Załącznik nr 5
do Regulaminu
Organizacyjnego Urzędu
Marszałkowskiego

ZARZĄDZENIE nr 12

DYREKTORA GENERALNEGO LASÓW PAŃSTWOWYCH

z dnia 3 lutego 2022 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

OI.0413.13.2017

(Znak: EI.413.4.2022)

Na podstawie art. 33 ust. 1 ustawy z dnia 28 września 1991 r. o lasach[1], w związku z § 6 Statutu Państwowego Gospodarstwa Leśnego Lasy Państwowe[2], w wykonaniu zadań Dyrektora Generalnego Lasów Państwowych, o których mowa w § 8 ust. 1 pkt 6 Statutu Państwowego Gospodarstwa Leśnego Lasy Państwowe[3] oraz w art. 33 ust. 3 pkt 8 ustawy o lasach[4], zarządza się, co następuje:

§1

Zmienia się treść załącznika nr 2 do zarządzenia nr 31 Dyrektora Generalnego Lasów Państwowych z dnia 18 września 2017 r., który otrzymuje 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] Art. 33 ust. 1 ustawy z dnia 28 września 1991 r. o lasach (t.j. Dz. U. z 2021 r. poz. 1275 ze zm.) stanowi, że Lasami Państwowymi kieruje Dyrektor Generalny przy pomocy dyrektorów regionalnych dyrekcji Lasów Państwowych.

[2] Statut Państwowego Gospodarstwa Leśnego Lasy Państwowe został nadany zarządzeniem nr 50 Ministra Ochrony Środowiska, Zasobów Naturalnych i Leśnictwa z dnia 18 maja 1994 r. § 6 Statutu stanowi, że w wykonaniu zadań określonych przez ustawę o lasach oraz przez przepisy wykonawcze do ustawy, a także inne przepisy prawa, Dyrektor Generalny wydaje zarządzenia i decyzje obowiązujące w Lasach Państwowych.

[3] § 8 ust. 1 pkt 6 Statutu Państwowego Gospodarstwa Leśnego Lasy Państwowe stanowi, że Dyrektor Generalny ustala system informacyjny Lasów Państwowych.

[4] Art. 33 ust. 3 pkt 8 ustawy o lasach stanowi, że Dyrektor Generalny organizuje wspólne przedsięwzięcia jednostek organizacyjnych Lasów Państwowych.

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, przy spełnieniu następujących warunków:
   1) dostęp będzie możliwy jedynie na czas obowiązywania umowy;
   2) podmiot zewnętrzny podpisze oświadczenie o zasadach udzielenia dostępu i zachowaniu poufności.
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. 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.
15. W przypadku likwidacji nośników lub sprzętu z nośnikami zawierającymi dane SILP, należy usunąć te dane w sposób uniemożliwiający ich odtworzenie.
16. 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.
17. Dopuszcza się czasowe odstąpienie od aktualizacji, w szczególnych przypadkach, skutkujących brakiem możliwości użytkowania oprogramowania stosowanego w LP.
18. Sieć komputerowa w jednostkach organizacyjnych LP opiera się o model zgodny z „Projektem usług katalogowych PGL LP" zatwierdzonym przez naczelnika WI DGLP.
19. Za utrzymanie, konserwację i prawidłowe działanie systemów informatycznych odpowiadają administratorzy SILP.
20. 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://poczta.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 będzie możliwy jedynie na czas obowiązywania umowy;
   2) firma zewnętrzna podpisze oświadczenie o zasadach udzielenia dostępu.
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.
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.
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.

§ 11.
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

Zmienia się treść załącznika nr 3 do zarządzenia nr 31 Dyrektora Generalnego Lasów Państwowych z dnia 18 września 2017 r., który otrzymuje brzmienie:

„ZASADY UDOSTĘPNIANIA BAZ SYSTEMU LAS

§ 1.

1. Przez dostęp do danych systemu LAS rozumie się:
   1) zalogowanie się do bazy danych danej jednostki organizacyjnej LP;
   2) odczyt lub zapis danych bazy systemu LAS.
2. Dostęp do danych systemu LAS jednostki organizacyjnej LP może być realizowany w trybie:
   1) dostępu stałego;
   2) dostępu tymczasowego.
3. Dostęp stały do danych systemu LAS może być realizowany dla:
   1) użytkowników SILP zatrudnionych w jednostce wyłącznie na podstawie udokumentowanej dyspozycji kierownika jednostki, określającej:
      a) zasoby danych,
      b) zakres uprawnień dostępu do danych;
   2) użytkowników SILP 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:
   1) użytkowników SILP zatrudnionych w jednostce na czas określony, wyłącznie na podstawie udokumentowanej dyspozycji kierownika jednostki, określającej:
      a) zasoby danych,
      b) zakres uprawnień dostępu do danych,
      c) datę odebrania uprawnień;
   2) użytkowników SILP zatrudnionych w jednostce nadrzędnej, w ramach sprawowania nadzoru na podstawie udokumentowanej dyspozycji kierownika tej jednostki, określającej:
      a) zasoby danych jednostki nadzorowanej,
      b) datę odebrania uprawnień;
   3) pracowników ILP na podstawie pisemnego upoważnienia do przeprowadzenia kontroli, z zachowaniem postanowień zawartych w § 2;
   4) członków zespołów zadaniowych powołanych zarządzeniem lub decyzją Dyrektora Generalnego Lasów Państwowych, posiadających uprawnienia o dostępie do danych systemu LAS jednostek nadzorowanych, określone w akcie powołania zespołu;
   5) członków zespołów zadaniowych powołanych zarządzeniem lub decyzją Dyrektora Regionalnego Lasów Państwowych, posiadających uprawnienia o dostępie do danych systemu LAS jednostek nadzorowanych, określone w akcie powołania zespołu;
   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. Zgodnie z wyznaczonym terminem kierownik komórki WI realizuje:

1) odebranie uprawnień dostępu do systemu LAS jednostki, poprzez zablokowanie użytkownika w systemie LAS, oraz zablokowanie konta domenowego;
2) odebranie wszelkich środków technicznych związanych z dostępem do bazy danych.

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 sytemu LAS. Z wnioskiem o zmianę uprawnień występuje do kierownika jednostki bezpośredni przełożony pracownika.
7. Za realizację postanowień ust. 3, ust. 4, ust. 5 i ust. 6 odpowiada kierownik jednostki organizacyjnej Lasów Państwowych, lub osoby przez niego upoważnione.

§ 2.

1. Przez udostępnienie danych systemu LAS jednostki organizacyjnej LP inspektorowi ILP rozumie się:
   1) nadanie upoważnionemu inspektorowi LP dostępu z zakresem uprawnień zdefiniowanym przez Dyrektora Generalnego Lasów Państwowych dla użytkowników grupowych ILP;
   2) udostępnienie danych w formie raportu zdefiniowanego wcześniej przez kontrolującego.
2. Pracownicy jednostek nadzorujących mogą mieć udostępnione dane systemu LAS w jednostkach podległych w trybie dostępu stałego lub tymczasowego, w zakresie uprawnień określonych przez kierownika jednostki nadzorującej.
3. Pracownicy jednostek nadzorujących oraz ILP mogą posiadać wyłącznie uprawnienie do przeglądania danych systemu LAS w jednostkach organizacyjnych LP.

§ 3.

1. Przepisy zawarte w § 1 i § 2 nie dotyczą pracowników WI oraz ZILP w ramach wykonywania czynności administracyjnych.
2. W celu zapewnienia poprawności funkcjonowania SILP pracownicy wymienieni w ust. 1 mogą mieć pełny dostęp do baz informatycznych jednostek, w których są zatrudnieni oraz do baz informatycznych jednostek nadzorowanych.
3. WI prowadzą ewidencję wniosków, nadawanych uprawnień restrykcyjnych.
4. Jednostka organizacyjna prowadzi nadzór zmian wykonanych na bazie danych. Zmiany na bazie danych wykonywane są za akceptacją głównego księgowego jednostki.
5. Administrator w jednostce organizacyjnej LP prowadzi ewidencję udostępniania tymczasowego danych systemu LAS z wyłączeniem inspektorów ILP oraz

członków zespołów zadaniowych powołanych odrębnymi decyzjami lub zarządzeniami.

§ 4.

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 z zachowaniem anonimizacji danych osobowych, tj. w sposób uniemożliwiający ustalenie, jakiej osoby fizycznej dotyczy dany dokument, zestawienie, informacja dane płacowo-kadrowe, itd.. 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."

§3

Zmienia się treść załącznika nr 5 do zarządzenia nr 31 Dyrektora Generalnego Lasów Państwowych z dnia 18 września 2017 r., który otrzymuje brzmienie:

„WZÓR OŚWIADCZENIA PRACOWNIKA

Miejscowość ..... dnia ...../...../.....

Imię i nazwisko: .....

Jednostka Lasów Państwowych: ....

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 zgodnie z art. 22^3 Kodeksu pracy;
2) zobowiązuję się do:
   - przestrzegania „Zasad bezpiecznej eksploatacji zasobów informatycznych Lasów Państwowych" i powstrzymania się od jakichkolwiek działań niezgodnych z Zasadami, bądź nieprzewidzianych przez Zasady,

- przestrzegania „Regulaminu użytkowania Konta Pocztowego LP",
- zachowania w tajemnicy wszelkich danych (w tym także, gdy ustanie mój stosunek pracy lub cywilnoprawny w jednostce Lasów Państwowych), o których użytkownik posiadł wiedzę korzystając z systemu informatycznego Lasów Państwowych,
- zachowania w tajemnicy danych (w tym także, gdy ustanie mój stosunek pracy lub cywilnoprawny w jednostce Lasów Państwowych), 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,
- powiadamiania przełożonych o wszelkich znanych mi przypadkach, 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."

§4

1. Zarządzenie wchodzi w życie z dniem podpisania z wyjątkiem § 11 załącznika nr 2 do Zarządzenia nr 31 Dyrektora Generalnego Lasów Państwowych z dnia 18 września 2017 r., który wchodzi w życie 1 sierpnia 2022 r.
2. Dotychczasowy przepis § 11 zmienianego załącznika nr 2 do Zarządzenia nr 31 Dyrektora Generalnego Lasów Państwowych z dnia 18 września 2017 r. stosuje się do 31 lipca 2022 r.

LASY PAŃSTWOWE DYREKCJA GENERALNA LASÓW PAŃSTWOWYCH W WARSZAWIE

p.o. DYREKTORA GENERALNEGO
Lasów Państwowych

Józef Kubica

Polityka bezpieczeństwa

dla urządzeń mobilnych w PGL LP

Projekt techniczny

do Załącznika nr 2 do 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.

Metryka Dokumentu

Data	Autor		Wersja	Opis zmian
03.02.2022	EI	DGLP	1.0	Pierwsza wersja dokumentu

ZATWIERDZIŁ:

Paweł Jacek Pogoda

Elektronicznie podpisany przez Paweł Jacek Pogoda
Data: 2022.02.03 13:17:49 +01'00'

Spis treści

1. Terminy użyte w tekście

AER (ang. Android Enterprise Recommended) – rekomendacja zawierająca listę urządzeń i usług zatwierdzanych przez firmę Google. Program wsparcia ma zapewniać zgodność, spójny sposób wdrażania, zarządzania oraz gwarancję dostępu do aktualizacji i poprawek bezpieczeństwa.

Android – system operacyjny urządzenia mobilnego. System może różnić się w zależności od producenta urządzenia i posiadać różne nazewnictwo. Przykładem takich systemów jest Google Android, MIUI, HarmonyOS.

Apple ID - to metoda uwierzytelniania używana dla urządzeń Apple. Identyfikatory Apple ID zawierają dane osobowe i ustawienia użytkownika.

Apple iOS – system operacyjny na urządzenie mobilne firmy Apple Inc.

Apps – ogólne nazewnictwo aplikacji instalowanych na urządzenia mobilne.

Apps publiczne – aplikacje dostępne z oficjalnych źródeł dystrybucji, możliwe do pobrania z oficjalnych sklepów z aplikacjami lub sklepu korporacyjnego LP.

AppsLP – grupa aplikacji wewnętrznych wytworzonych w PGL LP lub na zlecenie PGL LP, które wymagają podczas instalacji lub obsługi, specjalnej konfiguracji lub tunelowania. Lista aplikacji wchodzących w skład aplikacji AppsLP podana została w dokumencie i może być aktualizowana w przyszłości.

Bluetooth – standard bezprzewodowej komunikacji krótkiego zasięgu pomiędzy różnymi urządzeniami, takimi jak klawiatura, komputer, laptop, palmtop, smartfon i wieloma innymi.

Brakarz+ - aplikacja wytworzona i zarządzana przez PGL LP, instalowana na wybranych urządzeniach mobilnych z systemem Android.

Centralny system zarządzania urządzeniami mobilnymi – system informatyczny z konsolą zarządzająca realizujący funkcje rejestrowania, zarządzania, konfiguracji, ochrony danych i monitorowania stanu urządzeń mobilnych, zamiennie nazywany w dokumentacji systemem EMM.

COBO (ang. Company Owned/Business Only) - tryb pracy urządzenia z systemem Android posiadający tylko przestrzeń firmową.

COPE (ang. Company Owned/Personally Enabled) – tryb pracy urządzenia z system Android posiadający przestrzeń osobista poza kontenerem firmowym.

EMM (ang. Enterprise Mobility Management) - centralny system zarządzania urządzeniami mobilnymi wykorzystywany w PGL LP.

GPS (ang. Global Positioning System) – system lub informacja na temat pozycji geograficznej urządzenia. W dokumencie nazwą GPS określono tryb rejestracji urządzenia, w którym informacja o lokalizacji może być zbierana przez system EMM za wiedzą i zgodą użytkownika, wykorzystywana tylko na wniosek i tylko na wypadek sytuacji kradzieży lub zgubienia lub innego istotnego zagrożenia.

Hasło – ciąg znaków o wymaganej złożoności znany tylko osobie, która je ustala, wykorzystywane przy kontroli dostępu.

Konto Google – konto, które po założeniu umożliwia dostęp do usług Google wymagających logowania.

Leśnik+ - aplikacja wytworzona i zarządzana przez PGL LP, instalowana na wybranych urządzeniach mobilnych z systemem Android.

LP Store – wewnętrzny sklep z aplikacjami na urządzenia mobilne dostępny dla urządzeń zarejestrowanych w systemie EMM. Katalog zawiera zarówno aplikacje wewnętrzne jak i aplikacje publiczne. Liczba aplikacji jest ograniczona i może różnić się w zależności od rodzaju urządzenia i systemu operacyjnego.

Mapa+ - aplikacja (w przygotowaniu) wytworzona i zarządzana przez PGL LP, instalowana na wybranych urządzeniach mobilnych z systemem Android.

MapaLeśnik+ - aplikacja wytworzona i zarządzana przez PGL LP, instalowana na wybranych urządzeniach mobilnych z systemem Android.

Metoda biometryczna – rodzaj zabezpieczenia opartego na danych biometrycznych: wizerunku twarzy, zapisu linii papilarnych palców, zapisu obrazu tęczówki zapisana w urządzeniu i wykorzystywana przy kontroli dostępu.

mLas – aplikacja wytworzona przez firmę Taxus, instalowana w zależności od wersji na wybranych urządzeniach mobilnych z systemem Androd.

OS (ang. Operating System) – system operacyjny urządzenia.

PIN – rodzaj hasła składającego się z samych cyfr.

Smart Lock – rozwiązania ułatwiające odblokowanie urządzenia mobilnego np. za pomocą zaufanych miejsc lub innego zaufanego urządzenia.

USB (ang. Universal Serial Bus) – szybki interfejs do podłączania zewnętrznych urządzeń.

Wi-Fi – standard dla sieci bezprzewodowej wykorzystywanej głównie do łączenia z siecią publiczną Internet. Użytkownik łącząc się z siecią Wi-Fi nie ma nigdy pewności kto jest jej właścicielem, co wiąże się z ryzykiem wycieku danych. Zaleca się łączenie tylko z sieciami zaufanymi a przede wszystkim zabezpieczonymi.

Wi-Fi Direct - technologia bezprzewodowa wykorzystywana w telekomunikacji. Swym działaniem jest podobna do Bluetooth ale charakteryzuje się większym zasięgiem i szybkością przesyłania danych.

Wzór – rodzaj hasła składającego się z takich elementów jak linie prowadzone między punktami.

Zaufana sieć (Wi-Fi) – sieć, której właścicielem jest zaufana instytucja lub osoba. Zaufana sieć charakteryzuje się ograniczonym dostępem za pomocą hasła lub innej bezpiecznej metody a jej nazwa jest autentyczna (bezprzewodowe sieci otwarte z reguły nie są sieciami zaufanymi i mogą przyjmować różne nazwy, często zbliżone do zaufanych sieci a ich celem może być pozyskanie danych z urządzenia połączonego do takiej sieci).

2. Rekomendacja dla urządzeń mobilnych określona przez WI DGLP

1. Przyjmuje się, że urządzenia mobilne stosowane w Państwowych Gospodarstwie Leśnym Lasy Państwowe (PGL LP) to urządzenia typu smartfon lub tablet, zdolne do przechowywania i przetwarzania danych, nie będące jednocześnie obiektami domeny ad.lasy.gov.pl (urządzenia te posiadają oddzielną politykę bezpieczeństwa).

2. Urządzenia muszą pracować pod kontrolą jednego z systemów: Android lub iOS, przy czym wersja używanego systemu musi posiadać aktywne wsparcie jego producenta.

3. W celu ujednolicenia platformy systemowej i zachowania zgodności z posiadanymi rozwiązaniami informatycznymi w PGL LP, rekomenduje się stosowanie przede wszystkim urządzeń z systemem Android.

4. W celu zachowania kompatybilności z centralnym systemem zarządzania urządzeniami mobilnymi w PGL LP zaleca się aby urządzenia z systemem Android wykorzystywane do przechowywania

i przetwarzania danych służbowych i/lub łączenia się z zasobami LP były zgodne z programem AER (ang. Android Enterprise Recommended). Lista urządzeń rekomendowanych dostępna jest na stronie: https://www.android.com/enterprise/. Stosowanie urządzeń poza AER może powodować ich niestabilne działanie w systemie i wiązać się z brakiem wsparcia dla zgłoszonych problemów jeśli wystąpią.

5. Urządzenia z systemem Android, wykorzystywane do przechowywania i przetwarzania danych służbowych i/lub łączenia się z zasobami LP, oraz posiadające aplikacje wewnętrzne (AppsLP) wytworzone przez/dla PGL LP (w tym rejestratory), muszą znajdować się na liście urządzeń publikowanej na:

   - **Stronie internetowej Zakładu Informatyki Lasów Państwowych**
     https://www.zilp.lasy.gov.pl/rejestrator-lesniczego > Lista urządzeń

     Lista jest również publikowana w serwisie Panelu Leśnika uzupełniona o szczegółowe dane techniczne:

   - **Panel Leśnika**
     https://lesnikpanel.silp.lasy.gov.pl > Menu > Materiały Wdrożeniowe > Rekomendacje dla urządzeń

3. Rodzaje urządzeń mobilnych

Podział urządzeń mobilnych został określony ze względu na realizowane funkcje oraz posiadane oprogramowanie. Wyróżnia się następujące rodzaje służbowych urządzeń mobilnych:

1) **zdolne do przechowywania i przetwarzania danych** (z pominięciem danych służbowych) – dla tych urządzeń obowiązują zasady ogólne konfiguracji opisane w zarządzeniu i polityce bezpieczeństwa,

2) **wykorzystywane do przechowywania i przetwarzania danych służbowych i/lub łączenia się z zasobami LP** (nieposiadające aplikacji wewnętrznych wytworzonych przez/dla PGL LP) – dla tych urządzeń obowiązują zasady ogólne i wymagania dodatkowe dotyczące konfiguracji opisane w zarządzeniu i polityce bezpieczeństwa,

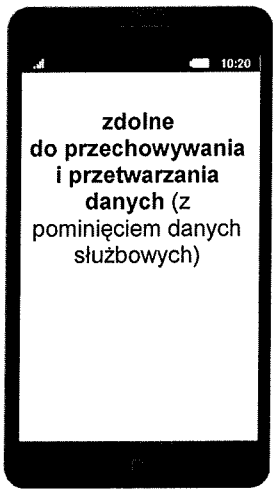
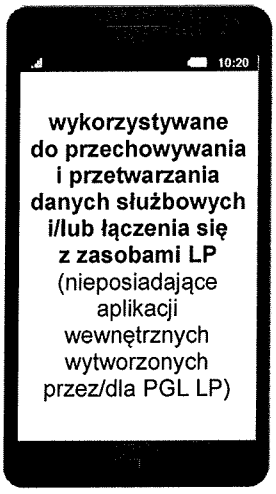
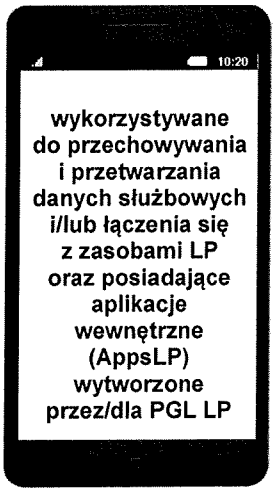
3) **wykorzystywane do przechowywania i przetwarzania danych służbowych i/lub łączenia się z zasobami LP oraz posiadające aplikacje**

wewnętrzne (AppsLP) wytworzone przez/dla PGL LP – dla tych urządzeń obowiązują zasady ogólne i wymagania dodatkowe dotyczące konfiguracji opisane w zarządzeniu i polityce bezpieczeństwa oraz ograniczona liczba modeli pracujących z aplikacjami AppsLP.

Szczegółowe informacje dotyczące ustawień, które nie zostały ujęte w dokumentacji zamieszczone zostały w instrukcjach dla poszczególnych systemów i urządzeń. Instrukcje zostały udostępnione administratorom i użytkownikom w PGL LP i obowiązują aktualne wersje tych dokumentów.

Powyższy podział został opisany w tabeli nr 1.

Tabela nr 1: Rodzaje urządzeń mobilnych

Opis	**Rodzaje urządzeń mobilnych**		
Lp	1	2	3
			
Oznaczenie	**TL**	**TS**	**TA**
Dane służbowe	**NIE**	**TAK**	**TAK**
Dostęp do zasobów PGL LP	**NIE**	**TAK**	**TAK**
Obecność aplikacji AppsLP*	**NIE**	**NIE**	**TAK**
Zasady ogólne	**TAK**	**TAK**	**TAK**
Wymagania dodatkowe	**NIE**	**TAK**	**TAK**
Dostęp do Internetu	**ZALECANY**	**TAK**	**TAK**
Aktualizacja OS	**INTERNET**	**INTERNET**	**EMM / INTERNET**
Aktualizacja Apps publiczne	**INTERNET**	**INTERNET**	**INTERNET**
Aktualizacja AppsLP	NIE DOTYCZY	NIE DOTYCZY	**EMM**
System Antywirusowy	**TAK**	**TAK**	**TAK**
System EMM	**NIE**	**TAK**	**TAK**
Tryb rejestracji w EMM**	NIE DOTYCZY	**COPE** (Android)	**COBO** (Android)

Kontener	NIE DOTYCZY	**OSOBISTY + FIRMOWY (PRACA)**	**FIRMOWY (PRACA)**
Certyfikat Android (AER)	NIE DOTYCZY	**ZALECANE**	**TAK**
Ograniczenie urządzeń	**NIE**	**ZGODNE Z EMM**	**Z LISTY***

* lista urządzeń kompatybilna z AppsLP publikowana na portalu pracowniczym i Panelu Leśnika.

** tryby rejestracji:

TL

Nie dotyczy. Urządzenia TL nie są objęte środowiskiem EMM.

TS

Dla urządzeń TS w systemie Android właściwy tryb rejestracji: COPE posiadający część firmową (kontener Praca) i osobistą (poza kontenerem Praca) z możliwością dodania osobistego konta Google i pobierania aplikacji publicznych.

Tryb COPE jest trybem o ograniczonej funkcjonalności pod względem zarządzania. Należy go traktować jako opcjonalny tryb rejestracji. Dla systemu Android możliwe tryby rejestracji: COPE GPS, COPE.

Dla systemu iOS właściwy tryb rejestracji: iOS GPS, iOS.

TA

Dla urządzeń TS w systemie Android właściwy tryb rejestracji: COBO posiadający tylko część firmową (kontener Praca).

Tryb COBO jest trybem o pełnej funkcjonalności pod względem zarządzania. Należy go traktować jako podstawowy tryb rejestracji. Możliwe tryby rejestracji: COBO GPS, COBO.

Dla systemu iOS urządzenia TA nie występują. Możliwe tryby rejestracji: brak.

4. Konwencja nazewnicza

Dla urządzeń mobilnych będących własnością PGL LP nie będących jednocześnie obiektami domeny ad.lasy.gov.pl (urządzenia takie posiadają oddzielny schemat nazewnictwa) przyjęto następującą konwencję nazewniczą:

{Lokalizacja(1)}{Typ(2)}{Kod jednostki(4)}-{Numer identyfikacyjny(6)}

Nazwa przyjmuje postać:

LTTKKKK-NNNNNN

Lokalizacja	Typ	Kod jednostki	-	Nr identyfikacyjny

Gdzie:

- **Lokalizacja:** jeden znak oznaczający poziom organizacji, na którym znajduje się lokalizacja danego obiektu analogicznie jak w projekcie usług katalogowych PGL LP

Tabela nr 2: Oznaczenia lokalizacji w zależności od poziomu organizacji

Oznaczenie	Poziom organizacji
G	Urządzenie mobilne w DGLP
R	Urządzenie mobilne w RDLP
N	Urządzenie mobilne w nadleśnictwie
Z	Urządzenie mobilne w zakładzie Lasów Państwowych

- **Typ:** dwa znaki oznaczający typ urządzenia mobilnego. Poniżej została przedstawiona tabela zawierająca przyjęte oznaczenia typów urządzeń mobilnych.

Tabela nr 3: Oznaczenia typu w zależności od rodzaju urządzenia

Oznaczenie	Typ urządzenia
TL	Urządzenie mobilne zdolne do przechowywania i przetwarzania danych (z pominięciem danych służbowych)
TS	Urządzenie mobilne wykorzystywane do przechowywania i przetwarzania danych służbowych lub łączenia się z zasobami LP (nieposiadające aplikacji wewnętrznych wytworzonych przez/dla PGL LP - AppsLP).
TA	Urządzenia mobilne wykorzystywane do przechowywania i przetwarzania danych służbowych lub łączenia się z zasobami LP oraz posiadające aplikacje wewnętrzne wytworzone przez/dla PGL LP (AppsLP)

- **Kod jednostki:** cztery znaki oznaczające jednostkę, w której znajduje się urządzenie mobilne. Kod jednostki zbudowany jest z czterech znaków adresu leśnego danej jednostki. Pełna lista kodów dla poszczególnych lokalizacji przedstawiona została w dokumencie „Projekt usług katalogowych PGL LP".

- **Numer identyfikacyjny**: sześć znaków składających się z numeru inwentarzowego z pominięciem rodzaju inwentarza, uzupełniony wiodącymi zerami z przodu do wymaganej liczby znaków, przypisany do każdego urządzenia mobilnego.

  Przykładowo w RDLP Wrocław (13) w Nadleśnictwie Henryków (02) dla urządzenia mobilnego typu TL o numerze inwentarzowym N623/9452 nazwa zgodna

z przyjętą konwencją nazewniczą przedstawia się następująco: NTL1302–009452.

Każde urządzenie mobilne w polu „ustawienia > urządzenie – informacje > edytuj" (podana ścieżka może różnić się w zależności od urządzenia) powinno mieć zmienioną domyślną nazwę na właściwą zgodną z przyjętą konwencją. Nazwę tą należy również wprowadzić przy rejestracji urządzenia w systemach EMM i antywirusowym w przypadku gdy nie zostanie ona pobrana automatycznie z urządzenia. Sposób i miejsce wprowadzenia nazw będą określały właściwe instrukcje.

5. Konfiguracja urządzeń

5.1. Wymagania ogólne dla urządzeń TL, TS, TA

Polityka bezpieczeństwa odnosząca się do konfiguracji urządzeń mobilnych będących własnością jednostek LP stanowi uzupełnienie treści Zarządzenia w zakresie bezpieczeństwa urządzeń mobilnych i przedstawia się następująco:

1. Urządzenie musi posiadać certyfikację CE (Conformité Européenne), instrukcję w języku polskim oraz oprogramowanie systemowe zainstalowane przez producenta urządzenia.
2. Urządzenie nie może być poddawane modyfikacjom mającym na celu zmianę uprawnień zdefiniowanych przez jego producenta, w szczególności: usuwania ograniczeń dla instalowanych aplikacji, uzyskania uprawnień administratora bądź innych funkcji wpływających na bezpieczeństwo lub utratę gwarancji.
3. Urządzenie oprócz połączenia do Internetu realizowanego przez transmisję danych komórkowych może łączyć się z zaufanymi sieciami Wi-Fi.
4. Urządzenie musi mieć instalowane na bieżąco aktualizacje krytyczne, bezpieczeństwa systemu i aplikacji, które nie powinny być pomijane lub przekładane bez istotnej przyczyny.
5. Uprawnienia dostępu dla instalowanych aplikacji, w szczególności do funkcji telefonu: kontaktów, wykonywania i rejestru połączeń, SMS, mikrofonu, kamery, mogą być nadane jedynie aplikacjom używanym w celach realizacji zadań służbowych.
6. Urządzenie musi posiadać włączoną funkcję automatycznej blokady ekranu po wejściu w stan uśpienia i na żądanie użytkownika przyciskiem zasilania. Po zakończonej pracy na urządzeniu za każdym razem ekran musi zostać zablokowany.
7. Jeżeli system urządzenia pozwala na zdefiniowanie komunikatu na ekranie blokady, musi być on włączony i posiadać odpowiedni format: „Kontakt: +48XXXXXXXXX | jednostka@subdomena.lasy.gov.pl" zawierające w kolejności numer telefonu do sekretariatu oraz adres e-

mail jednostki LP. Długość znaków może być ograniczona w zależności od modelu urządzenia.

8. Blokada ekranu musi być włączona na poziomie minimum: niski (przynajmniej wzór). Dopuszczalne metody: wzór, PIN, hasło, opcjonalna metoda biometryczna: odcisk palca, rozpoznawanie twarzy, skan tęczówki (dotyczy tylko TL).
9. Widoczność hasła, pinu lub ślad wzoru podczas wprowadzania muszą być wyłączone.
10. Urządzenie musi mieć wyłączoną funkcję inteligentnego odblokowania (Smart Lock).
11. Jeżeli urządzenie posiada opcję „bezpieczne uruchamianie/szyfrowanie" – musi być włączona, co skutkuje wymaganiem podania wzoru/PIN/hasła przy włączaniu urządzenia.
12. Urządzenie powinno mieć wyłączone opcje programistyczne. Funkcję tą można włączać na czas realizacji zadań służbowych, wymagających użycia tych opcji.
13. Urządzenie powinno mieć wyłączony tryb debugowania USB. Funkcję tą można włączać na żądanie i wyłączać po zakończeniu korzystania.
14. Urządzenie powinno mieć wyłączoną funkcję routera udostępniającego połączenie internetowe (Wi-Fi, Bluetooth, USB). Funkcję tą można włączać czasowo z użyciem hasła dostępowego i należy wyłączać po zakończonej transmisji.
15. Urządzenie powinno mieć wyłączoną opcję widoczności Bluetooth dla innych urządzeń w pobliżu. Funkcję tą można włączać na żądanie i należy wyłączać po zakończonej transmisji.
16. Urządzenie powinno mieć wyłączoną opcję sieci Wi-Fi. Funkcję tą można włączać na żądanie i należy wyłączać po zakończonej transmisji.
17. Urządzenie w ustawieniach musi mieć wprowadzoną nazwę zgodną z obowiązującą konwencją nazewniczą dla urządzeń mobilnych. Nazwa zostanie pokazana na innych urządzeniach gdy będzie dostępny do podłączenia przy użyciu Bluetooth, Wi-Fi Direct oraz innymi metodami (ustawienia > urządzenie – informacje > edytuj, podana ścieżka może różnić się w zależności od urządzenia i może znajdować się w ustawieniach połączeń bezprzewodowych).
18. Zabronione jest łączenie z niezabezpieczonymi sieciami Wi-Fi.
19. Konta prywatne służące do autoryzacji np. w usługach Google Play i AppGallery (Android), App Store (Apple), Microsoft Store (Microsoft) i innych (np. skrzynek pocztowych skojarzonych z usługami i aplikacjami w sieci Internet) mogą być stosowane na urządzeniach służbowych po warunkiem ich należytego zabezpieczenia przez użytkownika na wszystkich innych urządzeniach, na których mają zastosowanie poprzez: stosowanie silnych haseł, korzystanie z opcji dwuetapowego logowania, systematyczną kontrolę aktywnych sesji, kontrolę zdarzeń dotyczących prywatnych kont autoryzujących (dotyczy tylko TL i TS).
20. Aplikacje uznane jako potencjalnie niebezpieczne, niepożądane lub żądające zwiększonych uprawnień nie mogą być instalowane na urządzeniu. Aplikacje takie mogą zostać usunięte przez administratora.

21. Urządzenie lub autoryzacja na nim nie mogą być udostępniane osobom trzecim, w tym także współpracownikom i członkom rodziny. Urządzenie może zostać udostępnione administratorowi w celu przeprowadzenia właściwej konfiguracji, wykonania diagnozy lub ewentualnej naprawy.
22. Urządzenie należy chronić przed uszkodzeniem bądź zniszczeniem, a w przypadku pozostawienia bez nadzoru, przechowywać w bezpiecznym miejscu.
23. W przypadku zmiany użytkownika, likwidacji lub naprawy urządzenia w serwisie zewnętrznym wszelkie zapisane dane (aktywne sesje logowania, kontakty, wiadomości, multimedia i inne) nie mogą pozostawać w pamięci telefonu i kart. W tym celu urządzenie uprzednio powinno zostać przywrócone do stanu fabrycznego.
24. Urządzenie mobilne oraz jego obsługa powinny być zgodne z powyższymi ustawieniami, co najmniej w zakresie konfiguracji możliwych do realizacji.

5.2. Wymagania dodatkowe dla urządzeń TS i TA

Polityka bezpieczeństwa odnosząca się do konfiguracji urządzeń mobilnych będących własnością jednostek LP, wykorzystywane do przechowywania i przetwarzania danych służbowych oraz łączenia się z zasobami LP, stanowi uzupełnienie treści Zarządzenia w zakresie bezpieczeństwa urządzeń mobilnych, jest uzupełnieniem wymagań ogólnych i przedstawia się następująco:

1. Urządzenie musi być objęte kontrolą centralnego systemu zarządzania urządzeniami mobilnymi klasy EMM.
2. Blokada ekranu musi być włączona na poziomie minimum: średni (przynajmniej 6 cyfrowy PIN). Dopuszczalne metody: PIN, hasło, opcjonalna metoda biometryczna: odcisk palca.
3. Wyświetlanie zawartości powiadomień przy zablokowanym ekranie jest zabronione (widok szczegółowy: wyłączony, dopuszczone są tylko skróty i ikony powiadomień).
4. Zabrania się dodawania kont prywatnych w kontenerze firmowym (praca).

6. Lista aplikacji wewnętrznych wytworzonych przez/dla PGL LP (AppsLP)

Poniższe aplikacje należą do grupy **AppsLP** i wymagają rejestracji urządzenia z systemem Android wyłącznie w trybie COBO GPS lub COBO. Urządzenia takie przyjmują oznaczenie TA.

Lista urządzeń kompatybilna z AppsLP publikowana jest na portalu pracowniczym i Panelu Leśnika.

7. Obsługa sklepu korporacyjnego w systemie EMM

1) Akceptację, dodawanie oraz dystrybucję aplikacji w sklepie korporacyjnym LP Store realizuje DGLP.
2) Propozycje nowych aplikacji zgłaszają do DGLP Wydziały Informatyki na poziomie regionu lub zakładu o zasięgu krajowym zgodnie z przyjętą procedurą.
3) Aplikacje dostępne w sklepie korporacyjnym LP Store mogą być instalowane automatycznie i na żądanie przez użytkownika.
4) Lista widocznych aplikacji w sklepie korporacyjnym LP Store może różnić się w zależności od systemu operacyjnego urządzenia, trybu rejestracji urządzenia oraz grupy organizacyjnej, w której znajduje się urządzenie.

8. Konta prywatne

Konta prywatne mogą być stosowane na urządzeniu mobilnym typu TL i TS w zakresie niezbędnym do obsługi i konfiguracji urządzenia oraz pobierania aplikacji poza chronionym kontenerem firmowym. Dla urządzeń typu TA dodawanie kont jest zabronione. Wymogi dotyczące bezpieczeństwa kont

zostały opisane w dokumencie. PGL LP nie ponosi odpowiedzialności za nieprawidłową konfigurację konta osobistego na urządzeniu służbowym.

Sposób zakładania konta przedstawiony został w aktualnej instrukcji użytkownika systemu EMM do zarządzania urządzeniami mobilnymi w PGL LP.

Użytkownik przy zakładaniu kont ma obowiązek zapoznania się z regulaminem i informacjami dostawcy usługi w zakresie dostępnych metod zabezpieczenia niepowołanego dostępu do konta i jest zobowiązany do jego przestrzegania.

Poniżej ważne odnośniki w zależności od systemu operacyjnego:

Google Android

- **Dodawanie i używanie** konta Google na urządzeniu https://support.google.com/googleplay/answer/2521798?hl=pl
- **Zmienianie i resetowanie hasła** na koncie Google https://support.google.com/accounts/answer/41078?hl=pl
- **Zwiększanie bezpieczeństwa** konta Google https://support.google.com/accounts/answer/46526?hl=pl

W przypadku niedostępności bezpośrednich odnośników należy skorzystać z wyszukiwarki na stronie wsparcia https://support.google.com/accounts?hl=pl

iOS

- **Dodawanie i używanie** konta Apple ID na urządzeniu https://support.apple.com/pl-pl/HT204316
- **Zmienianie i resetowanie hasła** na koncie Apple ID https://support.apple.com/pl-pl/HT201355
- **Zwiększanie bezpieczeństwa** konta Apple ID https://support.apple.com/pl-pl/HT201303

W przypadku niedostępności bezpośrednich odnośników należy skorzystać z wyszukiwarki na stronie wsparcia https://support.apple.com/pl-pl

9. Urządzenia z systemem iOS

1) Dla urządzeń oznaczonych jako TL dopuszcza się stosowanie urządzeń z systemem iOS.
2) Dla urządzeń oznaczonych jako TS dopuszcza się stosowanie urządzeń z systemem iOS z zachowaniem podstawowego dostępu do poczty PGL LP i WebSILP.
3) Urządzenia z systemem iOS muszą mieć ustawiony co najmniej ten sam poziom zabezpieczeń dotyczący blokady ekranu i pozostałych ustawień urządzenia.
4) Z uwagi na ograniczone możliwości zarządzania systemem iOS urządzenia te nie są zalecane do pracy służbowej w PGL LP.