

INSTRUKCJA

w sprawie prowadzenia i przyznawania dostępu do systemu informatycznego *Ewidencja ZHP* oraz trybu powoływania administratorów bezpieczeństwa informacji

Postanowienia ogólne

1. Podstawę prawną wydania niniejszej instrukcji stanowi § 18 Statutu ZHP.
2. Postanowienia niniejszej instrukcji, w których mowa o harcerzu, harcerzu starszym, wędrowniku, instruktora, stosuje się odpowiednio do harcerek, harcerek starszych, wędrowniczek, instruktorek.
3. Przepisy niniejszej instrukcji dotyczące instruktorów stosuje się odpowiednio do wędrowników i starszyny, pełniących funkcje instruktorskie.
4. Jeżeli w niniejszej instrukcji jest mowa o właściwym komendancie, należy przez to rozumieć komendanta hufca, komendanta chorągwi, naczelnika ZHP, określającego przydział służbowy członka ZHP.
5. Jeżeli w niniejszej instrukcji jest mowa o właściwym ABI, należy przez to rozumieć administratora bezpieczeństwa informacji w myśl ustawy o ochronie danych osobowych mianowanym przez właściwego komendanta.
6. Jeżeli w niniejszej instrukcji jest mowa o *Ewidencja ZHP*, należy przez to rozumieć zbiór systemów informatycznych „Elektroniczny system harcerskich danych” zawierających rejestr członków i jednostek, zwanym dalej *Ewidencja ZHP*, jak również inne moduły aplikacyjne korzystające z jej zasobów.
7. Jeżeli w niniejszej instrukcji jest mowa o uprawnieniach w systemie, należy przez to rozumieć system *Ewidencja ZHP*.
8. Jeżeli w niniejszej instrukcji jest mowa o administratorze systemu, należy przez to rozumieć osobę wskazaną przez Naczelnika ZHP posiadającą uprawnienia do całości aplikacji.
9. Jeżeli w niniejszej instrukcji jest mowa o administratorze lokalnym, należy przez to rozumieć osobę wskazaną przez właściwego komendanta posiadającą uprawnienia do poziomu, na który został mianowany.
10. Jeżeli w niniejszej instrukcji jest mowa o właściwym administratorze, należy przez to rozumieć administratora lokalnego na poziomie hufca, Administratora lokalnego na poziomie chorągwi, Administratora lokalnego na poziomie Głównej Kwatery lub administratora systemu *Ewidencja ZHP* poziomie ZHP.
11. Jeżeli w niniejszej instrukcji jest mowa o dostępie do systemu, należy przez to rozumieć przyznanie uprawnień użytkownikowi pozwalających na zmianę danych w systemie *Ewidencja ZHP*, bez prawa zakładania użytkowników i przydzielania im dalszych uprawnień.
12. Jeżeli w niniejszej instrukcji jest mowa o uprawnieniach administracyjnych dostępu do systemu, należy przez to rozumieć uprawnienia użytkownika pozwalające na zmianę danych w systemie *Ewidencja ZHP* wraz z prawem zakładania użytkowników i przydzielania im dalszych uprawnień.
13. Jeżeli w niniejszej instrukcji jest mowa o katalogu funkcji, należy przez to rozumieć spis funkcji w ZHP, zatwierdzonych przez GK jako funkcje podlegające rejestracji w systemie *Ewidencja ZHP*.
14. System informatyczny *Ewidencja ZHP* i jest obowiązkowym elektronicznym obrazem rejestrów członków i jednostek ZHP.

System *Ewidencja ZHP* służy do elektronicznego rejestrowania następujących zdarzeń dotyczących członków ZHP:

1. Zmian w rejestrach zuchów, harcerzy, harcerzy starszych, wędrowników, instruktorów (w tym seniorów), starszyny (w tym seniorów) i działaczy.
2. Zmian przydziału służbowego i przynależności do poszczególnych jednostek.
3. Pełnionych funkcji w ZHP zgodnie z katalogiem funkcji.
4. Posiadanych stopni i sprawności zgodne z instrukcjami i Statutem ZHP.
5. Posiadanych odznak i odznaczeń.
6. Ukończonych kursów i warsztatów organizowanych przez CSI oraz zespołu kadry kształcącej do poziomu hufca włącznie, w tym odznak kadry kształcącej.
7. Posiadanych uprawnień państwowych i harcerskich.
8. Złożonej obietnicy zucha, przyrzeczenia harcerskiego i zobowiązania instruktorskiego.
9. Wydania książeczki zuchowej, harcerskich, instruktorskich, działaczy.

Prowadzenie systemu *Ewidencja ZHP*.

1. Dostęp do systemu otrzymują:
 - w podstawowej jednostce organizacyjnej - kierujący podstawową jednostką organizacyjną,
 - w szczepie - komendant szczepu,
 - w związku drużyn - komendant związku drużyn,
 - w hufcu
 - komendant hufca i inni funkcyjni wskazani przez komendanta hufca po uzyskaniu aprobaty ABI na poziomie chorągwi i uzyskaniu uprawnień adekwatnych do pełnionej funkcji.
 - administrator lokalny systemu *Ewidencja ZHP* - w zakresie nadawania uprawnień instruktorom w hufcu.
 - w chorągwi
 - komendant chorągwi i inni funkcyjni wskazani przez komendanta chorągwi po uzyskaniu aprobaty ABI na poziomie Głównej Kwatery i uzyskaniu uprawnień adekwatnych do potrzeb,
 - administrator lokalny systemu *Ewidencja ZHP* - w zakresie nadawania uprawnień instruktorom w Chorągwi.
 - w Głównej Kwaterze ZHP
 - naczelnik ZHP
 - kierownicy wydziałów wskazani przez Naczelnika ZHP i uzyskaniu uprawnień adekwatnych do potrzeb.
 - inni funkcyjni GK wskazani przez naczelnika ZHP, o ile dostęp do systemu jest im niezbędny do realizacji celów statutowych ZHP i uzyskaniu uprawnień adekwatnych do potrzeb,
 - członkowie zespołu „ESH” wskazani przez naczelnika ZHP po uzyskaniu uprawnień adekwatnych do potrzeb,
 - administratorzy systemu *Ewidencja ZHP*.

Dane statyczne i wykaz jednostek nie zawierające danych osobowych, w tym dane teleadresowe jednostek są dostępne bez logowania.

2. Każda osoba, która z mocy instrukcji lub upoważnienia właściwego komendanta ma otrzymać dostęp do systemu musi spełniać łącznie następujące warunki:
 - być członkiem ZHP,
 - mieć ukończone 18 lat. (w uzasadnionych przypadkach właściwy komendant może, za zgodą opiekuna z ramienia ZHP, upoważnić członka ZHP pełniącego funkcję drużynowego, który ma ukończone 16 lat),

- ukończyć szkolenie w zakresie ochrony danych osobowych,
 - posiadać upoważnienie do przetwarzania danych osobowych w systemach informatycznych ZHP wystawione przez właściwego komendanta.
3. Za rzetelne i terminowe prowadzenie systemu *Ewidencja ZHP* w jednostkach odpowiedzialni są:
 - w podstawowej jednostce organizacyjnej - kierujący podstawową jednostką organizacyjną,
 - w szczepie i podległych mu jednostkach - komendant szczepu
 - w związku drużyn i podległych mu jednostkach - komendant związku drużyn,
 - w hufcu i podległych mu jednostkach - komendant hufca,
 - w chorągwi i podległych mu jednostkach - komendant chorągwi,
 - w Głównej Kwaterze ZHP i podległych jej jednostkach - naczelnik ZHP
 4. Właściwy komendant ma prawo z ważnych przyczyn odmówić dostępu do systemu członkowi ZHP, który powinien posiadać prawo dostępu z mocy instrukcji, jednocześnie wskazując mu osobę, która będzie miała dostęp do danych i która będzie miała obowiązek w jego imieniu na jego wniosek te dane aktualizować.
 5. Za ważne przyczyny do odmowy dostępu do systemu uważa się:
 - niepełnoletność członka ZHP pełniącego funkcję instruktorską - w takim przypadku właściwy komendant przyznaje prawo dostępu do systemu *Ewidencja ZHP* jego pełnoletniemu opiekunowi z ramienia ZHP,
 - nieprzestrzeganie przez członka ZHP ustawy o ochronie danych osobowych i dokumentów wewnętrznych w tym zakresie, w tym polityki bezpieczeństwa i instrukcji przetwarzania danych osobowych w systemach informatycznych,
 - notoryczne problemy z hasłem lub udostępnianie go osobie trzeciej,
 - brak przeszkolenia w zakresie obsługi aplikacji,
 - brak przeszkolenia z zakresu ochrony danych osobowych,
 - notoryczne i uporczywe nie aktualizowanie systemu *Ewidencja ZHP*,
 - w innych uzasadnionych przypadkach - decyzją naczelnika ZHP.
 6. Centralna Szkoła Instruktorska w porozumieniu z ABI GK ZHP określa tematykę szkolenia z zakresy ochrony danych osobowych i prowadzi nadzór nad systemem szkoleń w ZHP.

Funkcja administratora bezpieczeństwa informacji.

1. Naczelnik, komendant chorągwi, zobligowani są do mianowania podległych im administratorów bezpieczeństwa informacji w swoich jednostkach. W przypadku niemianowania ABI przez właściwego komendanta, przyjmuje się, iż funkcję administratora bezpieczeństwa informacji pełni osobiście naczelnik, komendant chorągwi.
2. Funkcja ABI odnosi się do wszystkich sposobów przetwarzania danych osobowych w danej jednostce, również w systemach innych niż *Ewidencja ZHP* oraz w dokumentacji w formie papierowej.
3. Nie jest możliwe łącznie funkcji administratora systemu *Ewidencja ZHP* oraz administratora lokalnego systemu *Ewidencja ZHP* z funkcją ABI, niezależnie od poziomu pełnienia tych funkcji.
4. W uzasadnionych przypadkach właściwy komendant może powołać Zespół do spraw ochrony danych osobowych. Szefem takiego zespołu jest zawsze ABI, który określa kompetencje zespołu. Zespół ten może jedynie wpierać ABI w jego obowiązkach. ABI odpowiada za działania upoważnionych członków zespołu jak za własne.
5. Szczególne obowiązki ABI:

- znajomość przepisów o ochronie danych osobowych i rozporządzeń wykonawczych, w tym dokumentów wewnętrznych ZHP.
- przygotowywanie analiz wskazanych przez właściwego komendanta zbiorów baz danych pod względem zgodności z wymaganiami prawa i zaleceniami pod kątem ochrony danych, przed ich utratą oraz nieuprawnionym dostępem,
- prowadzenie analizy zagrożeń i ryzyka związanych z przetwarzaniem danych osobowych, które winny obejmować cały proces przetwarzania danych osobowych,
- określanie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.
- nadzór nad sposobami fizycznego i organizacyjnego zabezpieczenia pomieszczeń oraz informatycznego zabezpieczenia systemów komputerowych baz danych, w których przetwarzane są dane osobowe,
- nadzór nad funkcjonowaniem awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych osobowych,
- nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych służących do przetwarzania danych osobowych,
- prowadzenie szkoleń użytkowników systemu (wprowadzających i przypominających) w zakresie ochrony danych osobowych,
- nadzór nad przydzielaniem użytkownikom wskazanym przez właściwego komendanta określonych przez niego uprawnień w systemie, prowadzenie rejestru użytkowników zawierającego imię i nazwisko, stanowisko, login, zakres uprawnień,
- zarządzanie hasłami użytkowników i nadzór nad przestrzeganiem procedur określających częstotliwość ich zmiany oraz stopień złożoności zgodnie z wytycznymi,
- okresowe weryfikacje i nadzór nad procedurami nadawania uprawnień do przetwarzania danych osobowych,
- współudział w określeniu miejsc i sposobów przechowywania:
 - elektronicznych nośników informacji zawierających dane osobowe,
 - kopii zapasowych.
- nadzór nad wykonywaniem (częstość, jakość, okresowa wymiana nośników) kopii baz danych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem dalszej przydatności do odtwarzania danych w przypadku awarii systemu,
- nadzór i koordynowanie odtwarzania zbioru danych z kopii baz danych w każdej sytuacji wymagającej takiego odtworzenia; przeanalizowanie przyczyny i przedstawienie wniosków właściwemu komendantowi,
- nadzór nad przeglądami, konserwacjami oraz uaktualnieniami systemów służących do przetwarzania danych osobowych oraz wszystkimi innymi czynnościami wykonywanymi na bazach danych osobowych; komunikacja z firmami serwisowymi winna być prowadzona za pośrednictwem lub przy współudziale administratora bezpieczeństwa Informacji,
- nadzór nad obiegiem oraz przechowywaniem i niszczeniem dokumentów i wydawnictw zawierających dane osobowe generowane przez systemy informatyczne,

- podjęcie natychmiastowych działań zabezpieczających stan systemu informatycznego oraz odpowiednich dokumentów w przypadku otrzymania informacji o naruszeniu zabezpieczeń systemu informatycznego lub informacji o zmianach w sposobie działania programu lub urządzeń wskazujących na naruszenie bezpieczeństwa danych,
- analiza sytuacji, okoliczności i przyczyn, które doprowadziły do naruszenia bezpieczeństwa danych, przygotowanie oraz przedstawienie właściwemu komendantowi odpowiednich wniosków,
- śledzenie publikacji dotyczących przetwarzania danych osobowych, proponowanie wdrożenia odpowiednich rozwiązań technicznych i organizacyjnych,
- prowadzenie dokumentacji wymaganej przepisami prawa, przygotowywanie projektów dokumentów dotyczących procedur, zasad i zaleceń bezpieczeństwa komputerowych baz danych,
- bieżące informowanie właściwego komendanta lub ABI na wyższym poziomie o postępach prac, napotkanych trudnościach oraz podejmowanych środkach zabezpieczających wykonanie zadania.

Procedury nadawania i unieważniania uprawnień oraz generowanie haseł startowych dla systemu *Ewidencja ZHP*.

1. Niedopuszczalne jest przetwarzania danych w systemie przez osoby nieupoważnione i niebędące członkami ZHP.
2. Nadzór nad przebiegiem nadawania uprawnień i haseł sprawuje właściwy ABI lub w przypadku jego niepowołania właściwy komendant.
3. Naczelnik ZHP wyznacza administratora systemu *Ewidencja ZHP*, po zasięgnięciu opinii administratora bezpieczeństwa informacji na poziomie GK.
4. Funkcję administratora systemu *Ewidencja ZHP* może pełnić jedynie osoba pełnoletnia, której Naczelnik ZHP powierzył funkcję pisemnie określając jej zakres obowiązków i odpowiedzialności. Administrator jest zobowiązany do pisemnego potwierdzenia przyjęcia obowiązków i podpisanie zobowiązania do ochrony systemu i danych w nim zawartych.
5. Komendant hufca, chorągwi i naczelnik ZHP mianują administratora lokalnego do prowadzenia systemu.
6. Administrator lokalny jest odpowiedzialny za przyznawanie dostępu do systemu innym użytkownikom.
7. Lokalny administrator ma możliwość przydzielania dostępu do systemu tylko na niższym poziomie.
8. Lokalny administrator może nadawać uprawnienia administracyjne innym użytkownikom systemu na wniosek:
 - właściwego komendanta - administrator systemu dla administratora lokalnego na każdym poziomie,
 - komendanta chorągwi - administrator lokalny na poziomie GK dla administratora lokalnego na poziomie chorągwi,
 - komendanta hufca - administrator lokalny na poziomie chorągwi dla administratora lokalnego,
 Administrator lokalny na poziomie hufca nie może delegować swoich uprawnień administracyjnych na inne osoby.
9. W każdym hufcu, chorągwi i GK nadanie uprawnień administratora lokalnego większej liczbie osób jest możliwe wyłącznie na podstawie łącznej zgody tych osób. W takim przypadku osoby te odpowiadają solidarnie za stan dokumentacji wymaganej instrukcją, jak również za wykonanie czynności administracyjnych.

10. Każdej osobie posiadającej dostęp do systemu właściwy administrator przydziela uprawnienia najmniejsze z możliwych, umożliwiające wykorzystanie systemu zgodnie z pełnioną funkcją oraz przydziela hasła startowe. Katalog funkcji, zgodnie z którym przydzielane są uprawnienia oraz zakres obowiązków określa GK ZHP.
11. Przyznanie dostępu do systemu jest możliwe tylko dla członków ZHP posiadającym swoje dane osobowe w systemie, dla konkretnej przypisanej im funkcji w konkretnej jednostce ZHP. W przypadku pełnienia większej liczby funkcji w różnych jednostkach administrator lokalny nadaje dodatkowe uprawnienia do innych jednostek.
12. Właściwy komendant upoważnia osobę do przetwarzania danych osobowych i określa jej uprawnienia w aplikacji w zależności od pełnionej funkcji. Upoważnienie pod rygorem nieważności musi posiadać formę pisemną.
13. Właściwy administrator systemu generuje hasło startowe i ustawia dostęp do systemu do jednostki wskazanej przez właściwego komendanta na dokumencie *Upoważnienie do przetwarzania danych osobowych* w systemie oraz generuje z systemu protokół przekazania hasła startowego i zobowiązanie do przestrzegania przepisów odnośnie ochrony danych osobowych. Zobowiązanie podpisane przez upoważnionego do przetwarzania danych dołącza się do dokumentacji.
14. Nie jest możliwe odebranie hasła startowego i podpisanie zobowiązania w innej formie jak tylko osobiście po wylegitymowaniu przez upoważnioną osobę. Administrator lokalny za pomocą biura właściwego komendanta może przekazać hasło startowe w kopercie zabezpieczonej przed nieautoryzowanym dostępem.
15. Użytkownik ma obowiązek zmienić otrzymane hasło startowe przy pierwszym logowaniu się do systemu i nie udostępniać go osobie trzeciej.
16. system wymusza zmianę hasła startowego na inne znane tylko użytkownikowi.
17. Hasła startowe muszą zawierać co najmniej 10 znaków, w tym duże i małe litery, cyfry i znaki specjalne. Szczegółowe instrukcje generowania haseł zawiera *Instrukcja przetwarzania danych osobowych w systemie*.
18. Dostęp do systemu wygasa w przypadku:
 - wygaśnięcia mandatu - jeżeli dostęp przyznany był instruktorowi z racji jego pełnienia,
 - rezygnacji lub odwołania z funkcji - jeżeli dostęp do systemu został przyznany z racji pełnienia funkcji,
 - wycofania upoważnienia komendanta do dostępu do systemu *Ewidencja ZHP* - jeżeli dostęp do systemu został przyznany decyzją właściwego komendanta,
 - rezygnacji, skreślenia z listy członków lub wykluczenia z ZHP.
19. W przypadku wygaśnięcia dostępu do systemu właściwy komendant niezwłocznie poinformuje administratora lokalnego, a ten ma obowiązek wprowadzić zmianę w systemie nie później niż w ciągu 24 godzin od daty wygaśnięcia uprawnień.
20. W przypadku braku możliwości wprowadzenia zmiany przez administratora lokalnego właściwy komendant powiadamia administratora systemu na wyższym poziomie.
21. Właściwy komendant ma obowiązek zawiesić dostęp do systemu członkowi ZHP i zawiadomić właściwy sąd harcerski w następujących przypadkach:
 - wprowadzania przez użytkownika do systemu danych osób niebędących członkami ZHP lub innych danych nie mających odzwierciedlenia w rzeczywistości - potwierdzania nieprawdy,
 - udostępnianie danych z systemu *Ewidencja ZHP* osobom do tego nieupoważnionym,

- próby wykorzystania otrzymanego dostępu do łamania zabezpieczeń systemu.
22. W przypadku potwierdzenia przez właściwy sąd powyższych faktów właściwy komendant ma obowiązek zawiadomić organy ścigania.

Obowiązki użytkownika systemu *Ewidencja ZHP*.

1. Użytkownik ma obowiązek sumiennie i zgodnie ze stanem faktycznym na bieżąco (nie rzadziej niż raz w miesiącu) uzupełniać dane w systemie *Ewidencja ZHP*.
2. Użytkownik ma obowiązek generowania okresowo haseł (nie rzadziej niż co 30 dni) spełniających następujące kryteria: co najmniej 10 znaków, w tym duże i małe litery, cyfry i znaki specjalne.
3. Użytkownik jest zobowiązany otrzymane hasło zachować w poufności, strzec przed ujawnieniem.
4. W przypadku ujawnienia hasła użytkownik zobowiązany jest bez zbędnej zwłoki zmienić na inne, znane tylko sobie.
5. Niedopuszczalne jest posługiwanie się loginem i hasłem należącym do innej osoby.

Procedury wprowadzania, edycji danych i rozdział kompetencji.

Wprowadzanie nowych danych

1. Do systemu dodaje:
 - nowego członka zwyczajnego - kierujący podstawową jednostką organizacyjną w ciągu 30 dni od deklaracji członka o przynależności do jednostki, ustawiając mu jednocześnie przydział służbowy do swojej jednostki.
 - nowego członka starszyny - właściwy komendant lub upoważniona przez niego osoba w ciągu 30 dni od deklaracji.
 - nowego instruktora - właściwy komendant lub upoważniona przez niego osoba w ciągu 30 dni od złożenia deklaracji.

Właściwy Administrator może w uzasadnionych przypadkach wprowadzać nowych członków, do swojego poziomu włącznie w zastępstwie osób do tego umocowanych.
2. Nową podstawową jednostkę wprowadza do systemu właściwy administrator w ciągu 7 dni od daty ukazania się rozkazu:
 - wpisuje nazwę i numer jednostki - z określeniem jej statusu np. próbna.
 - dodaje mianowanemu członkowi ZHP na funkcje kierującego jednostką informacje o pełnionej funkcji,
 - dodaje uprawnienia do edycji danych jednostki,
 - dodaje uprawnienia do dodawania nowych członków ZHP oraz możliwość przypisywania przynależności do jednostki i edycji ich danych.
3. Nowy szczebel dodaje do systemu właściwy administrator lokalny w ciągu 7 dni od daty ukazania się rozkazu, przypisując istniejące już w systemie jednostki do nowego szczebla.
4. Nowy związek drużyn dodaje do systemu właściwy administrator lokalny w ciągu 7 dni od daty ukazania się rozkazu, przypisując istniejące już w systemie jednostki do nowego związku drużyn.
5. Nowy hufiec dodaje administrator lokalny chorągwi lub GK w ciągu 7 dni od daty ukazania się rozkazu, przypisując istniejące już w systemie jednostki do nowego hufca.
6. Nową chorągiew dodaje administrator lokalny GK w ciągu 7 dni od daty ukazania się rozkazu, przypisując istniejące już w systemie jednostki do nowej chorągwi.

Edycja danych w systemie

1. Każda edycja danych jest rejestrowana przez system.

2. Prawo do edycji danych posiadają:
 - użytkownik dopuszczony do pracy z systemem do poziomu jego uprawnień włącznie,
 - właściwy administrator systemu do swojego poziomu włącznie.

Rejestrowanie zmiany przydziału służbowego członka ZHP

1. Rejestrowanie zmian przydziału służbowego wymaga od:
 - kierującego jednostką, dotychczasowego przełożonego - odnotowanie w systemie faktu zgłoszenia informacji o zmianie przydziału - niezwłocznie - jednak nie później niż w ciągu 14 dni,
 - kierującego jednostką, który przyjmuje członka ZHP, dodania członka do swojej jednostki - niezwłocznie - jednak nie później niż w ciągu 14 dni.
2. Operacji powyższej, na podstawie zgody kierujących jednostką, może dokonać właściwy administrator.

Dopisanie członkowi, mającego przydział służbowy w innej jednostce, przynależności do kolejnej jednostki

1. Rejestrowanie dodatkowej przynależności wymaga od:
 - kierującego jednostką, aktualnego przełożonego - odnotowania w systemie faktu zgłoszenia informacji o dodatkowej przynależności - niezwłocznie - jednak nie później niż w ciągu 14 dni,
 - kierującego jednostką, który przyjmuje członka ZHP, dodania członka do swojej jednostki - niezwłocznie - jednak nie później niż w ciągu 14 dni.
2. Operacji powyższej, na podstawie zgody kierujących jednostką, może dokonać właściwy administrator.

Rejestrowanie zmiany przydziału służbowego instruktora ZHP

1. Rejestrowanie zmian przydziału służbowego wymaga od:
 - członka starszyny, instruktora - poinformowania właściwego komendanta, że zamierza zmienić przydział służbowy,
 - właściwego komendanta, dotychczasowego przełożonego odnotowania w systemie faktu zgłoszenia informacji o zmianie przydziału - niezwłocznie - jednak nie później niż w ciągu 14 dni,
 - właściwego komendanta, który przyjmuje członka starszyny, instruktora ZHP, dodania członka starszyny, instruktora do swojej jednostki i ustanowienie mu nowego przydziału - niezwłocznie - jednak nie później niż w ciągu 14 dni.
2. Operacji powyższej, na podstawie informacji od właściwego komendanta, może dokonać właściwy administrator, którego uprawnienia obejmują obie jednostki.

Objęcie przez członka starszyny, instruktora ZHP mającego przydział służbowy w innej jednostce funkcji w innej jednostce:

1. Rejestracja podjęcia dodatkowej funkcji wymaga od:
 - instruktora - poinformowania właściwego komendanta, że zamierza podjąć funkcję w innej jednostce,
 - właściwego komendanta, dotychczasowego przełożonego odnotowania w systemie faktu zgłoszenia informacji o podjęciu funkcji - niezwłocznie - jednakże nie później niż w ciągu 14 dni,
 - właściwego komendanta, który powierza funkcję członkowi starszyny, instruktorowi ZHP, dodania członka starszyny, instruktorowi do swojej jednostki i ustanowienie mu nowej funkcji - niezwłocznie - jednakże nie później niż w ciągu 14 dni.

Przenoszenie danych o członkach ZHP do archiwum

1. Dane o członkach przenoszone są do archiwum niezwłocznie, jednak nie później niż 7 dni od daty ogłoszenia w rozkazie informacji o ustaniu członkostwa.
2. Przeniesienie danych do archiwum może dokonać:
 - członka zwyczajnego - kierujący podstawową jednostką organizacyjną - niezwłocznie, nie później jednak niż w ciągu 30 dni od ustania członkostwa,
 - członka zwyczajnego pełniącego funkcję instruktorską, członka starszyny oraz instruktora - właściwy komendant lub upoważniona przez niego osoba - niezwłocznie, jednak nie później niż w ciągu 30 dni od ustania członkostwa.
3. Przeniesienie danych do archiwum (procedura ustania członkostwa) jest możliwe jeżeli:
 - członkowi zakończono przynależność do wszystkich jednostek,
 - wprowadzono datę zakończenia pełnienia funkcji wcześniejszą niż data ustania członkostwa dla każdej aktywnej funkcji,
 - wprowadzono do systemu datę i rodzaj ustania członkostwa,
 - dane członka nie są wprowadzone do systemu w wyniku błędu operatora.

Przenoszenie danych o jednostkach do archiwum

1. Dane o rozwiązanych jednostkach przenoszone są do archiwum niezwłocznie, jednak nie później niż 7 dni od daty ogłoszenia w rozkazie informacji o rozwiązaniu.
2. Przeniesienia do archiwum może dokonać jedynie właściwy administrator lokalny do swojego poziomu włącznie.
3. Przeniesienie danych do archiwum (procedura rozwiązania jednostki) jest możliwe jeżeli:
 - nie ma przypisanych członków ZHP do tej jednostki,
 - wszystkim członkom, którzy pełnili w niej funkcję wprowadzono datę zakończenia pełnienia funkcji wcześniejszą niż data rozwiązania jednostki,
 - nie są do niej przypisane żadne jednostki podległe,
 - nie jest wprowadzona w wyniku błędu operatora.

Usunięcie danych jednostki z systemu

1. Usunięcie danych wprowadzonej jednostki jest możliwe w przypadku, gdy nie ma przypisanych do niej członków lub podległych innych jednostek i jest następstwem błędnego wprowadzenia danych do systemu. Niedopuszczalne jest usuwanie z systemu danych o jednostkach rozwiązanych. W przypadku rozwiązania jednostek należy przenieść dane do archiwum.
2. Jednostkę może usunąć właściwy administrator lokalny do swojego poziomu.
3. Usunięcie jednostki hufiec, chorągiew, jest możliwe jedynie przez administratora systemu *Ewidencja ZHP*, uprzednim przeniesieniem danych do właściwej jednostki organizacyjnej.

Usunięcie danych członka ZHP z systemu

1. Usunięcie danych członka jest możliwe w przypadku, gdy nie ma przypisanych funkcji, nie należy do żadnej jednostki i jest następstwem błędnego wprowadzenia danych do systemu. Niedopuszczalne jest usuwanie z systemu danych o członkach ZHP, którzy odeszli, zostali skreśleni lub wykluczeni z ZHP. W takim przypadku należy wprowadzić informację o ustaniu członkostwa i przenieść dane do archiwum.
2. Błędnie wprowadzone dane o członku ZHP może usunąć administrator lokalny na poziomie chorągwi, GK lub administrator systemu.