Zarządzenie nr 135
Dyrektora Generalnego Lasów Państwowych
z dnia 21 listopada 2024 r.

w sprawie zmiany Zarządzenia nr 31 Dyrektora Generalnego Lasów Państwowych z dnia 18 września 2017 r. w sprawie zasad funkcjonowania i zasad bezpieczeństwa systemu informatycznego w Państwowym Gospodarstwie Leśnym Lasy Państwowe

(znak: EI.0413.28.2024)

Na podstawie art. 33 ust. 1 ustawy z dnia 28 września 1991 r. o lasach (t.j. Dz. U. z 2024 r. poz. 530; zm. Dz. U. z 2024 r. poz. 1473) oraz § 6 Statutu Państwowego Gospodarstwa Leśnego Lasy Państwowe, wprowadzonego zarządzeniem nr 50 Ministra Ochrony Środowiska, Zasobów Naturalnych i Leśnictwa z dnia 18 maja 1994 r. – w wykonaniu zadań Dyrektora Generalnego Lasów Państwowych, wynikających z realizacji jego uprawnienia określonego w § 8 ust. 1 pkt 6 ww. statutu oraz art. 33 ust. 3 pkt 8 ustawy o lasach, zarządzam, co następuje:

§ 1

Zmienia się treść załącznika nr 2 do Zarządzenia nr 31 Dyrektora Generalnego Lasów Państwowych z dnia 18 września 2017 w sprawie zasad funkcjonowania i zasad bezpieczeństwa systemu informatycznego w Państwowym Gospodarstwie Leśnym Lasy Państwowe, który przyjmuje brzmienie:

„Załącznik nr 2 do Zarządzenia nr 31
Dyrektora Generalnego Lasów Państwowych
z dnia 18 września 2017 r.

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 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 oprogramowania użytkowego 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.
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 usunąć te 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. Dopuszcza się czasowe odstąpienie od aktualizacji, w szczególnych przypadkach, skutkujących brakiem możliwości użytkowania oprogramowania stosowanego w LP.
19. Sieć komputerowa w jednostkach organizacyjnych LP opiera się o model zgodny z „Projektem usług katalogowych PGL LP" zatwierdzonym przez naczelnika WI DGLP.
20. Za utrzymanie, konserwację i prawidłowe działanie systemów informatycznych odpowiadają administratorzy SILP.
21. 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 karty kryptograficznej i certyfikatu korporacyjnego PKI LP lub haseł jednorazowych.
2. Systemy wewnętrznych zasobów 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 i uwierzytelnianie za ich pomocą administratorów SILP w krytycznych, ze względu na działanie SILP, elementach infrastruktury.
5. Dopuszcza się zakładanie lokalnych 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 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 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:

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 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 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.
14. Systemy serwerowe SILP działające pod kontrolą systemów operacyjnych Microsoft Windows muszą posiadać włączoną i aktualną ochronę antywirusową:
    1) program antywirusowy musi posiadać aktualną bazę sygnatur wirusów aktualizowaną co najmniej raz na dzień, w sposób automatyczny;
    2) oprogramowanie antywirusowe musi pracować w trybie skanowania plików w czasie rzeczywistym;
    3) przynajmniej raz na miesiąc musi być wykonywane pełne skanowanie systemu w sposób automatyczny.

15. Dopuszcza się brak ochrony antywirusowej, w szczególnych przypadkach skutkujących brakiem możliwości użytkowania oprogramowania stosowanego w LP.
16. 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.
17. Zabronione jest podłączanie do sieci LAN PC interfejsów zarządzających serwerów, systemów i urządzeń sieciowych SILP.
18. 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.
19. Systemy SILP muszą rejestrować i przechowywać przez co najmniej 3 miesiące lub przekazywać do zewnętrznego dziennika zdarzeń:
    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.
20. Systemy SILP mogą mieć uruchomione jedynie usługi i oprogramowanie zgodne z przeznaczeniem systemów.
21. Instalowanie oraz usuwanie oprogramowania może wykonywać jedynie uprawniony administrator SILP lub firma zewnętrzna świadcząca serwis.
22. Zabronione jest instalowanie i używanie oprogramowania:
    1) bez posiadania wymaganej przez producenta lub autora licencji;
    2) pochodzącego z nieznanego źródła;
    3) z nośników innych niż oryginalne nośniki producenta, które nie zostały sprawdzone programem antywirusowym;
    4) wpływającego negatywnie na pracę SILP.

§ 3.
Bezpieczeństwo stacji roboczych

1. Zasady ogólne:
    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;
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. 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. W przypadku instalacji aktualizacji wymagającej restartu systemu, administrator lub użytkownik SILP niezwłocznie wykona restart.
3. Ochrona antywirusowa stacji roboczych z systemem Windows:
   1) każda stacja robocza podłączona do sieci WAN LP musi posiadać aktywne oprogramowanie antywirusowe podłączone do dedykowanej konsoli zarządzającej tym oprogramowaniem;
   2) oprogramowanie antywirusowe musi pracować w trybie skanowania plików i poczty w czasie rzeczywistym;
   3) przynajmniej raz na miesiąc ma być wykonywane pełne skanowanie systemu w sposób automatyczny;
   4) program antywirusowy musi posiadać aktualną bazę sygnatur wirusów, aktualizowaną co najmniej raz na dzień, w sposób automatyczny;
   5) użytkownik SILP nie może posiadać uprawnień do wyłączania i deinstalacji programu antywirusowego;
   6) program antywirusowy może wyłączyć lub dokonać jego deinstalacji jedynie Administrator SILP, na czas przeprowadzania czynność administracyjnych, wymagających takiego postępowania;
   7) każdy elektroniczny nośnik danych pochodzący z zewnątrz, przed jego użyciem, należy sprawdzić programem antywirusowym.
4. Instalacja oprogramowania:
   1) instalowanie i usuwanie oprogramowania może wykonywać jedynie administrator SILP lub firma zewnętrzna świadcząca serwis;
   2) zabronione jest instalowanie i używanie oprogramowania:
      a) bez posiadania wymaganej przez producenta lub autora licencji,
      b) pochodzącego z nieznanego źródła,

c) z nośników innych niż oryginalne nośniki producenta, które nie zostały sprawdzone programem antywirusowym,
d) wpływającego negatywnie na pracę sieci LP;

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.

5. 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 naczelnika WI DGLP;
   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, 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 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 spis jego 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 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:
      a) elementy umożliwiające dostęp do usługi APN tj. karta SIM, urządzenie mobilne muszą być własnością LP,
      b) adresację IP urządzeń w sieci APN ustala WI DGLP,
      c) w przypadku połączenia sieci APN do sieci LP poprzez sieć Internet wymagane jest użycie tunelu VPN typu site-to-site;
   3) dopuszcza się dostęp zdalny do wewnętrznych zasobów SILP za pośrednictwem wbudowanych mechanizmów VPN centralnego systemu EMM w PGL LP.

4) dopuszcza się dostęp zdalny VPN z sieci Internet do wewnętrznych zasobów SILP. Warunki i sposób dostępu zostały określone w § 9;
5) zabrania się fizycznego podłączenia do sieci LP komputerów nie będących własnością Lasów Państwowych, bez zgody właściwych WI;
6) 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;
7) 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) z 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,
d) w przypadku awarii i braku możliwości komunikacji z centralnymi serwerami uwierzytelniania dostępu, możliwe jest uwierzytelnienie dostępu do sieci bezprzewodowej za pomocą dedykowanego awaryjnego identyfikatora sieci. Po przywróceniu komunikacji z centralnymi serwerami uwierzytelniania dostępu hasło do awaryjnego identyfikatora sieci musi zostać zmienione;

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 jednorazowych kodów i portalu dla dostępu gościnnego,
b) kody generowane są przez osobę wyznaczoną przez kierownika danej jednostki organizacyjnej lub będą dostarczane do jednostki przez właściwe WI,
c) dostęp będzie możliwy jedynie po akceptacji regulaminu określającego zasady dostępu,
d) ruch z sieci dla dostępu gościnnego przesyłany jest tunelem pomiędzy ruterem brzegowym jednostki 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. System poczty elektronicznej LP posiada mechanizmy zabezpieczające przed nieautoryzowanym dostępem przez osoby trzecie.
5. Zabronione jest udostępnianie przez użytkowników konta pocztowego lub danych dostępowych do konta pocztowego osobom nieupoważnionym.
6. W systemie poczty Lasów Państwowych funkcjonują tylko imienne konta pocztowe oraz nieimienne konta specjalne tworzone za zgodą naczelnika WI DGLP.
7. 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.

8. 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.
9. Użytkownicy kont pocztowych zawartych w domenie LP muszą przestrzegać „Regulaminu użytkowania systemu poczty elektronicznej LP".
10. Aktualny „Regulamin użytkowania systemu poczty elektronicznej LP" publikowany jest pod adresem https://mail.lasy.gov.pl/regulamin.
11. Regulamin zatwierdza naczelnik WI DGLP. Wszelkie zmiany Regulaminu zaczynają obowiązywać z momentem ich opublikowania. Użytkownicy są informowani o zmianach Regulaminu poprzez wiadomość poczty elektronicznej.
12. 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 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 przez 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 ruchu na styku sieci WAN LP i Internet", tworzony oraz aktualizowany przez ZCI i zatwierdzany przez naczelnika WI DGLP.
4. 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..
5. Zabronione jest używanie oprogramowania służącego do anonimizacji ruchu sieciowego, w szczególności wykorzystującego technologie TOR lub VPN.
6. Polityki dla ruchu na styku sieci WAN LP i Internet realizowane są na centralnych systemach zabezpieczeń sieciowych będących własnością PGL LP.
7. 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 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 podmiotów zewnętrznych do zasobów SILP może być przydzielony jedynie w przypadku, gdy została podpisana Umowa wymagającej 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 następuje 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 wymagającej 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 łączą 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 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 następuje 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) witryny informacyjne WWW – wszystkie nadleśnictwa, zakłady LP, RDLP i DGLP, zobowiązane są do utrzymywania własnej witryny informacyjnej WWW w domenie lasy.gov.pl na portalu korporacyjnym LP;
   6) centralny system zarządzania telefonią IP - Cisco Unified Communications Manager;
   7) Elektroniczne Zarządzanie Dokumentacją - system elektronicznego obiegu dokumentów;
   8) centralny system zarządzania urządzeniami mobilnymi klasy EMM;
   9) 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 uruchomienia ochrony antywirusowej, urządzenie musi mieć aktywną i aktualną ochronę;
   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.

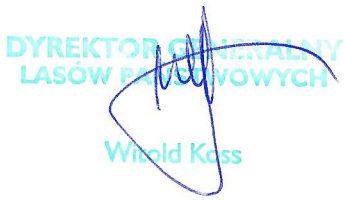
2. Urządzenia mobilne będące własnością PGL LP, wykorzystywane do przechowywania i przetwarzania danych służbowych oraz łączenia się z zasobami LP, dodatkowo podlegają następującym wymaganiom:
   1) urządzenie musi spełniać obowiązującą rekomendację określoną przez WI DGLP;
   2) urządzenie musi pracować 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."

§ 2

Zarządzenie wchodzi w życie z dniem podpisania.



Zarządzenie nr 135
Dyrektora Generalnego Lasów Państwowych
z dnia 21 listopada 2024 r.

w sprawie zmiany Zarządzenia nr 31 Dyrektora Generalnego Lasów Państwowych z dnia 18 września 2017 r. w sprawie zasad funkcjonowania i zasad bezpieczeństwa systemu informatycznego w Państwowym Gospodarstwie Leśnym Lasy Państwowe

(znak: EI.0413.28.2024)

Na podstawie art. 33 ust. 1 ustawy z dnia 28 września 1991 r. o lasach (t.j. Dz. U. z 2024 r. poz. 530; zm. Dz. U. z 2024 r. poz. 1473) oraz § 6 Statutu Państwowego Gospodarstwa Leśnego Lasy Państwowe, wprowadzonego zarządzeniem nr 50 Ministra Ochrony Środowiska, Zasobów Naturalnych i Leśnictwa z dnia 18 maja 1994 r. – w wykonaniu zadań Dyrektora Generalnego Lasów Państwowych, wynikających z realizacji jego uprawnienia określonego w § 8 ust. 1 pkt 6 ww. statutu oraz art. 33 ust. 3 pkt 8 ustawy o lasach, zarządzam, co następuje:

§ 1

Zmienia się treść załącznika nr 2 do Zarządzenia nr 31 Dyrektora Generalnego Lasów Państwowych z dnia 18 września 2017 w sprawie zasad funkcjonowania i zasad bezpieczeństwa systemu informatycznego w Państwowym Gospodarstwie Leśnym Lasy Państwowe, który przyjmuje brzmienie:

„**Załącznik nr 2 do Zarządzenia nr 31**
Dyrektora Generalnego Lasów Państwowych
z dnia 18 września 2017 r.

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 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 oprogramowania użytkowego 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.
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 usunąć te 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. Dopuszcza się czasowe odstąpienie od aktualizacji, w szczególnych przypadkach, skutkujących brakiem możliwości użytkowania oprogramowania stosowanego w LP.
19. Sieć komputerowa w jednostkach organizacyjnych LP opiera się o model zgodny z „Projektem usług katalogowych PGL LP” zatwierdzonym przez naczelnika WI DGLP.
20. Za utrzymanie, konserwację i prawidłowe działanie systemów informatycznych odpowiadają administratorzy SILP.
21. 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 karty kryptograficznej i certyfikatu korporacyjnego PKI LP lub haseł jednorazowych.
2. Systemy wewnętrznych zasobów 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 i uwierzytelnianie za ich pomocą administratorów SILP w krytycznych, ze względu na działanie SILP, elementach infrastruktury.
5. Dopuszcza się zakładanie lokalnych 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 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 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:
   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 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 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.
14. Systemy serwerowe SILP działające pod kontrolą systemów operacyjnych Microsoft Windows muszą posiadać włączoną i aktualną ochronę antywirusową:
   1) program antywirusowy musi posiadać aktualną bazę sygnatur wirusów aktualizowaną co najmniej raz na dzień, w sposób automatyczny;
   2) oprogramowanie antywirusowe musi pracować w trybie skanowania plików w czasie rzeczywistym;
   3) przynajmniej raz na miesiąc musi być wykonywane pełne skanowanie systemu w sposób automatyczny.

15. Dopuszcza się brak ochrony antywirusowej, w szczególnych przypadkach skutkujących brakiem możliwości użytkowania oprogramowania stosowanego w LP.
16. 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.
17. Zabronione jest podłączanie do sieci LAN PC interfejsów zarządzających serwerów, systemów i urządzeń sieciowych SILP.
18. 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.
19. Systemy SILP muszą rejestrować i przechowywać przez co najmniej 3 miesiące lub przekazywać do zewnętrznego dziennika zdarzeń:
    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.
20. Systemy SILP mogą mieć uruchomione jedynie usługi i oprogramowanie zgodne z przeznaczeniem systemów.
21. Instalowanie oraz usuwanie oprogramowania może wykonywać jedynie uprawniony administrator SILP lub firma zewnętrzna świadcząca serwis.
22. Zabronione jest instalowanie i używanie oprogramowania:
    1) bez posiadania wymaganej przez producenta lub autora licencji;
    2) pochodzącego z nieznanego źródła;
    3) z nośników innych niż oryginalne nośniki producenta, które nie zostały sprawdzone programem antywirusowym;
    4) wpływającego negatywnie na pracę SILP.

§ 3.
Bezpieczeństwo stacji roboczych

1. Zasady ogólne:
    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;
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. 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. W przypadku instalacji aktualizacji wymagającej restartu systemu, administrator lub użytkownik SILP niezwłocznie wykona restart.
3. Ochrona antywirusowa stacji roboczych z systemem Windows:
   1) każda stacja robocza podłączona do sieci WAN LP musi posiadać aktywne oprogramowanie antywirusowe podłączone do dedykowanej konsoli zarządzającej tym oprogramowaniem;
   2) oprogramowanie antywirusowe musi pracować w trybie skanowania plików i poczty w czasie rzeczywistym;
   3) przynajmniej raz na miesiąc ma być wykonywane pełne skanowanie systemu w sposób automatyczny;
   4) program antywirusowy musi posiadać aktualną bazę sygnatur wirusów, aktualizowaną co najmniej raz na dzień, w sposób automatyczny;
   5) użytkownik SILP nie może posiadać uprawnień do wyłączania i deinstalacji programu antywirusowego;
   6) program antywirusowy może wyłączyć lub dokonać jego deinstalacji jedynie Administrator SILP, na czas przeprowadzania czynność administracyjnych, wymagających takiego postępowania;
   7) każdy elektroniczny nośnik danych pochodzący z zewnątrz, przed jego użyciem, należy sprawdzić programem antywirusowym.
4. Instalacja oprogramowania:
   1) instalowanie i usuwanie oprogramowania może wykonywać jedynie administrator SILP lub firma zewnętrzna świadcząca serwis;
   2) zabronione jest instalowanie i używanie oprogramowania:
      a) bez posiadania wymaganej przez producenta lub autora licencji,
      b) pochodzącego z nieznanego źródła,

c) z nośników innych niż oryginalne nośniki producenta, które nie zostały sprawdzone programem antywirusowym,
d) wpływającego negatywnie na pracę sieci LP;
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.

5. 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 naczelnika WI DGLP;
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, 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 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 spis jego 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 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:
      a) elementy umożliwiające dostęp do usługi APN tj. karta SIM, urządzenie mobilne muszą być własnością LP,
      b) adresację IP urządzeń w sieci APN ustala WI DGLP,
      c) w przypadku połączenia sieci APN do sieci LP poprzez sieć Internet wymagane jest użycie tunelu VPN typu site-to-site;
   3) dopuszcza się dostęp zdalny do wewnętrznych zasobów SILP za pośrednictwem wbudowanych mechanizmów VPN centralnego systemu EMM w PGL LP.

4) dopuszcza się dostęp zdalny VPN z sieci Internet do wewnętrznych zasobów SILP. Warunki i sposób dostępu zostały określone w § 9;
5) zabrania się fizycznego podłączenia do sieci LP komputerów nie będących własnością Lasów Państwowych, bez zgody właściwych WI;
6) 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;
7) 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) z 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,
d) w przypadku awarii i braku możliwości komunikacji z centralnymi serwerami uwierzytelniania dostępu, możliwe jest uwierzytelnienie dostępu do sieci bezprzewodowej za pomocą dedykowanego awaryjnego identyfikatora sieci. Po przywróceniu komunikacji z centralnymi serwerami uwierzytelniania dostępu hasło do awaryjnego identyfikatora sieci musi zostać zmienione;

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 jednorazowych kodów i portalu dla dostępu gościnnego,
b) kody generowane są przez osobę wyznaczoną przez kierownika danej jednostki organizacyjnej lub będą dostarczane do jednostki przez właściwe WI,
c) dostęp będzie możliwy jedynie po akceptacji regulaminu określającego zasady dostępu,
d) ruch z sieci dla dostępu gościnnego przesyłany jest tunelem pomiędzy ruterem brzegowym jednostki 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. System poczty elektronicznej LP posiada mechanizmy zabezpieczające przed nieautoryzowanym dostępem przez osoby trzecie.
5. Zabronione jest udostępnianie przez użytkowników konta pocztowego lub danych dostępowych do konta pocztowego osobom nieupoważnionym.
6. W systemie poczty Lasów Państwowych funkcjonują tylko imienne konta pocztowe oraz nieimienne konta specjalne tworzone za zgodą naczelnika WI DGLP.
7. 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.

8. 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.
9. Użytkownicy kont pocztowych zawartych w domenie LP muszą przestrzegać „Regulaminu użytkowania systemu poczty elektronicznej LP".
10. Aktualny „Regulamin użytkowania systemu poczty elektronicznej LP" publikowany jest pod adresem https://mail.lasy.gov.pl/regulamin.
11. Regulamin zatwierdza naczelnik WI DGLP. Wszelkie zmiany Regulaminu zaczynają obowiązywać z momentem ich opublikowania. Użytkownicy są informowani o zmianach Regulaminu poprzez wiadomość poczty elektronicznej.
12. 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 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 przez 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 ruchu na styku sieci WAN LP i Internet", tworzony oraz aktualizowany przez ZCI i zatwierdzany przez naczelnika WI DGLP.
4. 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..
5. Zabronione jest używanie oprogramowania służącego do anonimizacji ruchu sieciowego, w szczególności wykorzystującego technologie TOR lub VPN.
6. Polityki dla ruchu na styku sieci WAN LP i Internet realizowane są na centralnych systemach zabezpieczeń sieciowych będących własnością PGL LP.
7. 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 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 podmiotów zewnętrznych do zasobów SILP może być przydzielony jedynie w przypadku, gdy została podpisana Umowa wymagającej 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 następuje 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 wymagającej 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 łączą 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 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 następuje 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) witryny informacyjne WWW – wszystkie nadleśnictwa, zakłady LP, RDLP i DGLP, zobowiązane są do utrzymywania własnej witryny informacyjnej WWW w domenie lasy.gov.pl na portalu korporacyjnym LP;
   6) centralny system zarządzania telefonią IP - Cisco Unified Communications Manager;
   7) Elektroniczne Zarządzanie Dokumentacją - system elektronicznego obiegu dokumentów;
   8) centralny system zarządzania urządzeniami mobilnymi klasy EMM;
   9) 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 uruchomienia ochrony antywirusowej, urządzenie musi mieć aktywną i aktualną ochronę;
   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.”

§ 2

Zarządzenie wchodzi w życie z dniem podpisania.