanej konsoli zarządzającej tym oprogramowaniem.

3.2. oprogramowanie antywirusowe musi pracować w trybie skanowania plików i poczty w czasie rzeczywistym.
3.3. przynajmniej raz w miesiącu ma być wykonane pełne skanowanie systemu w sposób automatyczny.
3.4. program antywirusowy musi posiadać aktualną bazę sygnatur wirusów, aktualizowaną co najmniej raz na dzień, w sposób automatyczny.
3.5. użytkownik SILP nie może posiadać uprawnień do wyłączania i deinstalacji programu antywirusowego.
3.6. program antywirusowy może wyłączyć lub dokonać jego deinstalacji jedynie administrator SILP, na czas przeprowadzania czynności administracyjnych, wymagających takiego postępowania.
3.7. każdy elektroniczny nośnik danych pochodzący z zewnątrz, przed jego użyciem należy sprawdzić programem antywirusowym.

4. Instalacja oprogramowania
4.1. instalowanie i usuwanie oprogramowania może wykonywać jedynie administrator SILP.
4.2. zabronione jest instalowanie i używanie oprogramowania bez posiadania wymaganej przez producenta lub autora licencji, pochodzącego z nieznanego źródła, z nośników niesprawdzonych programem antywirusowym, wpływającego negatywnie na pracę sieci lp.
4.3. administrator SILP zobowiązany jest do nadzorowania zgodności instalowanego oprogramowania z posiadanymi licencjami.
4.4. zakupy oprogramowania muszą być dokonywane za wiedzą administratora silp nadleśnictwa.

5. Stanowisko leśniczego
5.1. podstawowym systemem pracy na stanowisku leśniczego jest knx udostępniony przez WI DGLP. używanie innego systemu do pracy na stanowisku leśniczego wymaga zgody naczelnika WI DGLP.
5.2. podstawowym sposobem łączności ze stanowiska leśniczego do sieci wan lp są połączenia ssl VPN przez portal leśniczego https://portal.lesniczego.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 i administratorów SILP oraz komputerów pracujących w sieci WAN LP.
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 umożliwiających 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. Szczegółowe zasady wykonywania kopii bezpieczeństwa określa osobny dokument „Polityka kopii zapasowych SILP" tworzony oraz aktualizowany przez ZCI i zatwierdzany przez naczelnika WI DGLP.

2. Kopie zapasowe danych ze stacji roboczych.
   2.1 za kopie danych ze stacji roboczych odpowiedzialni są użytkownicy stacji roboczych; w przypadku uruchomienia serwera kopii bezpieczeństwa w danej jednostce LP odpowiedzialność za tworzenie i przechowywanie kopii regulują wytyczne właściwych WI.
3. Kopie zapasowe danych systemów sieciowych i serwerowych SILP.
   3.1 Wszystkie produkcyjne systemy sieciowe i serwerowe SILP objęte są wymogiem tworzenia ich kopii zapasowych.
   3.2 Osobą odpowiedzialną za tworzenie i utrzymywanie spisu wykonanych kopii systemów oraz utworzenie i aktualizowanie procedury odtworzenia systemu przy użyciu kopii zapasowej jest:
      3.2.1 administrator SILP odpowiedzialny za dany system – w przypadku, gdy system nie jest objęty zewnętrznym oprogramowaniem odpowiedzialnym za jego kopię,
      3.2.2 administrator zewnętrznego systemu kopii – w przypadku, gdy system jest objęty zewnętrznym oprogramowaniem odpowiedzialnym za jego kopię.
   3.3 Za testowe odtworzenie kopii zapasowej i weryfikację poprawności działania po odtworzeniu systemu SILP odpowiedzialny jest jego Administrator.
4. Kopie bezpieczeństwa systemu LAS.
   4.1 Administrator SILP odpowiedzialny za System LAS tworzy i utrzymuje spis jego kopii bezpieczeństwa.
   4.2 Administrator SILP odpowiedzialny za System LAS tworzy i aktualizuje procedurę odtworzenia systemu z kopii bezpieczeństwa.

§ 6.

Praca w sieci Lasów Państwowych

1. Zasady ogólne
   1.1 stacje robocze podłączone do sieci LP nie mogą mieć włączonych innych połączeń transmisji danych.
   1.2 dopuszcza się dostęp do wewnętrznych zasobów SILP za pośrednictwem dedykowanych dla LP usług pakietowych transmisji danych Access Point Name (APN), dostarczanych przez operatorów sieci komórkowych, przy spełnieniu wymagań:
      1.2.1 elementy umożliwiające dostęp do usług APN tj. karta SIM, urządzenie mobilne muszą być własnością LP.
      1.2.2 adresację IP urządzeń w sieci APN ustala WI DGLP.
      1.2.3 w przypadku połączenia sieci APN do sieci LP poprzez sieć Internet wymagane jest użycie tunelu VPN typu site-to-site.
   1.3 dopuszcza się dostęp zdalny VPN z sieci Internet do wewnętrznych zasobów SILP. Warunki i sposób dostępu zostały określone w punkcie „Dostęp zdalny VPN do zasobów SILP.
   1.4 zabrania się fizycznego podłączenia do sieci LP komputerów nie będących własnością Lasów Państwowych, bez zgody właściwych WI.
   1.5 w przypadku pojawienia się w sieci LP ruch zaburzającego prawidłowe działanie SILP lub świadczącego o infekcji stacji roboczej, serwera lub systemu sieciowego SILP, ZCI może zablokować cały ruch pochodzący z danego źródła.
2. Adresacja urządzeń w sieci LP
   2.1 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.
   2.2 z każdej sieci LAN PC musi być dostępny serwer DHCP przyznający adresacje dla stacji roboczych.
   2.3 w sieci WAN LP zabronione jest używanie translacji i maskowania adresów IP (NAT, PAT, Proxy itp.).
   2.4 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.
   3.1 ruch wewnętrzny sieci WAN LP polega ograniczeniom w celu ochrony zasobów SILP przed nieuprawnionym dostępem.
   3.2 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.
   3.3 zmiany polityk dla ruch w sieci WAN LP wprowadzane są przez ZCI na zatwierdzony przez naczelnika WI DGLP wniosek od właściwych WI.
   3.4 polityki dla ruch w sieci WAN LP realizowane są na znajdujących się w nadleśnictwie urządzeniach będących własnością LP. Za implementacje polityk na urządzeniach w sieci WAN LP odpowiada ZCI.
4. Sieci bezprzewodowe WiFi
   4.1 sieci LAN jednostek LP mogą być budowane w oparciu o bezprzewodowe sieci komputerowe Wi-Fi.
   4.2 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.
   4.3 sieci bezprzewodowe muszą używać szyfrowania WPA2 AES.
   4.5 za pośrednictwem sieci bezprzewodowych można realizować dostęp użytkowników SILP do sieci LP przy spełnieniu wymagań:
      4.5.1 uwierzytelnienie dostępu zostanie wykonane w oparciu o certyfikat wystawiony przez PKI LP.
      4.5.2 do uwierzytelnienia dostępu wykorzystany jest standard IEEE 802.1X oraz centralne serwery radius utrzymywane przez ZCI.
      4.5.3 po uwierzytelnieniu użytkownik SILP otrzyma za pośrednictwem DHCP adresację sieci LAN jednostki i dostęp do sieci LP identyczny, jak stacje z dostępem przewodowym.
      4.5.4 w przypadku awarii i braku możliwości komunikacji z centralnym serwerem radius, możliwe jest uwierzytelnienie dostępu do sieci bezprzewodowej za pomocą dedykowanego awaryjnego identyfikatora sieci.
5. Za pośrednictwem sieci bezprzewodowych można realizować dostęp gościnny do Internetu z urządzeń nie będących własnością LP, przy spełnieniu wymagań:
   5.1 uwierzytelnienie dostępu odbywa się za pośrednictwem jednorazowych kodów i portalu dla dostępu gościnnego. Kody generowane są przez osobę wyznaczoną przez kierownika nadleśnictwa lub będą dostarczane do jednostki przez właściwe WI.
   5.2 dostęp będzie możliwy jedynie po akceptacji regulaminu określającego zasady dostępu.
   5.3 ruch z sieci dla dostępu gościnnego przesyłany jest tunelem pomiędzy ruterem brzegowym jednostki a urządzeniem terminującym, w centralnym węźle sieciowym centralnym CP.

§ 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
   2.1 Pracownicy jednostek organizacyjnych Lasów Państwowych.
   2.2 Pozostali użytkownicy SILP.
3. Każdy uprawniony do posiadania konta pocztowego posiada tylko jedne imienne konto pocztowe w systemie poczty elektronicznej LP, we właściwej domenie, zgodnie z „Projektem usług katalogowych PGL LP".
4. System poczty elektronicznej posiada mechanizmy zabezpieczające przed nieautoryzowanym dostępem przez osoby trzecie.

5. Dostęp do konta pocztowego jest chroniony hasłem. Hasło stanowi zabezpieczenie dostępu do systemu oraz treści wiadomości przechowywanych na koncie pocztowym.
6. Zabronione jest udostępnianie przez użytkowników konta pocztowego lub danych dostępowych do konta pocztowego osobom nieupoważnionym.
7. W systemie poczty Lasów Państwowych funkcjonują tylko imienne konta pocztowe oraz nieimienne konta specjalne tworzone za zgodą naczelnika WI DGLP.
8. Każdy uprawniony posiadający konto pocztowe oraz kartę kryptograficzną PKI LP może wystąpić do administratora PKI LP o certyfikat do szyfrowania i podpisywania poczty elektronicznej, który umożliwi szyfrowanie, deszyfrowanie i jednoznaczne potwierdzenie autentyczności wysyłanej oraz odbieranej poczty.
9. 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.
10. Użytkownicy kont pocztowych zawartych w domenie LP muszą przestrzegać „Regulaminu użytkowania systemu poczty elektronicznej LP".
11. Aktualny „Regulamin użytkowania systemu poczty elektronicznej LP" publikowany jest pod adresem http://poczta.lasy.gov.pl/regulamin.
12. Regulamin tworzy oraz aktualizuje ZCI i zatwierdza naczelnik WI DGLP. Wszelkie zmiany Regulaminu zaczynają obowiązywać z momentem ich opublikowania. Użytkownicy są informowani o zmianach Regulaminu poprzez wiadomości poczty elektronicznej.
13. W przypadku naruszenia przez użytkownika „Regulaminu użytkowania systemu poczty elektronicznej LP", administrator SILP systemu poczty elektronicznej LP ma prawo zablokowania konta pocztowego.

§ 8.

Praca w sieci Internet i styk z Internetem

1. Dostęp da sieci Internet z sieci WAN LP realizowany jest jedynie za pośrednictwem węzła centralnego w CP. Zabrania się łączenia sieci LAN jednostek organizacyjnych LP z zewnętrznymi sieciami komputerowymi inaczej, niż za pośrednictwem węzła centralnego.
2. W sytuacji awarii styku z Internetem w CP, dopuszcza się realizację dostępu do sieci Internet poprzez zapasowy węzeł internetowy w CZ.
3. 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 ruch na styku WAN LP i Internet", tworzony oraz aktualizowany przez ZCI i zatwierdzany przez naczelnika WI DGLP.
4. Na styku sieci WAN LP i Internet dozwolony jest ruch szyfrowany jedynie do ustalonej listy adresów sieciowych. Naczelnik WI DGLP zatwierdza listę adresów w dokumencie „Polityka dla ruchu na styku sieci WAN LP i Internet". Ruch do adresów spoza ustalonej listy może być deszyfrowany lub zablokowany. Użytkownik SILP może za pośrednictwem właściwych WI wnioskować o dodanie adresów do listy zezwalającej na szyfrowany ruch.
5. Zmiany polityk dla ruch na styku sieci WAN LP i Internet wprowadzane są przez ZCI na zatwierdzony przez naczelnika WI DGLP wniosek od właściwych WI.
6. Polityki dla ruchu na styku sieci WAN LP i Internet realizowane są na centralnych systemach zabezpieczeń sieciowych będących własnością PGL LP.
7. Za implementacje polityk dla ruchu na styku sieci WAN LP i Internet odpowiada ZCI.

§ 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 nadleśnictwa ma prawo posiadać dostęp zdalny VPN do SILP, z uprawnieniami jakie posiada w sieci LAN PC nadleśnictwa, po otrzymaniu pisemnej zgody Nadleśniczego i przekazaniu stosownego wniosku do WI odpowiedzialnych za utworzenie dostępu z zachowaniem drogi służbowej.

3. Dostęp zdalny VPN do SILP dla pracowników nadleśnictwa jest dozwolony jedynie z urządzeń 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 firm lub instytucji zewnętrznych może zostać przydzielony na zatwierdzony przez naczelnika WI DGLP wniosek od WI. Dostęp do zasobów SILP może być przydzielony jedynie w przypadku, gdy z firmą zewnętrzną została podpisana umowa wymagającej takiego dostępu, przy spełnieniu następujących warunków:
   5.1 dostęp będzie możliwy jedynie na czas obowiązywania umowy,
   5.2 firma zewnętrzna podpisze oświadczenie o zasadach udzielania dostępu.
6. Dostęp zdalny VPN do SILP jest realizowany przy spełnieniu następujących warunków:
   6.1 uwierzytelnienie i autoryzacja następuje w oparciu o certyfikat wystawiony przez pki lp lub imienne konta ad założone zgodnie z „projektem usług katalogowych PGL LP".
   6.2 dostęp zapewnia poufności i integralność przesyłanych danych oraz wzajemne uwierzytelnienie obu stron połączenia.
   6.3 tunel VPN jest terminowany na centralnym koncentratorze VPN znajdującym się w CP.
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:
   7.1 dostęp będzie możliwy jedynie na czas obowiązywania umowy,
   7.2 firma zewnętrzna podpisze oświadczenie o zasadach udzielania dostępu.
8. Stały dostęp zdalny VPN typu site-to-site może zostać wykonany za pośrednictwem sieci Internet w jednostkach 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:
   8.1 dostęp zdalny vpn typu site-to-site dla jednostek lp musi zapewniać poufność i integralność przesyłanych danych oraz wzajemne uwierzytelnienie obu stron połączenia.
   8.2 tunel VPN po stronie lokalizacji zdalnej lp terminowany jest na dedykowanym urządzeniu szyfrującym, po stronie sieci lp tunel terminowany jest centrum podstawowym przetwarzania danych w DGLP.
   8.3 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 adresacje z zakresu sieci 172.16.0.0/12 przydzieloną przez ZCI.
   8.4 cały ruch z sieci lokalnej podłączonej lokalizacji zdalnej kierowany jest do tunelu VPN.
   8.5 polityki dostępu z sieci lokalizacji zdalnej do sieci WAN LP i do sieci Internet implementowane i realizowane są na centralnym koncentratorze VPN.
   8.6 szczegółowe parametry i konfiguracje tunelu dostępu zdalnego VPN ustala i wykonuje ZCI.
   8.7 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.

8.8 sieci LAN części biurowej i sal szkoleniowych powinny posiadać niezależne adresacje z zakresu sieci 172.16.0.0/12 przydzielone przez ZCI.

8.9 dopuszczone jest wykorzystanie zainstalowanego na potrzeby vpn łącza internetowego, również jako 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 p[od warunkami:

8.9.1 separacja sieci LAN dla części hotelowej za pomocą osobnego przełącznika lub przy użyciu przełącznika zarządzanego i osobnego VLAN.

8.9.2 posiadania na łączu dodatkowego stałego publicznego adresu IP, innego niż używany do terminowania tunelu VPN, na który będą translowane połączenia wychodzące do sieci Internet.

8.10 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.

Internetowe i Intranetowe usługi SILP

1. W sieci LP funkcjonują następujące usługi:
   1.1 System Las,
   1.2 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,
   1.3 PKI LP – infrastruktura klucza publicznego Lasów Państwowych utrzymywana w ramach wewnętrznych zasobów SILP,
   1.4 Poczta elektroniczna – każdy pracownik LP zarejestrowany w usłudze katalogowej musi posiadać imienne konto pocztowe,
   1.5 Witryny informacyjne www – nadleśnictwo zobowiązane jest do utrzymywania własnej witryny informacyjnej www w domenie lasy.gov.pl na portalu korporacyjnym LP,
   1.6 Centralny system zarządzania telefonią IP – Cisco Unified Communications Manager,
   1.7 Elektroniczne Zarządzanie Dokumentacją – system elektronicznego obiegu dokumentów,
   1.8 Komunikator intranetowy zatwierdzony przez WI DGLP – każdy użytkownik usługi katalogowej automatycznie uzyskuje dostęp do tej usługi,
   1.9 Serwis dystrybucji poprawek i aktualizacji systemów firmy Microsoft.
2. Na wniosek naczelnika komórki organizacyjnej DGLP właściwej do spraw informatyki, Dyrektor Generalny Lasów Państwowych zatwierdza uruchomienie innych globalnych obligatoryjnych usług sieciowych WAN LP.
3. Za prawidłowe funkcjonowanie serwerów usług internetowych i intranetowych LP odpowiedzialne są WI utrzymujące dany serwer oraz usługę.
4. Zasady funkcjonowania i korzystania z usług internetowych i intranetowych LP regulują osobne dokumenty techniczne zatwierdzane przez naczelnika WI DGLP.

§ 11.

Urządzenia mobilne

Urządzenia mobilne będące własnością LP, służące do przetwarzania i przechowywania danych SILP, stanowiących tajemnice przedsiębiorstwa, podlegają wymaganiom:

1. Urządzenie musi mieć włączoną aktywną kontrolę dostępu (np. PIN, wzór blokady, hasło).
2. Jeżeli system urządzenia posiada możliwość uruchomienia ochrony antywirusowej, urządzenie musi mieć aktywną i aktualną ochronę.
3. Urządzenia muszą mieć instalowane na bieżąco krytyczne aktualizacje systemów i używanego oprogramowania.

4. Wymagane jest zaszyfrowanie przestrzeni służącej do przechowywania danych SILP, stanowiących tajemnice przedsiębiorstwa.
5. Dostęp do sieci WAN LP z urządzeń mobilnych, realizowany jest za pośrednictwem połączeń VPN lub dedykowanych dla LP usług pakietowych transmisji danych Access Point Name (APN).
6. Urządzenia mobilne służące do przetwarzania i przechowywania danych SILP inne niż przenośne komputery PC, powinny być zarządzane za pomocą dedykowanego oprogramowania umożliwiającego:
   6.1 prowadzenie rejestru urządzeń,
   6.2 prowadzenie rejestru i kontrolę instalowanego oprogramowania,
   6.3 zdalne wyłączanie, usuwanie danych i blokowanie dostępu do urządzenia,
   6.4 tworzenie kopii zapasowej danych.
7. Urządzenia mobilne służące do przetwarzania i przechowywania danych SILP należy odpowiednio zabezpieczyć fizycznie przed kradzieżą, zwłaszcza urządzenia pozostawiane w samochodach oraz innych środkach transportu, pokojach hotelowych , centrach konferencyjnych i miejscach spotkań.

III. Zasady udostępniania baz systemu LAS

§ 1.

1. Przez dostęp do danych systemu LAS rozumie się:
   1.1 zalogowanie się do bazy danych w danej jednostce organizacyjnej LP,
   1.2 pobieranie danych z bazy danych LAS z zastosowaniem technik intranetowych.
2. Dostęp do danych systemu LAS nadleśnictwa może być realizowany w trybie:
   2.1 dostępu stałego,
   2.2 dostępu tymczasowego.
3. Dostęp stały do danych systemu LAS może być realizowany dla:
   3.1 osób zatrudnionych w nadleśnictwie wyłącznie na podstawie udokumentowanej dyspozycji nadleśniczego, określającej:
      3.1.1 zasoby danych,
      3.1.2 zakres uprawnień dostępu do danych.
   3.2 osób zatrudnionych w jednostce nadrzędnej, w ramach sprawowania nadzoru, na podstawie udokumentowanej dyspozycji kierownika tej jednostki, określającej zasoby danych jednostki nadzorowanej.
4. Dostęp tymczasowy do danych systemu LAS może być realizowany dla:
   4.1 osób zatrudnionych w nadleśnictwie na czas określony, wyłącznie na podstawie udokumentowanej dyspozycji nadleśniczego, określającej:
      4.1.1 zasoby danych,
      4.1.2 zakres uprawnień dostępu do danych,
      4.1.3 datę odebrania uprawnień.
   4.2 osób zatrudnionych w jednostce nadrzędnej, ramach sprawowania nadzoru na podstawie udokumentowanej dyspozycji kierownika tej jednostki, określającej:
      4.2.1 zasoby danych jednostki nadzorowanej,
      4.2.2 datę odebrania uprawnień.
   4.3 pracowników IPL na podstawie pisemnego upoważnienia do przeprowadzenia kontroli, z zachowaniem postanowień zawartych w § 2.
   4.4 członków zespołów zadaniowych powołanych zarządzeniem lub decyzją Dyrektora Generalnego LP, posiadających uprawnienia o dostępie do danych systemu Las jednostek nadzorowanych, określone w akcie powołania zespołu.
   4.5 członków zespołów zadaniowych powołanych zarządzeniem lub decyzja Dyrektora Regionalnego LP, posiadających uprawnienia o dostępie do danych systemu LAS jednostek nadzorowanych, określone w akcie powołania zespołu.
   4.6 innych osób, niż pracownicy jednostek organizacyjnych Lasów Państwowych, według zasad określonych odrębnymi umowami.
5. Rozwiązanie stosunku pracy z pracownikiem posiadającym dostęp do danych Systemu LAS, skutkuje odebraniem uprawnień dostępu. Komórka organizacyjna, w kompetencji

której są sprawy kadrowe, ustala datę i czas odebrania uprawnień i powiadamia komórkę WI.

6. Postanowienia ustępu 5 obowiązują w stosownym zakresie przy zmianie stanowiska pracy, zakresu czynności, czy też innych decyzjach kadrowych, mających wpływ na pisemnie udokumentowaną konieczność weryfikacji praw dostępu do danych systemu LAS. Z wnioskiem o zmianę uprawnień występuje do nadleśniczego bezpośredni przełożony pracownika.
7. Za realizację postanowień ust. 3, ust. 4, ust. 5 i ust. 6 odpowiada Nadleśniczy lub osoby przez niego upoważnione.

§ 2.

1. Przez udostępnienie danych systemu Las nadleśnictwa inspektorowi LP rozumie się:
   1.1 odblokowanie użytkownika grupowego w systemie LAS przez administratora nadleśnictwa, z zakresem dostępu zdefiniowanym w upoważnieniu do przeprowadzenia kontroli,
   1.2 udostępnienie danych w formie raportu zdefiniowanego wcześniej przez kontrolującego.
2. Pracownicy jednostek nadzorujących kontrolę danych systemu LAS w nadleśnictwie mogą realizować w trybie dostępu stałego lub tymczasowego, w zakresie uprawnień określonych przez kierownika jednostki nadzorującej.
3. Pracownicy jednostek nadzorujących oraz ILP mogą posiadać wyłącznie uprawnienia do przeglądania danych systemu LAS nadleśnictwa.

§ 3.

1. Administrator systemu LAS w nadleśnictwie, na polecenie Nadleśniczego, umożliwia dostęp do zasobów danych systemu pracownikowi ILP lub pracownikowi jednostki nadzorującej.
2. W uzgodnieniu z Nadleśniczym, dopuszcza się w szczególnych sytuacjach, umożliwienie dostępu do danych systemu LAS nadleśnictwa pracownikowi ILP lub pracownikowi jednostki nadzorującej przez administratorów regionalnych lub administratorów centralnych. W tym przypadku konieczne jest powiadomienie administratora nadleśnictwa o takim zdarzeniu.
3. Administrator systemu w nadleśnictwie – po zakończeniu czynności związanych z tymczasowym udostępnieniem danych systemu LAS pracownikowi ILP lub pracownikowi jednostki nadzorującej, blokuje dostęp do zasobów.

§ 4.

1. Przepisy zawarte w § 1. do § 3. nie dotyczą pracowników WI w ramach wykonywania czynności administracyjnych.
2. W celu zapewnienia poprawności funkcjonowania SILP pracownicy wymienieni w ust. 1 mogą mieć pełny dostęp do baz informatycznych nadleśnictwa.
3. WI prowadzą ewidencję wniosków, nadawanych uprawnień restrykcyjnych.
4. Nadleśnictwo prowadzi nadzór zmian wykonanych na bazie danych. Zmiany na bazie danych wykonywane są za akceptacją Głównego Księgowego.
5. Administrator w nadleśnictwie prowadzi ewidencję dokumentów źródłowych związanych z udostępnianiem stałym i tymczasowym danych systemu LAS.

§ 5.

1. Na potrzeby szkoleń, nauki zawodu, testów rozwojowych systemu LAS, oraz na potrzeby realizacji tematów badawczych zleconych przez LP, administrator bazy danych, w ramach posiadanych uprawnień w środowisku centralnym, wykonuje i udostępnia kopię danych przygotowaną w sposób uniemożliwiający identyfikację danych osobowych i płacowo kadrowych. Udostępnienie kopii danych przez administratora jest poprzedzone otrzymaniem wytycznych z DGLP lub od administratora danych (kierownika jednostki), ze wskazaniem zakresu udostępnianych danych.
2. Kopia danych systemu LAS jednostki organizacyjnej Lasów Państwowych może być udostępniona członkowi zespołu zadaniowego tworzącego na zlecenie DGLP oprogramowanie raportujące, sprawozdawcze lub inne oraz wykonującego diagnostykę działania systemu LAS.

IV. Zasady funkcjonowania systemu telefonii IP i wideokonferencji

§ 1.

Zasady ogólne

1. Telefony IP w sieci LP są obsługiwane przez centralny system zarządzający telefonią.
2. Terminale wideo a sieci LP są obsługiwane przez centralny system zarządzający telefonią oraz system zarządzający wideokonferencjami.
3. Dedykowanymi protokołami sygnalizacyjnymi dla telefonów IP oraz terminali wideo są SCCP lub SIP.
4. Telefony IP oraz terminale wideo w jednostkach organizacyjnych LP powinny znajdować się w wydzielonym VLAN o ID 200.
5. Adresacja IP dla VLAN-ów tworzona jest wg schematu 10.R.200+N.0/24 gdzie:
   5.1. R – numer 1-17 dla RDLP lub 18 dla DGLP i zakładów o zasięgu krajowym,
   5.2. N – numer jednostki podległej RDLP lub zakładu o zasięgu krajowym.
6. Katalog użytkowników systemu telefonii IP jest zsynchronizowany z usługą katalogową Active Directory.
7. Katalog użytkowników systemu wideokonferencji jest synchronizowany z katalogiem użytkowników systemu telefonii IP.
8. Nr telefonu IP wprowadzany jest w Active Directory zgodnie ze schematem opisu pól określonym w Projekcie usług katalogowych PGL LP.

§ 2.

Plan numeracyjny

1. Numer telefonu w systemie IP Lasów Państwowych tworzony jest wg schematu RRNNXXY, gdzie:
   1.1. RR – numer RDLP/DGLP
   31 – RDLP Białystok
   32 – RDLP Katowice
   33 – RDLP Kraków
   34 – RDLP Krosno
   35 – RDLP Lublin
   36 – RDLP Łódź
   37 – RDLP Olsztyn
   38 – RDLP Piła
   39 – RDLP Poznań
   10 – RDLP Szczecin
   11 – RDLP Szczecinek
   12 – RDLP Toruń
   13 – RDLP Wrocław
   14 – RDLP Zielona Góra
   15 – RDLP Gdańsk
   16 – RDLP Radom
   17 – RDLP Warszawa
   18 – DGLP
   1.2. NN – numer RDLP [71], nadleśnictwa lub zakładu
   1.3. XXY – numer wewnętrzny telefonu w jednostce.
2. Numer pokoju wideokonferencyjnego (pokoju CMR) przypisanego do konta osoby zarządzającej wideokonferencjami w nadleśnictwie tworzony jest wg schematu 5RRNN450, gdzie:
   2.1. RR – numer RDLP/DGLP
   31 – RDLP Białystok
   32 – RDLP Katowice
   33 – RDLP Kraków
   34 – RDLP Krosno
   35 – RDLP Lublin
   36 – RDLP Łódź
   37 – RDLP Olsztyn
   38 – RDLP Piła
   39 – RDLP Poznań
   10 – RDLP Szczecin
   11 – RDLP Szczecinek
   12 – RDLP Toruń
   13 – RDLP Wrocław
   14 – RDLP Zielona Góra
   15 – RDLP Gdańsk
   16 – RDLP Radom
   17 – RDLP Warszawa
   18 – DGLP
   2.2. NN – numer RDLP [71], nadleśnictwa lub zakładu
   2.3. XXY – numer wewnętrzny telefonu w jednostce.
3. Numer pokoju wideokonferencyjnego dla konferencji planowanych tworzony jest automatycznie przez system zarządzający wideokonferencjami według schematu 58XX.

4. Numer pokoju wideokonferencyjnego dla konferencji rendez-vous tworzony jest przez system zarządzający wideokonferencjami według schematu 57XX
5. Plan numeracyjny dla numerów wewnętrznych RDLP
   5.1. zarezerwowane numery wewnętrzne i zakresy - XXY:
      5.1.1. 100- Sekretariat/operator
      5.1.2. 101 – Drugi sekretariat/ operator
      5.1.3. 102 – 109 Faksy
      5.1.4. 121 – Dyrektor RDLP
      5.1.5. 311 – Zastępca Dyrektora ds.gospopdarki leśnej
      5.1.6. 411 – Zastępca Dyrektora ds.rozwoju
      5.1.7. 450 – Terminal wideo
      5.1.8. 511 – Zastępca Dyrektora ds.ekonomicznych
      5.1.9. 611 – Główny Księgowy,
      5.1.10. 600 – Kasa
      5.1.11. 200 – Portiernia
      5.1.12. 800 – 899 zarezerwowane na funkcje systemowe
   5.2. numery wewnętrzne i zakresy w RDLP – XXY,
      gdzie XX – numer przypisany do komórki organizacyjnej RDLP
      22.1.1. 12 – Gabinet Dyrektora RDLP
      22.1.2. 13 – Organizacja i Kadry
      22.1.3. 15 – Kontrola i Audyt Wewnętrzny
      22.1.4. 17 – Radca Prawny
      22.1.5. 19 – Obronność i ochrona mienia
      22.1.6. 21 – Rzecznik Prasowy/Promocja i media
      22.1.7. 22 – Stanowiska wydzielone np..stanowisko ds. BHP, ds. UE itp.
      22.1.8. 31 – Gabinet z-cy Dyrektora ds. gospodarki leśnej
      22.1.9. 33 – Gospodarowanie Ekosystemami
      22.1.10. 34 – Ochrona Ekosystemów
      22.1.11. 37 – Zarządzanie Zasobami Leśnymi
      22.1.12. 38 – Rozwój i Innowacje
      22.1.13. 41 – Gabinet z-cy dyrektora ds. rozwoju
      22.1.14. 51 – Gabinet z-cy Dyrektora ds.ekonomicznych
      22.1.15. 53 – Gospodarka Drewnem
      22.1.16. 55 – Administracja
      22.1.17. 57 – Informatyka
      22.1.18. 61 – Księgowość
      22.1.19. 65 – Analizy i Planowanie
      22.1.20. 70 -79 – pozostałe
      Y – numer użytkownika wewnątrz komórki organizacyjnej.
6. Plan numeracyjny dla numerów wewnętrznych nadleśnictwa
   6.1. zarezerwowane numery wewnętrzne i zakresy - XXY
      6.1.1. 100 - Sekretariat/operator
      6.1.2. 101 - Drugi sekretariat/ operator
      6.1.3. 102 - 109 Faksy
      6.1.4. 121 - Nadleśniczy
      6.1.5. 311 - Zastępca nadleśniczego
      6.1.6. 611 - Główny Księgowy
      6.1.7. 219 - Inżynier Nadzoru
      6.1.8. 671 - Sekretarz
      6.1.9. 211 - Rzecznik prasowy
      6.1.10. 571 - Administrator
      6.1.11. 600 - Kasa
      6.1.12. 200 - Portiernia
      6.1.13. 444 - PAD
      6.1.14. 800-899 – Zarezerwowane na funkcje systemowe.

6.2. numery wewnętrzne i zakresy w jednostce XXY,
gdzie XX – numer przypisany do komórki organizacyjnej nadleśnictwa:
6.2.1. 12 – gabinet nadleśniczego
6.2.2. 13 – stanowisko ds. pracowniczych
6.2.3. 17 – Radca Prawny
6.2.4. 21 – Inżynier Nadzoru
6.2.5. 22 – Straż Leśna
6.2.6. 31 – Gabinet Z-cy nadleśniczego
6.2.7. 33 – Dział Gospodarki Leśnej
6.2.8. 57 – Administrator systemu informatycznego
6.2.9. 61 – Dział Finansowo-Księgowy
6.2.10. 67 – Dział Administracyjno-Gospodarczy
6.2.11. 68 – Stanowisko ds. Edukacji Leśnej
6.2.12. 70 -79 – pozostałe
Y – numer użytkownika wewnątrz komórki organizacyjnej

7. Plan numeracyjny dla numerów wewnętrznych zakładu
7.1. zarezerwowane numery wewnętrzne i zakresy - XXY:
7.1.1. 100 – Sekretariat ogólny/operator
7.1.2. 101 – Drugi sekretariat /operator
7.1.3. 102-109 – Faksy
7.1.4. 121 – Dyrektor
7.1.5. 311 – Zastępca Dyrektora
7.1.6. 611 – Główny Księgowy
7.1.7. 211 – Rzecznik prasowy
7.1.8. 571 – Administrator
7.1.9. 600 – kasa
7.1.10. 00 – portiernia
7.1.11. 800 do 899 – zarezerwowane na funkcje systemowe
7.2. numery wewnętrzne i zakresy w jednostce - XXY,
gdzie XX – numer przypisany do komórki organizacyjnej zakładu:
7.2.1. 12 – Gabinet dyrektora
7.2.2. 13 – Stanowisko ds. pracowniczych
7.2.3. 17 – Radca Prawny
7.2.4. 31 – Gabinet zastępcy dyrektora
7.2.5. 57 – Administrator systemu informatycznego
7.2.6. 61 – Dział Finansowo-Księgowy
7.2.7. 67 – Dział Administracyjno-Gospodarczy
7.2.8. 70 -79 – pozostałe
Y – numer użytkownika wewnątrz komórki organizacyjnej.

§ 3.

Uprawnienia użytkowników systemu telefonii IP

1. Wydzielone są trzy podstawowe grupy uprawnień do wykonywania połączeń przez użytkowników:
1.1 tylko numery wewnątrz sieci telefonii IP LP,
1.2 numery wewnątrz sieci telefonii IP LP i krajowe numery zewnętrzne,
1.3 numery wewnątrz sieci telefonii IP LP i krajowe numery zewnętrzne i międzynarodowe.
2. Każdy użytkownik telefonii IP ma możliwość wykonywania połączeń na numery alarmowe oraz specjalne (8XX).
3. Nadleśniczy może nadać bardziej szczegółowe uprawnienia dla wskazanych użytkowników.

V. Wzór oświadczenia pracownika

OŚWIADCZENIE PRACOWNIKA

Miejscowość ....., ... dnia .....I.....I..

Imię i Nazwisko:.....
Adres zamieszkania:.....
Świadoma/y odpowiedzialności karnej, cywilnej i służbowej, wynikającej z przepisów prawa dotyczących ochrony danych osobowych, ochrony informacji niejawnych, kodeksu pracy, kodeksu cywilnego, kodeksu karnego oraz regulaminu pracy w jednostce organizacyjnej LP niniejszym:

1. Przyjmuję do wiadomości, że połączenia telefoniczne, e-maile oraz korzystanie z Internetu mogą być monitorowane.
2. Zobowiązuję się do:
   - Przestrzegania ,,Zasad bezpiecznej eksploatacji zasobów informatycznych Lasów Państwowych" i powstrzymania się od jakichkolwiek działań z Zasadami niezgodnych, bądź przez Zasady nieprzewidzianych.
   - Przestrzegania ,,Regulaminu użytkowania Konta Pocztowego LP".
   - Zachowania w tajemnicy wszelkich danych, o których użytkownik posiadł wiedzę korzystając z systemu informatycznego Lasów Państwowych.
   - Zachowania w tajemnicy danych, które mogłyby umożliwić osobom niepowołanym dostęp do systemu informatycznego Lasów Państwowych, w szczególności: identyfikatorów, haseł, nazw komputerów i numerów IP.
   - Powstrzymania się od jakichkolwiek prób przełamywania zabezpieczeń systemów informatycznych oraz powiadamiania przełożonych o wszelkich zachowaniach lub zjawiskach, które mogłyby świadczyć o próbie przełamania bądź przełamaniu tych zabezpieczeń.
   - Pokrycia wszelkich start i szkód, jakie faktycznie odniosły Lasy Państwowe na skutek nieprzestrzegania Zasad lub niewypełnienia któregokolwiek z powyższych zobowiązań."

Zielona Góra, dn.....20..... r.

Zielona Góra, dnia 31. grudnia 2020 r.

Zatwierdzam:
Nadleśniczy

Maciej Taborski