ZARZĄDZENIE NR 24/2022
REKTORA-KOMENDANTA SZKOŁY GŁÓWNEJ SŁUŻBY POŻARNICZEJ
z dnia 24 marca 2022 r.

w sprawie wprowadzenia Polityki Bezpieczeństwa Systemów Informatycznych w Szkole Głównej Służby Pożarniczej

Na podstawie ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781, z późn. zm.) oraz rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r. poz. 2274, z późn. zm.), zarządza się, co następuje:

§ 1.

1. W Szkole Głównej Służby Pożarniczej (dalej „SGSP") wprowadza się Politykę Bezpieczeństwa Systemów Informatycznych, zwaną dalej „Polityką Bezpieczeństwa", stanowiącą załącznik do niniejszego zarządzenia.
2. Aktualizacji Polityki Bezpieczeństwa dokonuje kierownik Działu IT.

§ 2.

Zobowiązuje się kierowników jednostek organizacyjnych SGSP do zapoznania funkcjonariuszy i pracowników z Polityką Bezpieczeństwa Systemów Informatycznych w Szkole Głównej Służby Pożarniczej.

§ 3.

1. Uchyla się Instrukcję Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych, stanowiącą załącznik nr 4 do Polityki Ochrony Danych Osobowych w Szkole Głównej Służby Pożarniczej, wprowadzoną zarządzeniem nr 26/18 Rektora-Komendanta Szkoły Głównej Służby Pożarniczej z dnia 22 maja 2018 r.
2. Traci moc:
   1) zarządzenie nr 39/18 Rektora-Komendanta Szkoły Głównej Służby Pożarniczej z dnia 6 września 2018 r. w sprawie ustalenia regulaminu korzystania z zasobów informatycznych sieci komputerowej oraz komputerów służbowych;
   2) zarządzenie nr 17/17 Rektora-Komendanta Szkoły Głównej Służby Pożarniczej z dnia 21 marca 2017 r. w sprawie ustalenia regulaminu studenckiej sieci bezprzewodowej.

§ 4.

Zarządzenie wchodzi w życie z dniem podpisania.

REKTOR- KOMENDANT
nadbryg. dr inż. Mariusz FELTYNOWSKI, prof. uczelni

Załącznik
do zarządzenia nr 24/2022
Rektora-Komendanta SGSP
z dnia 24 marca 2022 r.

POLITYKA BEZPIECZEŃSTWA SYSTEMÓW INFORMATYCZNYCH W SZKOLE GŁÓWNEJ SŁUŻBY POŻARNICZEJ

Opracował:

st. bryg. dr inż. Rafał Turkiewicz

Administrator Bezpieczeństwa
Systemów - kierownik Działu IT

Warszawa, marzec 2022 r.

Rejestr zmian dokumentu

Lp.	Dokument, w którym wprowadzono zmiany	Rozdział/paragraf/ustęp /punkt/strona	Zakres/treść zmiany	Data wprowadzenia zmiany	Zaktualizował (podpis ABS-kierownika Działu IT)
1					
2					
3					
4					
5					

Spis treści:

Załączniki:

Nr 1. Oświadczenie podmiotu zewnętrznego w związku uzyskaniem zdalnego dostępu do zasobów SGSP

Nr 2. Rejestr awarii i naruszeń bezpieczeństwa

Nr 3. Instrukcja Zarządzania Systemem Informatycznym (załącznik wyłącznie dla administratorów)

Nr 4. Regulamin Sieci Informatycznej

Rozdział 1.
Postanowienia ogólne

§ 1.
Definicje

1. Użyte w niniejszej Polityce Bezpieczeństwa Systemów Informatycznych Szkoły Głównej Służby Pożarniczej (dalej „SGSP") pojęcia i skróty oznaczają:
   1) ABS - Administrator Bezpieczeństwa Systemów-kierownik Działu IT w SGSP odpowiedzialny za bezpieczeństwo i odpowiednie funkcjonowanie systemów informatycznych;
   2) AD - Administrator Dziedzinowy - Pracownik spoza Działu IT w SGSP lub podmiot zewnętrzny, upoważniony do administrowania określonym Oprogramowaniem dziedzinowym;
   3) ASI - Administrator Systemu Informatycznego - pracownik Działu IT w SGSP, wyznaczony przez ABS do realizacji zadań dotyczących bezpieczeństwa oprogramowania i bezpieczeństwa infrastruktury sieciowej;
   4) Dział IT - dział odpowiedzialny za obszar IT w SGSP;
   5) Gość - osoba w jakikolwiek sposób użytkującą systemy informatyczne w SGSP, inna niż Pracownik lub podmiot zewnętrzny;
   6) Help-Desk - system informatyczny przeznaczony do przyjmowania przez Dział IT zgłoszeń serwisowych i zgłoszeń o incydentach informatycznych, dostępny na komputerach służbowych przydzielonych Pracownikom;
   7) Incydent bezpieczeństwa - każde potwierdzone naruszenie przez Pracowników (lub osoby trzecie), bezpieczeństwa informacji przetwarzanych w systemach informatycznych lub zasad ich użytkowania;
   8) KJO - kierownik jednostki organizacyjnej SGSP lub osoba zatrudniona na samodzielnym stanowisku, zgodnie ze strukturą organizacyjną SGSP określoną w Regulaminie Organizacyjnym SGSP lub osoba zastępująca kierownika jednostki organizacyjnej SGSP lub osobę zatrudnioną na samodzielnym stanowisku pracy;
   9) Oprogramowanie dziedzinowe - oprogramowanie przeznaczone do świadczenia usług tylko dla określonego obszaru działalności SGSP;
   10) PBSI - Polityka Bezpieczeństwa Systemów Informatycznych w SGSP;
   11) podmiot zewnętrzny - osoba fizyczna prowadząca działalność gospodarczą, osoby prawne, jednostki organizacyjne nieposiadające osobowości prawnej, które łączy z SGSP umowa cywilno-prawna;
   12) PODO - Polityka Ochrony Danych Osobowych SGSP;
   13) Pracownik - osoba pozostająca z SGSP w stosunku pracy lub służby, w tym osoba fizyczna, którą łączy z SGSP umowa cywilno-prawna;
   14) PSP - Państwowa Straż Pożarna;
   15) Regulamin Sieci Informatycznej - zbiór zasad korzystania z systemów informatycznych przez Gości;
   16) Standardowe oprogramowanie systemowe - oprogramowanie tworzące środowisko, w którym uruchamiane jest Oprogramowanie dziedzinowe;
2. Pozostałe terminy, niezdefiniowane w ust. 1, pisane z małych liter należy rozumieć zgodnie z ich ogólnie przyjętym znaczeniem.

§ 2.

1. PBSI określa zasady użytkowania oraz zarządzania bezpieczeństwem systemów informatycznych, tj. sprzętu, oprogramowania i sieci teleinformatycznych w SGSP.
2. Dokument jest przeznaczony dla wszystkich Pracowników, z wyjątkiem Instrukcji Zarządzania Systemem Informatycznym (stanowiącym załącznik nr 3), która jest przeznaczona wyłącznie dla ASI i AD. Pozostałych użytkowników dotyczą postanowienia Regulaminu Sieci Informatycznej (stanowiący załącznik nr 4 do PBSI).
3. Przy doborze środków i metod ochrony systemów informatycznych, o których mowa w niniejszym dokumencie, należy uwzględniać:
   a) założenia Polityki Ciągłości Działania SGSP dotyczące obszaru teleinformatyki związane z zapewnieniem ciągłości realizacji procesów dydaktycznych oraz wykonywania zadań właściwych dla jednostki organizacyjnej PSP;
   b) rodzaj danych przetwarzanych w systemach informatycznych i ich przynależność do poszczególnych kategorii danych określonych w § 13;
   c) potrzebę utrzymania ryzyka związanego z funkcjonowaniem systemów informatycznych na akceptowalnym poziomie w oparciu o wyniki analiz ryzyka przeprowadzonych dla poszczególnych kategorii danych;
   d) konieczność zapewnienia zgodności z obowiązującym stanem prawnym oraz regulacjami wewnętrznymi PSP;
   e) zasadę racjonalnego gospodarowania środkami finansowymi.

Rozdział 2

ZASADY UŻYTKOWANIA SYSTEMÓW INFORMATYCZNYCH

§ 3.

Zasady korzystania ze sprzętu informatycznego i zasobów informatycznych

1. Każdy Pracownik zobowiązany jest użytkować powierzony mu sprzęt informatyczny zgodnie z przeznaczeniem oraz w miarę posiadanych możliwości chronić przed zagrożeniami ze strony otoczenia (kurz, ogień, wyciek wody itp.). W szczególności należy unikać działań mogących być przyczyną uszkodzenia lub zniszczenia tego sprzętu.
2. Przydział komputerów służbowych Pracownikom realizowany jest w oparciu o potrzeby zgłaszane do Działu IT przez KJO, przy uwzględnieniu zasady „jeden komputer na jednego użytkownika”. W uzasadnionych przypadkach, związanych z charakterem wykonywanych przez Pracownika obowiązków, na wniosek KJO Dział IT przydziela dodatkowy sprzęt informatyczny.
3. Użytkownicy mogą korzystać wyłącznie z tych systemów informatycznych, tj. programów i zasobów informatycznych, do korzystania z których zostały nadane im uprawnienia.
4. Zakazane są próby uzyskania dostępu do zasobów, do których użytkownikowi nie nadano uprawnień, a także samodzielne próby potwierdzania lub wykorzystywania podatności systemów informatycznych. Wykrycie takich prób będzie traktowane jako naruszenie zasad bezpieczeństwa systemów informatycznych.
5. Zabrania się Pracownikom wykorzystywania do celów służbowych, prywatnych urządzeń informatycznych, w szczególności ich podłączania do sieci informatycznej SGSP, jeżeli nie zostały one skonfigurowane i zabezpieczone przez ASI.

6. Zabrania się Pracownikom instalowania oraz zmiany konfiguracji jakiegokolwiek oprogramowania, urządzenia i służbowego sprzętu informatycznego bez uzyskania zgody ASI lub AD, zgodnie z nadanymi uprawnieniami.
7. Potrzebę instalacji dodatkowego oprogramowania lub sprzętu informatycznego Pracownik powinien zgłaszać do ASI za pośrednictwem systemu Help-Desk.
8. Za umożliwienie wykorzystania powierzonego sprzętu informatycznego przez inną osobę, w szczególności uzyskanie przez nią nieautoryzowanego dostępu do plików zapisanych lokalnie na urządzeniu oraz w zasobach sieciowych odpowiada Pracownik, któremu sprzęt przydzielono.
9. Wszystkie pochodzące z zewnątrz nośniki lub inne media z danymi muszą być sprawdzane przy pomocy aktualnego oprogramowania antywirusowego wskazanego przez ABS.
10. Każdy Pracownik jest odpowiedzialny za właściwe zabezpieczenie przed utratą tworzonych przez siebie dokumentów. Tworzone przez Pracowników dokumenty muszą być zapisywane w przeznaczonych do tego celu katalogach i serwerach plików.
11. Zabrania się przekazywania informacji o wykorzystywanym w SGSP sprzęcie komputerowym, oprogramowaniu, sieci, kartach dostępowych, procedurach oraz o wszelkich stosowanych środkach bezpieczeństwa. Informacji tych mogą udzielać jedynie pracownicy Działu IT.
12. Utrata lub kradzież sprzętu muszą być niezwłocznie zgłaszane do Działu IT.
13. Kontakt z serwisami zewnętrznymi, dotyczący powierzonego sprzętu, możliwy jest za pośrednictwem lub zgodą ASI lub ABS.
14. W przypadku zdalnego dostępu do komputera, w szczególności w celu wykonywania czynności serwisowych na komputerze, użytkownik komputera powinien potwierdzić przejęcie pulpitu komputera oraz nadzorować wszelkie czynności wykonywane przez ASI lub osobę przejmującą pulpit komputera, której zostały zlecone stosowne działania na podstawie zawartej umowy.
15. Na potrzeby awaryjnego dostępu do sprzętu informatycznego tworzone jest konto z uprawnieniami użytkownika uprzywilejowanego (administratora), do którego hasło przechowywane jest przez ASI. Z konta tego mogą korzystać jedynie w wyjątkowych sytuacjach ASI za zgodą ABS.

§ 4.
Zasady korzystania z haseł

1. Otrzymane przez użytkowników identyfikatory i hasła dostępowe do systemu informatycznego są poufne oraz zostały przekazane wyłącznie na jego użytek. Nie wolno ich użyczać lub przekazywać innym osobom, zapisywać lub pozostawiać w miejscu, w którym mogłyby być odkryte przez osobę nieupoważnioną (krawędź biurka, spód klawiatury itp.).
2. Użytkownicy muszą stosować hasła zgodne z polityką tworzenia haseł przyjętą w SGSP.
3. Jeżeli system informatyczny z powodów technologicznych nie ma możliwości wymuszenia odpowiednio silnego hasła lub wymuszenia jego zmiany co 30 dni - użytkownicy zobowiązani są do:
   1) ustanowienia indywidualnego hasła dostępu składającego się z minimum 8 znaków, zawierającego co najmniej jedną wielka i jedną małą literę oraz cyfrę lub znak specjalny;
   2) niezwłocznej zmiany hasła, gdy istnieje uzasadnione podejrzenie naruszenia bezpieczeństwa systemu lub ujawnienia hasła;
   3) zmiany hasła tymczasowego na indywidualne przy pierwszym logowaniu.

4. Zabrania się wprowadzania haseł na stałe do systemów informatycznych oferujących możliwość ich zapamiętania i ponownego logowania bez potrzeby podawania hasła.

§ 5.

Zasady korzystania z zewnętrznych usług sieciowych i poczty elektronicznej

1. Pracownicy mogą przeglądać zasoby sieci Internet wyłącznie w celach związanych z wykonywaną pracą. Zabrania się w szczególności przeglądania i rozpowszechniania treści i obrazów godzących w dobre imię SGSP lub sprzecznych z prawem oraz uczestniczenia w portalach społecznościowych, jeżeli nie jest to związane z wykonywaniem zadań służbowych.
2. Pracownikom nie wolno pobierać z sieci Internet plików, a tym bardziej instalować oprogramowania niezwiązanego z wykonywaniem zadań służbowych.
3. Zabrania się udostępnienia w sieci Internet własnych stacji roboczych.
4. Zabrania się wykorzystywania prywatnych skrzynek pocztowych do celów służbowych. Do celów służbowych Pracownikowi przydzielana jest uczelniana skrzynka pocztowa. Wszelka korespondencja służbowa musi odbywać się za pośrednictwem uczelnianych skrzynek pocztowych.
5. Korzystanie z uczelnianej skrzynki poczty elektronicznej, o której mowa w ust. 4, w celach prywatnych jest dopuszczalne w sytuacjach uzasadnionych okolicznościami, z zastrzeżeniem podania w tytule korespondencji wyrazu "osobiste", "prywatne", "poufne", "personal", "private", "confidential" lub równoznacznego.
6. Zabrania się uczestniczenia w listach dyskusyjnych, portalach społecznościowych itp. z wykorzystaniem firmowego adresu e-mail, o ile nie wiąże się to z wykonywaniem obowiązków służbowych.
7. Zabrania się otwierania załączników do poczty elektronicznej, jeżeli pochodzi ona z niewiadomego źródła (np. od nieznanych osób, zwłaszcza spoza SGSP).
8. Zabrania się rozsyłania zbiorowej korespondencji o tematyce pozazawodowej (Spamu) z wykorzystaniem służbowego sprzętu komputerowego oraz adresu e-mail.
9. Pliki zawierające zestawy danych osobowych przesyłane pocztą elektroniczną muszą być zabezpieczane kryptograficznie (np. hasło do pliku lub inna forma szyfrowania wskazana przez ASI).
10. W przypadku, gdy jest to niezbędne do zapewnienia organizacji pracy umożliwiającej pełne wykorzystanie czasu pracy oraz właściwego użytkowania udostępnionych Pracownikowi narzędzi pracy, Rektor-Komendant SGSP może wprowadzić kontrolę służbowej poczty elektronicznej pracownika, monitoring aktywności sieciowej, w tym działania w sieci Internet wykonywanych z sieci wewnętrznej SGSP, na zasadach określonych w art. 22^3 §1 KP. Dostęp do zgromadzonych danych związanych z aktywnością Pracownika może mieć wyłącznie osoba upoważniona przez Rektora-Komendanta.
11. Postanowień ust. 10 nie stosuje się do korespondencji Pracownika oznaczonej w tytule wyrazem "osobiste", "prywatne", "poufne", "personal", "private", "confidential" lub równoznacznym oraz do korespondencji adresowanej do Pracownika, której oznaczenie w tytule uprawdopodabnia, że ma ona charakter prywatny, jeżeli pracodawca wszedł w posiadanie treści korespondencji, o charakterze prywatnym, w wyniku przekonania, że ma do czynienia z korespondencją prowadzoną w celach służbowych, podejmuje dostępne mu środki mające na celu zachowanie tajemnicy tej korespondencji.

12. Dział IT, we współpracy z Polską Federacją Zarządzania Tożsamością PIONIER.Id zwanej dalej "Federacją PIONIER.Id", umożliwia użytkownikom dostęp do zewnętrznych usług sieciowych udostępnianych za przez Federację PIONIER.Id.
13. W trakcie logowania do usług zewnętrznych, o których mowa w ust. 12, konieczne jest przekazanie wybranych danych dotyczących konta użytkownika, takich jak adres mailowy, status użytkownika (pracownik lub student), nazwisko, imię.
14. Dane osobowe użytkownika w związku z logowaniem do usługi zewnętrznej, o której mowa w ust. 12, będą przekazywane usługodawcy przez cały okres członkostwa SGSP w Polskiej Federacji Zarządzania Tożsamością PIONIER.Id, jednak nie dłużej niż do chwili utraty przez użytkownika statusu wskazanego w ust. 13.

§ 6.

Rozpoczęcie, zakończenie, zawieszenie pracy w systemach informatycznych

1. Przed przystąpieniem do pracy z systemem informatycznym, Pracownik obowiązany jest dokonać sprawdzenia stanu urządzeń komputerowych oraz oględzin swojego stanowiska pracy, ze zwróceniem szczególnej uwagi, czy nie zaszły okoliczności wskazujące na naruszenie bezpieczeństwa i uzyskanie nieautoryzowanego dostępu do danych.
2. Rozpoczynając pracę na komputerze, Pracownik musi podać wszystkie wymagane, własne identyfikatory i hasła, w sposób uniemożliwiający ich ujawnienie innym osobom.
3. Pracownik zobowiązany jest uwierzytelniać się w systemie informatycznym, wyłącznie na podstawie własnego identyfikatora i hasła. Uwierzytelnienie lub próby uwierzytelniania przy pomocy identyfikatorów i haseł innych Pracowników będą traktowane jako świadome naruszenie zasad bezpieczeństwa systemów informatycznych.
4. Każdy Pracownik posiada dostęp tylko do tych funkcji aplikacji, które są mu niezbędne w codziennej pracy. Próby nieautoryzowanego dostępu do innych funkcji aplikacji lub jakichkolwiek zasobów informatycznych będą traktowane jako świadome naruszenie zasad bezpieczeństwa systemów informatycznych.
5. W przypadku braku możliwości zalogowania się Pracownika do działającego systemu informatycznego lub dostępu do funkcjonalności systemu, niezbędnych do realizacji zadań służbowych, należy o tym poinformować ASI za pomocą systemu Help-Desk lub telefonicznie.
6. Opuszczając stanowisko pracy należy wylogować się z systemu.
7. Przy krótkotrwałych przerwach w pracy należy zablokować stację roboczą (przyciski Ctr+Alt+Del „Zablokuj ten komputer” lub kombinacja klawiszy + L).
8. Kończąc pracę, Pracownik obowiązany jest do:
   1) wylogowania się z systemu, a następnie wyłączenia sprzętu komputerowego;
   2) zabezpieczenia stanowiska pracy, w szczególności schowania do zamykanych szaf, szuflad itp. wszelkiej dokumentacji oraz nośników magnetycznych, optycznych i papierowych (zasada "czystego biurka").

§ 7.

Zasady użytkowania służbowych komputerów przenośnych

1. Pliki tworzone i zapisywane na dyskach komputerów przenośnych należy przy pierwszej nadarzającej się okazji kopiować na dedykowany serwer plików SGSP lub sprawdzić, czy pliki te nie zostały automatycznie skopiowane (synchronizacja).

2. Zabrania się dokonywania innych zmian w konfiguracji, a w szczególności zmian konfiguracji systemów firewall, oprogramowania antywirusowego, ochrony kryptograficznej danych zapisywanych na dysku komputera przenośnego oraz instalacji/deinstalacji, aktywacji/deaktywacji jakiegokolwiek oprogramowania bez uzyskania zgody ASI.
3. Komputer przenośny nie może być pozostawiony bez opieki osoby, której został powierzony.
4. Komputer przenośny użytkowany poza siedzibą SGSP musi być przechowywany w miejscach minimalizujących ryzyko przypadkowego uszkodzenia oraz kradzieży.
5. Komputery przenośne, które są użytkowane poza siedzibą SGSP powinny być transportowane w specjalnie do tego celu przeznaczonych torbach, chroniących je przed uszkodzeniami mechanicznymi. Komputer przenośny powinien być całkowicie wyłączony, nie zaleca się transportowania w trybie hibernacji lub uśpienia.
6. Podczas transportu komunikacją publiczną zaleca się unikać umieszczania komputera przenośnego w ogólnodostępnych bagażnikach, do których dostęp mają inni pasażerowie, jak również pozostawiania urządzenia bez opieki.

§ 8.

Zasady pracy zdalnej

1. Przetwarzanie przez Pracowników danych osobowych w związku z wykonywaniem przez nich obowiązków służbowych następuje wyłącznie w siedzibie SGSP.
2. Poza siedzibą SGSP lub w czasie wykonywania pracy w formie zdalnej Pracownicy mogą przetwarzać:
   1) informacje zawierające dane osobowe, zgodnie z obowiązującymi w SGSP zasadami przetwarzania danych osobowych;
   2) informacje będące tajemnicą pracodawcy za uprzednią zgodą KJO wyłącznie z wykorzystaniem połączeń VPN/IPSec, na służbowych komputerach przenośnych.
3. Niedozwolone jest samodzielne dokonywanie jakichkolwiek ingerencji w strukturę oraz konfigurację oprogramowania klienta VPN.
4. Wszelkie prace prowadzone za pomocą zdalnego dostępu do sieci muszą przebiegać w taki sposób, aby w ich wyniku nie doszło do uszkodzeń bądź nieplanowanych przerw w działaniu infrastruktury informatycznej SGSP.
5. Obowiązkiem użytkownika jest zapewnienie, by w wyniku jego działań nie doszło do nieuprawnionych modyfikacji danych znajdujących się w systemach teleinformatycznych SGSP.
6. Pracownikom nie wolno wykorzystywać uzyskanych praw dostępu do innych celów, niż określone we wniosku o nadanie uprawnień.
7. Pracownika obowiązuje zakaz udostępniania utworzonego zdalnego połączenia innym osobom.
8. Zabrania się samodzielnego testowania zabezpieczeń sieci wewnętrznej SGSP. Wszelkie działania w tym zakresie wymagają wcześniejszej zgody ABS oraz muszą obywać się pod kontrolą wyznaczonego ASI.
9. Pracownicy ponoszą pełną odpowiedzialność za wszelkie czynności wykonane podczas zdalnej pracy w sieci wewnętrznej SGSP z użyciem ich danych uwierzytelniających.
10. Pracownik, któremu przyznano zdalny dostęp do wewnętrznej sieci informatycznej odpowiada za ujawnianie informacji i danych uzyskanych przez niego w związku z korzystaniem ze zdalnego dostępu do sieci, a także za szkody wywołane w związku z jego działaniem - również po ustaniu stosunku pracy lub okresu obowiązywania umowy będącej podstawą przyznania uprawnień zdalnego dostępu.

11. W trakcie pracy Pracownicy zobowiązani są do posługiwania się licencjonowanym oprogramowaniem z zainstalowanymi aktualnymi, krytycznymi aktualizacjami.
12. Pracownicy uzyskujący uprawnienia zdalnego dostępu mają obowiązek dołożenia starań w zakresie zagwarantowania bezpieczeństwa połączenia. Podstawowym wymogiem jest stosowanie właściwie skonfigurowanego systemu zabezpieczającego typu "firewall".
13. Przed przystąpieniem do wykonywania pracy w formie zdalnej, Pracownik jest zobowiązany do sprawdzenia systemu informatycznego programem antywirusowym z zainstalowanymi aktualnymi definicjami wirusów oraz do sprawdzenia systemu pod kątem obecności oprogramowania szpiegującego.
14. Pracownicy zobligowani są do niezwłocznego telefonicznego lub elektronicznego zgłaszania ASI wszelkich zaobserwowanych nieprawidłowości w funkcjonowaniu oprogramowania VPN oraz podejrzeń przejęcia hasła dostępu do konta służbowego.
15. Wszystkie zdalne połączenia do sieci wewnętrznej SGSP są rejestrowane.
16. Dział IT jest uprawniony do monitorowania prac wykonywanych w sieci informatycznej, jak również do zrywania połączenia bez wcześniejszego uprzedzenia, w przypadku wykrycia łamania lub też podejrzenia łamania zasad zdalnego dostępu.
17. W przypadku ujawnienia przez Dział IT przypadków korzystania z uprawnień zdalnego dostępu w sposób niezgodny z zasadami lub przyznanym zakresem uprawnień Dział IT może:
    1) cofnąć przyznane uprawnienia do korzystania z sieci;
    2) wnioskować do właściwego KJO o:
        a) zastosowanie wobec Pracownika kary porządkowej przewidzianej w regulaminie pracy SGSP;
        b) obciążenie karami wynikającymi z umowy, w przypadku gdy użytkownikiem był podmiot zewnętrzny.

§ 9.

Zgłaszanie incydentów i podatności

1. Każdy użytkownik ma obowiązek zgłaszać do ASI wszelkiego rodzaju zdarzenia, które w jego ocenie mają lub mogą mieć negatywny wpływ na bezpieczeństwo informacji przetwarzanych w systemach informatycznych.
2. Każdy użytkownik, a w szczególności ASI, powinien zwracać uwagę na występowanie zdarzeń związanych z:
    1) brakiem lub niedostępnością spodziewanych danych;
    2) niezgodnością danych w systemie informatycznym z danymi w postaci papierowej lub innymi kopiami elektronicznymi;
    3) pozostawionymi śladami włamania komputerowego, np. zmianami konfiguracji,
    4) nieplanowanymi zmianami sum kontrolnych plików;
    5) wszelkimi zapisami w logach systemów informatycznych świadczącymi o naruszeniu bezpieczeństwa, wykonywaniu niedozwolonych operacji itp.;
    6) samodzielnymi akcjami podejmowanymi przez system informatyczny (np. nawiązywanie połączeń, wysyłanie maili, itp.);
    7) intensywną pracą dysku w czasie, gdy z komputera nikt nie korzysta;
    8) powtarzającymi się "zawieszeniami" na ogół stabilnego systemu informatycznego;
    9) odczuwalnym spowolnieniem pracy systemu informatycznego lub sieci;
    10) innymi niż zwykle lub dodatkowymi oknami powitalnymi zachęcającymi do podania hasła;

11) odmową przyjęcia prawidłowego hasła użytkownika;
12) pojawianiem się niestandardowych okien, napisów i innych elementów ekranu;
13) znaczącymi zmianami w zajętości dysku;
14) nienaturalnymi rozmiarami zapisywanych na dysku plików;
15) pojawiającymi się budzącymi podejrzenie nazwami plików lub katalogów;
16) powtarzającym się zrywaniem połączeń sieciowych;
17) ujawnieniem indywidualnych haseł dostępowych;
18) otrzymywaniem spamu najczęściej z załącznikami typu, .doc, .exe, .com;
19) zgubieniem nośnika zawierającego informacje;
20) wykryciem braku nośnika informacji w jego miejscu przechowywania;
21) przekazaniem nośnika osobie nieuprawnionej do ich otrzymania;
22) znalezieniem nośnika z informacjami należącymi do SGSP poza siedzibą SGSP.

3. Zgłoszeń należy dokonywać w pierwszej kolejności w systemie Help-Desk, a gdy nie jest to możliwe telefonicznie na numer 22 561 77 76 lub za pośrednictwem poczty elektronicznej na adres pomoc@sgsp.edu.pl
4. W przypadku zdarzeń związanych z systemami informatycznymi zabrania się użytkownikom podejmowania jakichkolwiek działań w systemie informatycznym bez wcześniejszej konsultacji z ASI.
5. Niezgłoszenie przez użytkownika zaistniałego zdarzenia, odmowa udzielenia wyjaśnień dotyczących zaistniałych incydentów lub próba samodzielnego potwierdzenia występowania podatności systemu informatycznego może być podstawą do wyciągnięcia wobec użytkownika sankcji porządkowych, dyscyplinarnych lub karnych.

Rozdział 3

ZAKRESY ODPOWIEDZIALNOŚCI

§ 10.

1. Za bezpieczeństwo systemów informatycznych odpowiada ABS, do którego obowiązków należy w szczególności:
   1) nadzór nad właściwym funkcjonowaniem systemów informatycznych, ze szczególnym uwzględnieniem bezpieczeństwa danych, o których mowa w §13 ust.1;
   2) nadzór nad realizacją postanowień PBSI;
   3) wyznaczenie ASI pośród pracowników Działu IT;
   4) w uzgodnieniu z KJO nadawanie uprawnień oraz współpraca z AD;
   5) nadzór nad działaniami podejmowanymi przez ASI;
   6) przedkładanie do Rektora-Komendanta SGSP wniosków dotyczących bezpieczeństwa systemów informatycznych oraz niezbędnych do aktualizacji PBSI;
   7) udział w czynnościach związanych z monitorowaniem przestrzegania RODO, innych właściwych przepisów o ochronie danych osobowych oraz Polityce Ochrony Danych Osobowych (PODO), prowadzonych na zasadach określonych w PODO;
   8) podjęcie niezbędnych i odpowiednich do zagrożeń działań w zakresie zabezpieczenia systemów informatycznych w sytuacji naruszenia ochrony danych;
   9) wykonywanie innych zadań zgodnie z zapisami PODO.

2. ASI jest odpowiedzialny za zapewnienie ciągłości działania oprogramowania i sieciowej infrastruktury informatycznej, ze szczególnym uwzględnieniem bezpieczeństwa przetwarzanych danych. Do obowiązków ASI należy w szczególności:
   1) w zakresie bezpieczeństwa oprogramowania:
      a) nadawanie, modyfikacja i usuwanie uprawnień do Standardowego oprogramowania systemowego;
      b) nadzór nad funkcjonowaniem mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do danych przetwarzanych w systemach informatycznych;
      c) przeciwdziałanie dostępowi osób nieupoważnionych do systemów informatycznych;
      d) administrowanie serwerami, usługami sieciowymi i serwerowymi, przeciwdziałanie awariom i usuwanie awarii systemów serwerowych;
      e) analiza i dokumentowanie wszelkich zdarzeń związanych z naruszeniem bezpieczeństwa danych przetwarzanych w systemach informatycznych;
      f) wykonywanie kopii zapasowych oprogramowania i danych przetwarzanych w systemach informatycznych, ich zabezpieczanie i przechowywanie oraz okresowe sprawdzanie pod kątem dalszej przydatności do odtwarzania danych w sytuacji wystąpienia awarii;
      g) prowadzenie systematycznej ewidencji i przeglądu oprogramowania oraz systematyczne, automatyczne lub zgodne z bezpieczeństwem jego aktualizowanie;
      h) nadzór nad działaniami podejmowanymi przez Administratorów Dziedzinowych (AD), a w przypadku ich niepowołania realizacja obowiązków AD.
   2) w zakresie bezpieczeństwa sieciowej infrastruktury informatycznej:
      a) zapewnienie bezpieczniej wymiany danych w sieci wewnętrznej SGSP i ochrona przed zagrożeniami pochodzącymi z sieci publicznej;
      b) przeciwdziałanie dostępowi osób nieupoważnionych do systemów informatycznych,
      c) analiza i dokumentowanie wszelkich zdarzeń związanych z naruszeniem bezpieczeństwa systemów informatycznych;
      d) nadzór nad funkcjonowaniem awaryjnych źródeł zasilania systemów informatycznych;
      e) nadzór nad funkcjonowaniem mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do systemów informatycznych;
      f) prowadzenie systematycznej kontroli, przeglądu i konserwacji aktywnych urządzeń sieciowych (m.in.: routery, zapory sieciowe, przełączniki sieciowe, kontrolery WiFi);
      g) przeciwdziałanie awariom sieci LAN, awariom wydzielonych podsieci lokalnych i usuwanie zaistniałych awarii.
3. W odniesieniu do Oprogramowania dziedzinowego ABS w uzgodnieniu z właściwym KJO może nadawać Pracownikowi lub podmiotowi zewnętrznemu na podstawie zawartej umowy uprawnienia Administratora Dziedzinowego, który odpowiada za zapewnienie ciągłości działania określonego Oprogramowania dziedzinowego. Do obowiązków AD należy w szczególności:
   a) nadawanie, modyfikacja i usuwanie uprawnień do Oprogramowania dziedzinowego;
   b) świadczenie wsparcia w zakresie użytkowania Oprogramowania dziedzinowego;
   c) przeciwdziałanie dostępowi osób nieupoważnionych do danych przetwarzanych w Oprogramowaniu dziedzinowym;
   d) w uzgodnieniu z ASI prowadzenie rekonfiguracji i systematycznej aktualizacji Oprogramowania dziedzinowego;

e) przeciwdziałanie awariom Oprogramowania dziedzinowego i usuwanie błędów w przypadku ich wykrycia;
f) wykonywanie poleceń ABS dotyczących bezpieczeństwa Oprogramowania dziedzinowego, prowadzenia czynności monitorujących, raportujących i przetwarzania danych osobowych w systemach informatycznych.

Szczegółowy zakres uprawnień i obowiązków AD może ulec zmianie zależnie od specyfiki Oprogramowania dziedzinowego. W takiej sytuacji ABS uzgadnia zakres zmian z właściwym KJO.

4. Obowiązki pozostałych Pracowników, w tym KJO wynikają bezpośrednio z zapisów PBSI.
5. Umyślne lub nieumyślne naruszenie zawartych w niniejszym dokumencie zasad bezpieczeństwa systemów informatycznych lub niestosowanie się do poleceń służbowych w tym zakresie może być potraktowane jako naruszenie obowiązków pracowniczych.

Rozdział 4

ZARZĄDZANIE SPRZĘTEM I OPROGRAMOWANIEM

§ 11.

1. W SGSP sprzęt informatyczny oraz oprogramowanie mogą być wdrażane i użytkowane jedynie po uzyskaniu akceptacji ASI i zatwierdzeniu przez ABS.
2. Systemy informatyczne mogą być dopuszczone do produkcyjnego użytkowania po ich skonfigurowaniu przez ASI lub AD oraz wpisaniu do *Wykazu eksploatowanych systemów informatycznych*, prowadzonego przez ASI i zatwierdzonego przez ABS.
3. W przypadku wykrycia użytkowania przez użytkowników nieautoryzowanego sprzętu lub oprogramowania, ABS powinien poinformować o tym KJO wraz z wnioskiem o podjęcie odpowiednich działań porządkowych.

Rozdział 5

ZARZĄDZANIE DOKUMENTACJĄ SYSTEMÓW INFORMATYCZNYCH

§ 12.

1. Podstawowym dokumentem regulującym zasady zarządzania bezpieczeństwem systemów informatycznych jest PBSI. Za jej opracowanie i aktualizację odpowiada ABS.
2. ABS określa systemy informatyczne, dla których muszą zostać opracowane dodatkowe dokumenty: instrukcje użytkowania systemów (dla Pracowników) i *Instrukcja Zarządzania Systemami Informatycznymi* (załącznik nr 3, wyłącznie dla ASI i AD), *Regulamin Sieci Informatycznej* (załącznik nr 4, dla Gości).
3. Za opracowanie dokumentacji, o której mowa w ust. 2, odpowiadają ASI.
4. W instrukcjach uwzględniane są następujące zagadnienia:
   1) w instrukcjach użytkowania systemów informatycznych - procedury pracy dla użytkowników systemu;
   2) w *Instrukcji Zarządzania Systemem Informatycznym*:
      a) wytyczne do konfiguracji w zakresie pozwalającym na instalację i konfigurację systemu od podstaw (w tym elementy dokumentacji powykonawczej systemu);

b) procedury zarządzania uprawnieniami użytkowników, gdy ich zakres wykracza poza zapisy PBSI;
c) procedury tworzenia kopii zapasowych, gdy ich zakres wykracza poza zapisy PBSI;
d) procedury ponownego uruchomiania i odtwarzania systemu w przypadku awarii;
e) procedury zarządzania systemowymi dziennikami zdarzeń;
f) procedury obsługi błędów i awarii;
g) zasady testowania systemu po zmianach, w tym aktualizacjach oraz zabezpieczenia danych testowych;
h) kontakty umożliwiające uzyskanie wsparcia technicznego;

3) w *Regulaminie Sieci Informatycznej* - zasady korzystania z systemów informatycznych udostępnianych Gościom.

5. ASI uzupełnia *Wykaz eksploatowanych systemów informatycznych* oraz zamieszcza instrukcje użytkowania poszczególnych systemów w repozytorium systemu Help-Desk.
6. W przypadku pozostałych systemów informatycznych, przy administrowaniu nimi i ich użytkowaniu należy kierować się wytycznymi niniejszego dokumentu, zaleceniami producentów oprogramowania oraz dobrymi praktykami z obszaru IT.
7. Przynajmniej raz do roku ABS jest zobowiązany do przeglądu PBSI oraz pozostałej dokumentacji systemów informatycznych i potwierdzenia jej kompletności oraz aktualności przez złożenie podpisu w metrykach poszczególnych dokumentów.

Rozdział 6

KATEGORIE PRZETWARZANYCH DANYCH, ANALIZA RYZYKA I DOBÓR POZIOMÓW ZABEZPIECZEŃ

§ 13.

1. Określa się następujące kategorie danych przetwarzanych w systemach informatycznych SGSP:
   1) do kategorii I należą:
      a) dane osobowe, o których mowa w Polityce Ochrony Danych Osobowych SGSP;
      b) dane związane z działalnością naukowo-badawczą SGSP, chronione prawami autorskimi i prawami pokrewnymi;
      c) dane związane z realizacją przez SGSP prac zleconych;
      d) dane podlegające szczególnej ochronie, związane z wykonywaniem przez SGSP zadań jednostki organizacyjnej PSP;
   2) do kategorii II należą pozostałe dane przetwarzane w systemach informatycznych nie wymienione w pkt 1) powyżej.
2. Dla systemów informatycznych, w których przetwarzane są dane należące do kategorii I, o której mowa w ust.1 pkt 1) określa się **podstawowy poziom zabezpieczeń** systemów informatycznych obowiązujący w podsieciach przeznaczonych dla Pracowników, o którym mowa w rozdziale 6 PBSI. Jeśli w wyniku przeprowadzanej szczegółowej analizy ryzyka nie ustalono stosowania innych zabezpieczeń, należy stosować zabezpieczenia poziomu podstawowego. Za konfigurację zabezpieczeń odpowiadają ASI.
3. Dla systemów informatycznych, w których przetwarzane są dane należące do kategorii II, o której mowa w ust.1 pkt 2) określa się **minimalny poziom zabezpieczeń**, o którym mowa w rozdziale 7 PBSI.

4. W przypadku przetwarzania na danym systemie informatycznym danych przynależnych do obu kategorii wymienionych w ust. 1 zastosowanie mają wymagania jak dla podstawowego poziomu zabezpieczeń.
5. Analiza ryzyka dla bezpieczeństwa informacji jest prowadzona przez wszystkie jednostki organizacyjne SGSP, zgodnie z ustaloną w SGSP metodyką.
6. W procesie analizy ryzyka dla bezpieczeństwa informacji pracownicy Działu IT odpowiadają za:
   1) identyfikację potencjalnych zagrożeń i podatności dla systemów informatycznych;
   2) oszacowanie prawdopodobieństwa zmaterializowania się zagrożeń skutkujących utratą poufności, dostępności i integralności danych przetwarzanych w systemach informatycznych;
   3) przedstawienie propozycji zabezpieczeń systemów informatycznych w przypadku gdy ryzyko utraty poufności, dostępności lub integralności danych przetwarzanych w systemach informatycznych przekroczy akceptowalny poziom.
7. Za określenie skutków utraty poufności, dostępności i integralności danych przetwarzanych w systemach informatycznych oraz akceptowalnego poziomu ryzyka odpowiadają KJO.
8. Działania Działu IT w zakresie analizy ryzyka muszą być przeprowadzane dla wszystkich nowo powstających systemów informatycznych i aplikacji oraz okresowo (nie rzadziej niż raz na rok) dla już istniejących.
9. Analiza ryzyka dla nowych systemów informatycznych powinna stanowić element cyklu projektowego i prowadzić do określenia wymagań bezpieczeństwa dla nowego systemu oraz planowanych zabezpieczeń na poziomie technologicznym i organizacyjnym.
10. Analiza ryzyka dla istniejących systemów informatycznych powinna prowadzić do potwierdzenia lub zaprzeczenia skuteczności istniejących zabezpieczeń oraz ewentualnego przedstawienia rekomendacji dla podniesienia poziomu bezpieczeństwa.
11. Przeprowadzenie analizy ryzyka przez Dział IT jest dokumentowane w raportach z analizy ryzyka opracowywanych zgodnie z przyjętą przez ABS metodyką szacowania ryzyka.
12. Rektor-Komendant SGSP jest odpowiedzialny za zatwierdzenie proponowanych przez ABS zabezpieczeń poziomu podstawowego oraz zabezpieczeń i działań korygujących wynikających z przeprowadzonej analizy ryzyka.

Rozdział 7

PODSTAWOWY POZIOM ZABEZPIECZEŃ

§ 14.

Zabezpieczenia sieci informatycznej

1. Bezpieczeństwo okablowania:
   1) okablowanie sieci informatycznej powinno być prowadzone w listwach w sposób minimalizujący ryzyko uszkodzeń fizycznych oraz nieautoryzowanego dostępu do niego;
   2) tam, gdzie istnieje potrzeba prowadzenia okablowania przez obszary nie należące do SGSP zaleca się stosować kryptograficzne zabezpieczenia transmisji danych lub fizycznego zabezpieczenia trasy;
   3) szafy krosownicze powinny znajdować się w pomieszczeniach zapewniających kontrolę dostępu;
   4) gniazdka i kable powinny być oznaczone w sposób umożliwiający ich identyfikację.

2. Bezpieczeństwo sieci bezprzewodowej:
   1) konfiguracja urządzeń bezprzewodowych musi zapewniać uwierzytelnianie obu stron połączenia (możliwość identyfikacji także punktu dostępowego);
   2) stacje robocze użytkowników powinny mieć wyłączoną możliwość automatycznego nawiązywania połączeń bezprzewodowych z sieciami niezabezpieczonymi;
   3) jako obowiązkowe podstawowe zabezpieczenie kryptograficzne sieci bezprzewodowych należy przyjąć stosowanie protokołów nie słabszych niż WPA2 oraz AES256.
3. Kontrola ruchu sieciowego:
   1) wymagane jest stosowanie systemów firewall, filtrów treści, filtrów antyspamowych oraz systemów wykrywania naruszeń bezpieczeństwa (IDS) pomiędzy siecią wewnętrzną SGSP a sieciami publicznymi lub sieciami innych podmiotów;
   2) wymagane jest stosowanie podziału sieci wewnętrznej na podsieci i vlany zapewniające możliwość kontroli i filtrowania ruchu sieciowego w sieci wewnętrznej SGSP. W tym celu należy stosować segmentację sieci wewnętrznej, w wyniku której powinno wyodrębnić co najmniej:
      a) podsieć administracyjno-dydaktyczną (przeznaczona dla wszystkich Pracowników);
      b) podsieć laboratoryjna (w obrębie danej pracowni dydaktycznej);
      c) podsieć studencką (przeznaczona dla Gości).
   3) ruch sieciowy pomiędzy poszczególnymi podsieciami i vlanami sieci wewnętrznej SGSP powinien być filtrowany za pomocą list kontroli dostępu (ACL) konfigurowanych na przełącznikach sieciowych;
   4) systemy informatyczne SGSP udostępniane w sieciach publicznych muszą znajdować się w wydzielonych strefach DMZ chronionych za pomocą systemów firewall. Konfiguracja systemów firewall powinna uniemożliwiać nawiązywanie połączeń ze stref DMZ do innych stref i podsieci, w szczególności do sieci wewnętrznych;
   5) utworzenie połączeń sieci SGSP z siecią innego podmiotu lub siecią publiczną wymaga zgody ABS określającej wymagane zabezpieczenia, zakres i czas połączenia;
   6) konfiguracja urządzeń sieciowych musi zapewniać, że połączenia użytkowników z sieciami publicznymi lub sieciami innych podmiotów są kontrolowane i realizowane wyłącznie przez infrastrukturę zarządzaną przez Dział IT;
   7) ASI odpowiedzialni są za bieżące dokumentowanie topologii sieci, stosowanych w sieci zabezpieczeń oraz szczegółowych konfiguracji urządzeń sieciowych (w szczególności przełączników, routerów, systemów firewall i systemów IDS) w zakresie umożliwiającym odtworzenie funkcjonalności sieci SGSP;
   8) wszelkie poważne zmiany w topologii sieci, stosowanych zabezpieczeniach sieciowych (zaporach, systemach IDS, listach kontroli dostępu w routerach itp.) oraz ich konfiguracji muszą być odnotowywane przez ASI oraz akceptowane przez ABS.
4. Dostęp do zasobów sieci wewnętrznej SGSP:
   1) zdalny dostęp do zasobów sieci wewnętrznej jest możliwy jedynie z wykorzystaniem protokołów zapewniających poufność przesyłanych danych (ochrona kryptograficzna) oraz uwierzytelnianie połączeń i użytkowników;
   2) wszędzie gdzie to możliwe należy stosować kanały VPN/IPSec;
   3) w pozostałych przypadkach dopuszcza się stosowanie protokołów SSH oraz SSL przy założeniu, że ich konfiguracja zapewnia uwierzytelnienie obydwu końców połączenia oraz uwierzytelnienie użytkownika;

4) wymagane jest stosowanie mechanizmów filtrowania ruchu sieciowego pozwalającego na skuteczne ograniczenie dostępu jedynie do zdefiniowanych zasobów sieciowych niezbędnych do realizacji zadań wykonywanych w sposób zdalny.

5. Dostęp do zasobów sieci publicznych:
   1) konfiguracja urządzeń sieciowych musi ograniczać dostęp wszystkich Pracowników SGSP do zasobów sieci publicznych wyłącznie do usług i protokołów, które są im niezbędne do wykonywania pracy;
   2) użytkownicy sieci wewnętrznej, chcący uzyskać dostęp do usług i zasobów sieci publicznych muszą poprawnie przejść proces uwierzytelnienia wymuszany przez elementy infrastruktury informatycznej SGSP;
   3) wszystkie pliki i informacje pobierane z sieci publicznych powinny być poddawane kontroli antywirusowej.

§ 15.

Zabezpieczenia serwerów

1. Kontrola dostępu:
   1) dostęp fizyczny do pomieszczeń gdzie znajdują się serwery musi być chroniony i powinien być ograniczony wyłącznie do uprawnionych osób;
   2) dostęp do usług i zasobów serwerów musi być ograniczany poprzez umieszczanie ich w podsieciach lub vlanach chronionych przez urządzenia sieciowe przy pomocy list ACL;
   3) dostęp administracyjny do serwerów może odbywać się jedynie z określonych hostów w sieci;
   4) podstawowym mechanizmem uwierzytelniania użytkowników są indywidualne identyfikatory i hasła. Wymagana jest konfiguracja wymuszająca:
      a) stosowanie haseł o długości minimum 8 znaków, zawierających małe i wielkie litery oraz cyfry lub znaki specjalne,
      b) tworzenie hasła różnego od co najmniej 5 poprzednich,
      c) blokowanie dostępu na minimum 30 minut po 5 nieudanych próbach logowania. Dodatkowo zaleca się zmianę haseł co 30 dni;
   5) stosowanie innych mechanizmów uwierzytelniających takich jak certyfikaty, tokeny itp. jest zalecane podczas zdalnego dostępu;
   6) należy stosować restrykcyjne prawa dostępu do poszczególnych plików i katalogów przyznając użytkownikom minimalne uprawnienia niezbędne do realizacji zadań służbowych.
2. Poufność:
   1) wszystkie czynniki uwierzytelniające muszą być przesyłane do serwera w sposób zapewniający ich poufność;
   2) żaden czynnik uwierzytelniający nie może być zapisywany w postaci jawnej w plikach konfiguracyjnych serwera lub oprogramowaniu działającym na serwerze;
   3) dostęp do serwerów spoza sieci wewnętrznej SGSP może odbywać się wyłącznie z wykorzystaniem bezpiecznych protokołów, uniemożliwiających podsłuch i przechwytywanie informacji (protokoły VPN/IPSec, SSH, SSL).

3. Integralność:
    1) konfiguracje wszystkich serwerów powinny przejść proces utwardzania (hardeningu) na podstawie zaleceń producentów wykorzystywanego oprogramowania oraz ogólnie uznanych za poprawne zasad i standardów bezpieczeństwa. W szczególności hardening powinien obejmować:
        a) instalację wyłącznie niezbędnych pakietów oprogramowania (lub usunięcie zbędnych),
        b) instalację i uruchamianie wyłącznie niezbędnych usług sieciowych (lub wyłączenie zbędnych),
        c) instalację aktualizacji oprogramowania, a w szczególności poprawek bezpieczeństwa,
        d) określenie polityki haseł i polityki blokowania kont użytkowników,
        e) ustalenie restrykcyjnych praw dostępu do wszystkich krytycznych obiektów w systemie informatycznym;
    2) wszystkie serwery, powinny posiadać zaimplementowane narzędzia sprawdzające integralność systemu plików, pozwalające wykryć próby nieautoryzowanych zmian (w plikach konfiguracyjnych systemu operacyjnego, aplikacjach i danych);
    3) każdy serwer powinien mieć zainstalowane i skonfigurowane oprogramowanie antywirusowe. Aktualizacja oprogramowania antywirusowego i skanowanie muszą następować przynajmniej raz dziennie w sposób automatyczny;
    4) zegary czasu systemowego wszystkich serwerów muszą być synchronizowane ze wzorcem czasu.
4. Rozliczalność:
    1) systemy operacyjne serwerów powinny posiadać włączone mechanizmy śledzenia zdarzeń (audyt i accounting) pozwalające jednoznacznie zidentyfikować użytkownika lub proces, który wykonał określone działania lub zmiany w systemie;
    2) szczegółowy zakres logowania zdarzeń oraz czas przechowywania logów jest ustalany indywidualnie dla każdego systemu informatycznego przez ASI i zatwierdzany przez ABS.
5. Dostępność i niezawodność:
    1) wszędzie gdzie to możliwe i uzasadnione należy stosować generatory prądotwórcze lub inne zapasowe źródła zasilania zapewniające pracę serwerów w przypadku awarii podstawowych linii zasilających;
    2) wszystkie serwery muszą być wyposażone w urządzenia UPS podtrzymujące zasilanie przez co najmniej 30 minut i umożliwiające prawidłowe zamknięcie systemu;
    3) na serwerach sieciowych muszą być wydzielane dedykowane zasoby na których użytkownicy będą mogli przechowywać swoje pliki;
    4) dla wszystkich serwerów produkcyjnych muszą być wykonywane kopie bezpieczeństwa;
    5) ABS na podstawie analizy ryzyka określa serwery, dla których wymagane jest stosowanie dodatkowych rozwiązań redundantnych (serwerów zapasowych, rozwiązań klastrowych itp.).
6. Zarzadzanie bezpieczeństwem:
    1) systemy operacyjne serwerów muszą posiadać włączone mechanizmy logowania zdarzeń związanych z bezpieczeństwem (logi systemowe, logi aplikacji rejestrujące co najmniej identyfikator użytkownika oraz udane i nieudane próby logowania, zmiany hasła, próby dostępu do rejestru lub plików konfiguracyjnych serwera);

2) każdy serwer musi mieć instalowane poprawki bezpieczeństwa. Instalacja poprawek musi być poprzedzona testami potwierdzającymi brak negatywnego wpływu instalacji poprawki na funkcjonowanie serwera.

§ 16.
Zabezpieczenia stacji roboczych

1. Stacje robocze muszą być podłączone do domeny Active Directory SGSP i konfigurowane z poziomu serwera domeny poprzez mechanizm Group Policy.
2. Uwierzytelnianie użytkowników musi następować na podstawie indywidualnych identyfikatorów domenowych i haseł. Wymagana jest konfiguracja wymuszająca:
   1) stosowanie haseł o długości minimum 8 znaków, zawierających małe i wielkie litery oraz cyfry lub znaki specjalne;
   2) tworzenie hasła różnego od co najmniej 5 poprzednich;
   3) blokowanie dostępu na minimum 30 minut po 5 nieudanych próbach logowania.

   Dodatkowo zaleca się zmianę haseł co 30 dni;
3. Pracownicy nie mogą posiadać na stacjach roboczych lokalnych kont z uprawnieniami administracyjnymi. Za zgodą ABS uprawnienia administracyjne dla danej stacji roboczej mogą być nadane AD w celu realizacji jego zadań.
4. Stacje robocze muszą mieć skonfigurowane wygaszacze ekranu zabezpieczone hasłem. Po 5 minutach nieaktywności użytkownika wygaszacz musi się aktywować.
5. Stacje robocze muszą mieć zainstalowane i skonfigurowane oprogramowanie antywirusowe wskazane przez ABS. Aktualizacja oprogramowania antywirusowego i skanowanie muszą następować przynajmniej raz dziennie w sposób automatyczny.
6. Stacje robocze muszą posiadać włączone mechanizmy monitorowania i logowania zdarzeń związanych z bezpieczeństwem.
7. Aktualizacja oprogramowania stacji roboczych o niezbędne poprawki, w szczególności poprawki bezpieczeństwa, może odbywać się w sposób automatyczny. Sprawdzanie dostępności poprawek powinno odbywać się codziennie.
8. Stacje robocze nie mogą udostępniać żadnych usług, serwisów ani innych zasobów, z wyłączeniem usług związanych z użytkowaniem drukujących urządzeń wielofunkcyjnych.
9. Wskazane jest aktywowanie wbudowanego systemu firewall.

§ 17.
Zabezpieczenia komputerów przenośnych

Obowiązują zabezpieczenia jak dla stacji roboczych. Dodatkowo wymagane jest:

1) aktywowanie hasła do BIOS;
2) aktywowanie indywidualnych systemów firewall;
3) stosowanie szyfrowanych dysków lub partycji;
4) instalacja oprogramowania umożliwiającego nawiązywanie połączeń VPN.

§ 18.

Zabezpieczenia elektronicznych nośników danych

1. Przenośne nośniki danych (pendrive) powinny mieć możliwość kryptograficznej ochrony danych zapisywanych na nich.
2. Elektroniczne nośniki danych (dyski twarde, taśmy, płyty DVD) muszą być przechowywane w zamykanych szafach lub sejfach w obszarach zapewniających kontrolę dostępu.
3. Wszelkie nośniki danych (dyski twarde, pamięci flash) przeznaczone do powtórnego wykorzystania przez nowego użytkownika muszą zostać pozbawione zapisu danych poprzez wielokrotne nadpisanie danych przy użyciu dedykowanego oprogramowania.
4. Sprzęt informatyczny przeznaczony do naprawy poza siedzibami SGSP należy przekazywać bez dysków twardych. W przypadku braku takich możliwości należy usuwać bezpowrotnie dane z dysków lub podpisywać umowy o zachowaniu poufności z podmiotem dokonującym naprawy.
5. Likwidacja uszkodzonych lub niepotrzebnych nośników danych odbywa się poprzez fizyczne zniszczenie nośnika (złamanie, pocięcie, przedziurawienie) lub przez przekazanie na podstawie umowy do specjalistycznej firmy dokonującej likwidacji nośników danych.

§ 19.

Systemy wspomagające

1. Przez systemy wspomagające, których użytkowanie w SGSP jest wymagane należy rozumieć:
   1) Systemy awaryjnego zasilania (generatory prądotwórcze lub alternatywne linie zasilające);
   2) Systemy podtrzymywania zasilania (UPS);
   3) Systemy klimatyzacji;
   4) Systemy kontroli dostępu;
   5) Systemy alarmowe,
   6) Systemy sygnalizacji pożarowej.
2. Wszystkie systemy wspomagające muszą przechodzić okresowe przeglądy i testy zgodnie z wytycznymi producentów. Jeśli producent nie określił częstotliwości przeglądów należy przyjąć, że powinno być to realizowane co 6 miesięcy. Za przeprowadzanie regularnych przeglądów systemów wspomagających odpowiada kierownik jednostki właściwej dla spraw przeglądów i konserwacji.
3. Protokoły z testów i przeglądów systemów wspomagających powinny być przekazywane do wiadomości ABS lub osoby przez niego wyznaczonej.

Rozdział 8

MINIMALNY POZIOM ZABEZPIECZEŃ

§ 20.

Zabezpieczenia sieci informatycznej

1. Bezpieczeństwo okablowania:
   1) okablowanie sieci informatycznej powinno być prowadzone w listwach w sposób minimalizujący ryzyko uszkodzeń fizycznych oraz nieautoryzowanego dostępu do niego;

2) tam, gdzie istnieje potrzeba prowadzenia okablowania przez obszary nie należące do SGSP zaleca się stosować kryptograficzne zabezpieczenia transmisji danych lub fizycznego zabezpieczenia trasy;
3) gniazdka i kable powinny być oznaczone w sposób umożliwiający ich identyfikację.

2. Bezpieczeństwo sieci bezprzewodowej:
   1) konfiguracja urządzeń bezprzewodowych musi zapewniać uwierzytelnianie obu stron połączenia (możliwość identyfikacji także punktu dostępowego);
   2) jako obowiązkowe podstawowe zabezpieczenie kryptograficzne sieci bezprzewodowych należy przyjąć stosowanie protokołów nie słabszych niż WPA2 oraz AES256.
3. Kontrola ruchu sieciowego w sieciach udostępnianych użytkownikom:
   1) wymagane jest stosowanie systemów firewall, filtrów treści, filtrów antyspamowych oraz systemów wykrywania naruszeń bezpieczeństwa (IDS) pomiędzy siecią wewnętrzną SGSP a sieciami publicznymi lub sieciami innych podmiotów;
   2) wymagane jest stosowanie podziału sieci wewnętrznej na podsieci i vlany zapewniające możliwość kontroli i filtrowania ruchu sieciowego w sieci wewnętrznej SGSP;
   3) nie dopuszcza się ruchu sieciowego pomiędzy urządzeniami w sieci udostępnionej Gościom, a pozostałymi podsieciami i vlanami sieci wewnętrznej SGSP;
   4) utworzenie połączeń sieci udostępnionej użytkownikom z siecią innego podmiotu lub siecią publiczną wymaga zgody ABS określającej wymagane zabezpieczenia, zakres i czas połączenia;
   5) konfiguracja urządzeń sieciowych musi zapewniać, że połączenia użytkowników z sieciami publicznymi lub sieciami innych podmiotów są kontrolowane i realizowane wyłącznie przez infrastrukturę zarządzaną przez Dział IT;
   6) ASI odpowiedzialni są za bieżące dokumentowanie topologii podsieci udostępnianych Gościom, stosowanych zabezpieczeń oraz szczegółowych konfiguracji urządzeń sieciowych (w szczególności przełączników, routerów, systemów firewall i systemów IDS) w zakresie umożliwiającym odtworzenie funkcjonalności sieci SGSP;
   7) wszelkie poważne zmiany w topologii sieci, stosowanych zabezpieczeniach sieciowych (zaporach, systemach IDS, listach kontroli dostępu w routerach itp.) oraz ich konfiguracji muszą być odnotowywane przez ASI oraz akceptowane przez ABS.
4. Dostęp do zasobów sieci publicznych:
   1) konfiguracja urządzeń sieciowych musi ograniczać dostęp użytkownikom do zasobów sieci publicznych wyłącznie do usług i protokołów, które są niezbędne;
   2) użytkownicy sieci wewnętrznej, chcący uzyskać dostęp do usług i zasobów sieci publicznych muszą poprawnie przejść proces uwierzytelnienia wymuszany przez elementy infrastruktury informatycznej SGSP;
   3) wszystkie pliki i informacje pobierane z sieci publicznych powinny być poddawane kontroli antywirusowej.

§ 21.
Zabezpieczenia urządzeń informatycznych

1. Uwierzytelnianie użytkowników sieci wewnętrznej dla nich udostępnionej musi następować na podstawie identyfikatorów sieci i haseł. Wymagana jest konfiguracja wymuszająca:

1) stosowanie haseł o długości minimum 8 znaków, zawierających małe i wielkie litery oraz cyfry lub znaki specjalne;
2) tworzenie hasła różnego od co najmniej 5 poprzednich;
3) blokowanie dostępu na 30 minut po 5 nieudanych próbach logowania.

Dodatkowo zaleca się zmianę haseł co 30 dni;

2. Od użytkowników wymaga się zainstalowania i prowadzenia aktualizacji oprogramowania antywirusowego na urządzeniach podłączonych do udostępnionej sieci.
3. Za aktualizację oprogramowania systemowego sprzętu informatycznego użytkowników o niezbędne poprawki, w szczególności poprawki bezpieczeństwa odpowiada użytkownik. Wskazane jest aktywowanie wbudowanego systemu firewall.
4. Urządzenia użytkowników podłączone do sieci im udostępnionej nie mogą udostępniać żadnych usług, serwisów ani innych zasobów.
5. Pozostałe kwestie dotyczące korzystania z udostępnianych zasobów zawarte są w *Regulaminie Sieci Informatycznej.*

Rozdział 9

ZARZĄDZANIE KOPIAMI BEZPIECZEŃSTWA

§ 22.

Wykonywanie i odtwarzanie kopii

1. ASI ustala w porozumieniu z właściwymi KJO sposób wykonywania kopii bezpieczeństwa poszczególnych systemów informatycznych z uwzględnieniem potrzeb oraz możliwości technicznych.
2. Dla każdego systemu informatycznego należy określić i udokumentować:
   1) zakres danych podlegających zabezpieczeniu;
   2) częstotliwość wykonywania kopii bezpieczeństwa;
   3) czas i miejsce przechowywania kopii bezpieczeństwa;
   4) nośnik wykorzystywany do przechowywania kopii.
3. Wymagane jest przechowywanie kopii bezpieczeństwa poza lokalizacją, w której znajduje się system informatyczny dla którego wykonuje się kopię bezpieczeństwa.
4. Zatwierdzone podpisem ABS zasady wykonywania kopii bezpieczeństwa dla systemu informatycznego są przechowywane przez Dział IT.
5. ASI przed dokonywaniem istotnych zmian konfiguracyjnych w systemie informatycznym, mogących skutkować niestabilnym działaniem systemu (np. wgranie nowej wersji oprogramowania kluczowych komponentów systemu), jest zobowiązany do wykonania dodatkowej kopii bezpieczeństwa niezależnie od przyjętego harmonogramu wykonywania kopii zapasowych.
6. Nie wykonuje się kopii bezpieczeństwa stacji roboczych. Dane ze stacji roboczych, które są istotne dla działalności SGSP, muszą być zapisywane przez użytkowników na dedykowanych zasobach sieciowych wskazanych przez ASI.
7. Odtwarzanie kopii bezpieczeństwa następuje w wyniku:
   1) działań realizowanych przez Dział IT związanych z obsługą awarii lub rekonfiguracją systemu informatycznego;
   2) okresowego sprawdzania możliwości odtworzenia kopii bezpieczeństwa przez ASI;

3) na wniosek KJO skierowany do ABS.

8. ASI prowadzi w formie elektronicznej rejestr, w którym odnotowywane są błędy wykonania kopii bezpieczeństwa oraz awaryjne i okresowe odtworzenia kopii bezpieczeństwa.

Rozdział 10

ZARZĄDZANIE UPRAWNIENIAMI UŻYTKOWNIKÓW

§ 23.

Nadawanie uprawnień

1. Uprawnienia do systemu informatycznego są nadawane, odbierane lub modyfikowane wyłącznie na podstawie wypełnionego przez właściwego KJO wniosku w postaci elektronicznej lub papierowej skierowanego do Działu IT i zaakceptowanego przez ABS. Wzór wniosku stanowi załącznik nr 5 do PODO.
2. KJO akceptujący wniosek, jest zobowiązany do jego weryfikacji pod kątem zgodności wnioskowanych uprawnień z zakresem obowiązków podległego Pracownika lub zakresu umowy w przypadku podmiotu zewnętrznego.
3. Wniosek, który wpłynął do Działu IT, jest akceptowany przez ABS i przekazywany do realizacji właściwym ASI.
4. ASI realizują wniosek oraz prowadzą rejestr identyfikatorów przyznanych użytkownikom w poszczególnych systemach informatycznych.
5. Wnioski o nadanie lub odebranie uprawnień do systemów informatycznych są archiwizowane przez Dział IT.
6. ASI przekazuje informacje o przyznanych identyfikatorach i hasłach bezpośrednio użytkownikowi w sposób poufny.
7. Identyfikatora użytkownika nie należy zmieniać bez wyraźnej przyczyny, a po wyrejestrowaniu użytkownika z systemu informatycznego nie powinien być on przydzielany innej osobie.
8. Hasło ustanowione przez ASI podczas przyznawania uprawnień użytkownik jest zobowiązany zmienić na indywidualne podczas pierwszego logowania się w systemie informatycznym.

§ 24.

Zmiana i odbieranie uprawnień

1. Zmiana i obieranie uprawnień do systemów informatycznych odbywa się na podstawie wypełnionego wniosku o nadanie lub odebranie uprawnień, zaakceptowanego przez właściwego KJO i skierowanego do Działu IT.
2. Konto użytkownika zostaje również zablokowane przez ASI na polecenie Rektora-Komendanta lub na polecenie ABS w przypadku wystąpienia incydentu bezpieczeństwa.
3. W celu zapobieżenia sytuacji nadmiernego kumulowania się uprawnień użytkowników w systemach informatycznych, przyjmuje się że zmiana uprawnień polega na odebraniu uprawnień przyznanych wcześniej i nadaniu nowych uprawnień, zgodnie z nowym wnioskiem i procedurą opisaną w ust. 1.

4. ABS we wniosku o nadanie lub odebranie uprawnień do systemów informatycznych określa, które z uprawnień mogą nie być odbierane w przypadku gdy zmiana uprawnień wiąże się ze zmianą stanowiska lub zakresu obowiązków Pracownika.
5. Jeżeli zmiana uprawnień Pracownika wiąże się ze zmianą jednostki organizacyjnej, KJO, z której Pracownik odchodzi, ma obowiązek wnioskować o odebranie uprawnień Pracownika zaznaczając, że Pracownik przechodzi do innej jednostki organizacyjnej.
6. W przypadku zakończenia zatrudnienia KJO, któremu podlegał użytkownik, ma obowiązek wnioskować o całkowite odebranie uprawnień użytkownika do systemów informatycznych.
7. Postępowanie z zasobami sieciowymi (zgromadzonymi plikami, wiadomościami poczty elektronicznej) użytkownika, którego zatrudnienie w SGSP ustało, jest każdorazowo uzgadniane pomiędzy ABS a właściwym KJO.

§ 25.
Dostęp podmiotów zewnętrznych

1. Podmioty zewnętrzne mogą otrzymać dostęp, w tym zdalny, do systemów informatycznych SGSP, jeżeli jest to niezbędne do zapewnienia ciągłości działania systemów informatycznych lub prawidłowej realizacji zaplanowanych prac.
2. KJO nadzorujący realizację umowy z podmiotem zewnętrznym wnioskuje o nadanie uprawnień dla pracowników podmiotu zewnętrznego, zgodnie z procedurą opisaną w § 21.
3. Uprawnienia do systemów informatycznych dla pracowników podmiotu zewnętrznego są przyznawane na czas określony. Za określenie czasu obowiązywania uprawnień odpowiada KJO nadzorujący realizację umowy. Czas ten nie może być jednak dłuższy niż 3 miesiące lub czas realizacji zadań wynikających z umowy.
4. Pracownicy podmiotów zewnętrznych zobowiązani są wskazać numer telefonu, pod którym można będzie uzyskać bieżące informacje dotyczące aktualnie prowadzonych przez nich prac.
5. Niezwłocznie po ustaniu potrzeby dostępu pracowników podmiotu zewnętrznego do systemów informatycznych SGSP, KJO nadzorujący realizację umowy ma obowiązek wnioskować o odebranie im uprawnień.

§ 26.
Zdalny dostęp do zasobów sieci wewnętrznej SGSP

1. Przyznanie zdalnego dostępu do zasobów sieci wewnętrznej SGSP odbywa się zgodnie z § 23 (lub § 25 - w przypadku podmiotów zewnętrznych) na podstawie wypełnionego przez właściwego KJO wniosku o nadanie lub odebranie uprawnień do systemów informatycznych, skierowanego do i zaakceptowanego przez ABS.
2. W przypadku zdalnego dostępu do zasobów sieci wewnętrznej SGSP podmiotów zewnętrznych, KJO jest zobowiązany do wniosku, o którym mowa w ust. 1 dołączyć podpisane oświadczenie podmiotu zewnętrznego (wzór oświadczenia stanowi załącznik nr 1 do niniejszego dokumentu).
3. W przypadku stwierdzenia braku wystarczających przesłanek oraz mając na względzie poziom zabezpieczeń sieci wewnętrznej SGSP, ABS może odmówić umożliwienia zdalnego dostępu do zasobów sieci wewnętrznej SGSP.
4. Dział IT wydaje zgodę na zdalny dostęp tylko do określonych usług, portów, podsieci lub poszczególnych adresów, w zakresie wymaganym do wykonywania zaplanowanych czynności.

5. Zakres prac prowadzonych w sposób zdalny przez użytkowników musi obejmować wyłącznie czynności wynikające z umowy będącej podstawą przyznania uprawnień zdalnego dostępu oraz uprawnień przyznanych przez Dział IT.
6. Jakiekolwiek rozszerzenia zakresu prac wymagają wcześniejszego pisemnego zgłoszenia i zaakceptowania przez Dział IT.
7. Dział IT każdorazowo określa rodzaj danych uwierzytelniających, zakres ich złożoności jak i sposób ich przekazania użytkownikowi.

§ 27.
Przegląd uprawnień

1. Przegląd uprawnień użytkowników w systemach informatycznych jest realizowany raz na 6 miesięcy.
2. Raz na 6 miesięcy jednostka organizacyjna właściwa do spraw kadr przesyła do Działu IT listę Pracowników, którzy zakończyli pracę w SGSP.
3. ASI na podstawie otrzymanej listy, o której mowa w ust. 5, mają obowiązek zweryfikowania i ewentualnego zablokowania kont użytkowników których zatrudnienie w SGSP ustało.

Rozdział 11

POZYSKIWANIE I ROZWÓJ SYSTEMÓW INFORMATYCZNYCH

§ 28.

Umowy dotyczące systemów informatycznych

1. ABS jest odpowiedzialny za przekazanie:
   1) wymagań technologicznych;
   2) wymagań bezpieczeństwa;
   3) wymagań dotyczących jakości świadczonych usług (SLA).
2. Wymagania funkcjonalne dotyczące nowego systemu informatycznego muszą być sformułowane przez właściwych KJO i przekazane do ABS.
3. Jeżeli system informatyczny lub oprogramowanie ma służyć przetwarzaniu danych osobowych w umowie z dostawcą należy zastrzec wymóg zapewnienia jego zgodności z obowiązującymi przepisami dotyczącymi danych osobowych.
4. Każda umowa, której realizacja wiąże się z możliwością dostępu podmiotów zewnętrznych do danych SGSP, musi zawierać postanowienia zobowiązujące podmiot zewnętrzny do zachowania poufności informacji do których będzie miał dostęp.
5. Umowa musi być parafowana przez ABS oraz właściwych KJO.

§ 29.
Planowanie systemów

1. Dla wszystkich systemów wskazanych przez ABS, ASI zobowiązany jest prowadzić bieżący monitoring wykorzystania zasobów.

2. Na podstawie analizy wyników monitorowania ABS szacuje zasoby systemów, które zapewnią ich prawidłowe funkcjonowanie.
3. ABS zobowiązany jest wnioskować o zakupy urządzeń i systemów zapewniających wymaganą wydajność ze względu na potrzeby SGSP, uwzględniając plany rozwojowe jednostek organizacyjnych.

§ 30.

Dopuszczenie systemów informatycznych do eksploatacji

1. O dopuszczeniu systemu informatycznego do użytkowania w środowisku produkcyjnym decyduje ABS.
2. System może zostać dopuszczony do użytkowania w środowisku produkcyjnym jeżeli:
   1) spełnia ustalone wymagania prawne, funkcjonalne, wydajnościowe, bezpieczeństwa;
   2) pozytywnie przeszedł testy funkcjonalne, wydajnościowe i bezpieczeństwa;
   3) posiada ustaloną przez ABS dokumentację umożliwiającą bieżącą eksploatację zarówno użytkownikom jak i administratorom (ASI i AD);
   4) posiada ustalone procedury odtwarzania po awarii.
3. Testy wydajnościowe i bezpieczeństwa są prowadzone przez AD, ASI lub podmioty zewnętrzne.
4. Testy funkcjonalne są prowadzone przez Pracowników jednostek organizacyjnych, które będą wykorzystywały system informatyczny.
5. Testy powinny być prowadzone w miarę możliwości w dedykowanych środowiskach testowych bez ingerencji w istniejące systemy produkcyjne.
6. Dane testowe w miarę możliwości należy anonimizować. Jeśli nie jest to możliwe, środowisko testowe musi zostać zabezpieczone na poziomie nie gorszym niż środowisko produkcyjne.
7. Z przeprowadzonych testów należy sporządzać raporty.
8. Wszelkie raporty i protokoły potwierdzające zgodność systemu informatycznego z wymaganiami prawnymi, funkcjonalnymi, wydajnościowymi i bezpieczeństwa należy przekazać ABS.

§ 31.

Zarządzanie podatnościami

1. Każde wykorzystywane w SGSP oprogramowanie powinno mieć wsparcie producenta w zakresie publikacji uaktualnień w szczególności poprawek związanych z bezpieczeństwem.
2. ASI są odpowiedzialni za bieżące śledzenie podatności wykorzystywanego w SGSP oprogramowania oraz instalację i konfigurację systemów informatycznych zgodnie z zaleceniami producenta oprogramowania oraz najlepszymi praktykami IT.
3. Instalacja uaktualnień oprogramowania działającego na serwerach i urządzeniach sieciowych musi być poprzedzona testami potwierdzającymi brak jej negatywnego wpływu na funkcjonowanie oprogramowania.
4. Instalacja uaktualnień oprogramowania stacji roboczych może być przeprowadzana automatycznie.
5. W przypadku braku możliwości instalacji poprawki bezpieczeństwa ASI wraz z ABS są odpowiedzialni za opracowanie rozwiązań zastępczych mających na celu minimalizację ryzyka związanego z występowaniem podatności oraz dokonanie oceny ryzyka związanego z dalszym wykorzystywaniem oprogramowania posiadającego błędy bezpieczeństwa.

§ 32.

Przeglądy i konserwacja systemów informatycznych

1. Bieżące monitorowanie i aktualizacja systemów informatycznych odbywa się zgodnie z zasadami opisanymi w § 31 oraz § 33.
2. Okresowe przeglądy mające na celu weryfikację stanu zabezpieczeń systemów informatycznych są realizowane zgodnie z ustalonym wewnętrznie w Dziale IT harmonogramem i uwzględnieniem zaleceń producentów sprzętu i oprogramowania.
3. Przeglądu, konserwacji i napraw mogą dokonywać ASI lub podmioty zewnętrzne na podstawie odrębnych zleceń lub umów.
4. Prace, dotyczące przeglądów, konserwacji i napraw sprzętu i oprogramowania, wymagające zaangażowania autoryzowanych firm zewnętrznych, są wykonywane przez uprawnionych pracowników tych firm pod nadzorem ASI, w miarę możliwości bez dostępu do danych.
5. W wypadku konieczności dostępu pracowników firm zewnętrznych do danych, podpisują oni oświadczenie o zachowaniu poufności informacji pozyskanych w trakcie wykonywania prac oraz sposobów zabezpieczeń tych danych - zgodnie ze wzorem zawartym w PODO.

Rozdział 12

MONITOROWANIE BEZPIECZEŃSTWA SYSTEMÓW INFORMATYCZNYCH

§ 33.

1. Monitorowanie bezpieczeństwa systemów informatycznych jest realizowane przez ASI w sposób ciągły za pomocą narzędzi do przeglądu logów systemowych, alarmów systemów firewall, systemów IDS, systemów antywirusowych.
2. Przyjmuje się domyślne zakresy rejestrowania zdarzeń:
   1) naruszenie bezpieczeństwa systemów, aplikacji lub informacji w nich przetwarzanych;
   2) awarie;
   3) objawy niedostatecznej wydajności;
   4) objawy niedostatecznej dostępności;
   5) objawy niedostatecznej jakości technicznego środowiska użytkowania systemów informatycznych;
   6) fakty niedostatecznych umiejętności użytkowników, przekroczenia uprawnień, niedopełnienia obowiązków;
   7) przejawy nielogicznego działania systemu, oczywistych wad, niezgodności z dokumentacją.
3. Wszystkie systemy informatyczne muszą posiadać włączone mechanizmy rejestrowania zdarzeń w zakresie wykrywania naruszeń bezpieczeństwa i awarii. Jeżeli system wymaga szerszego zakresu rejestrowania zdarzeń, wymagania te są określane przez ABS.
4. ASI prowadzą rejestr awarii i naruszeń bezpieczeństwa, w którym odnotowują zdarzenia sklasyfikowane jako "KRYTYCZNE" i "POWAŻNE". Wzór rejestru stanowi załącznik nr 2 do niniejszego dokumentu.

Rozdział 13

AUDYTY BEZPIECZEŃSTWA SYSTEMÓW INFORMATYCZNYCH

§ 34.

1. Systemy informatyczne SGSP powinny przynajmniej raz do roku przechodzić wewnętrzne audyty bezpieczeństwa.
2. Za ustalenie zakresu i harmonogramu audytu odpowiada jednostka organizacyjna właściwa do spraw audytu wewnętrznego.
3. Audyt jest przeprowadzany zgodnie z procedurami jednostki organizacyjnej właściwej do spraw audytu wewnętrznego.

Rozdział 14

SZKOLENIA DLA PRACOWNIKÓW

§ 35.

1. Szkolenia z zakresu bezpieczeństwa i zasad użytkowania systemów informatycznych są organizowane:
   1) przez AD dla każdego nowego Pracownika SGSP w terminie ustalanym z KJO;
   2) okresowo dla wszystkich Pracowników SGSP w terminie ustalonym przez jednostkę organizacyjną właściwą do spraw szkoleń, nie rzadziej niż raz na trzy lata;
   3) dla wszystkich Pracowników SGSP na wniosek Działu IT w związku z istotnymi zmianami zasad użytkowania systemów informatycznych.
2. W ramach szkoleń przedstawiane są zagadnienia wymienione w rozdziale 2.

Rozdział 15

REAGOWANIE NA INCYDENTY

§ 36.

1. Za obsługę incydentów związanych z systemami informatycznymi odpowiadają ASI.
2. ASI mają obowiązek klasyfikować ze względu na poziom istotności zdarzenia identyfikowane samodzielnie oraz zgłaszane przez Pracowników lub osoby trzecie, wg poniższych wytycznych:
   1) KRYTYCZNY - jeżeli przewidywane skutki zdarzenia mogą uniemożliwić realizację zadań SGSP jako uczelni państwowej oraz jednostki organizacyjnej PSP lub doprowadzić do utraty poufności, dostępności lub integralności danych (w szczególności danych osobowych);
   2) POWAŻNY - jeżeli przewidywane skutki zdarzenia mogą w istotny sposób utrudnić realizację zadań SGSP jako uczelni państwowej oraz jednostki organizacyjnej PSP w związku z obniżoną jakością usług dostarczanych przez systemy informatyczne;
   3) NISKI - jeżeli przewidywane skutki zdarzenia są ograniczone w skali i zasięgu oraz jest mało prawdopodobne, aby negatywnie wpływały na działalność SGSP.
3. ASI przyjmujący zgłoszenie dotyczące systemu informatycznego jest odpowiedzialny za:
   1) zarejestrowanie zgłoszenia w systemie Help-Desk;
   2) analizę zgłoszenia i określenie:

a) rodzaju zdarzenia: błąd użytkownika, awaria systemu, naruszenie bezpieczeństwa,
b) poziomu istotności zdarzenia: Niski, Poważny, Krytyczny.

4. Zdarzenia zaklasyfikowane jako "błąd użytkownika" lub "awaria systemu" są obsługiwane zgodnie
z procedurami wewnętrznymi Działu IT.
5. W przypadku potwierdzenia naruszenia bezpieczeństwa informacji przetwarzanych w systemie informatycznym tj. wystąpienia incydentu bezpieczeństwa, ASI ma obowiązek powiadomić ABS w celu ustalenia dalszego sposobu postępowania. Postępowanie to obejmuje:
   1) w przypadkach zaklasyfikowanych jako "Poważne" i "Krytyczne" - powiadomienie ABS, który z kolei przekazuje informację Rektorowi-Komendantowi SGSP, odnotowanie naruszenia bezpieczeństwa w *Rejestrze awarii i naruszeń bezpieczeństwa*;
   2) zgromadzenie i zabezpieczenie materiału dowodowego umożliwiającego dalszą analizę incydentu;
   3) zapobieżenie rozprzestrzenianiu się zagrożenia w systemach informatycznych;
   4) likwidację skutków zdarzenia;
   5) przywrócenie prawidłowego funkcjonowania systemu informatycznego;
   6) identyfikację przyczyny wystąpienia zdarzenia;
   7) opracowanie raportu z zaistniałej sytuacji (dla przypadków "Poważny" i "Krytyczny").

Załącznik Nr 1

Oświadczenie podmiotu zewnętrznego w związku uzyskaniem zdalnego dostępu do zasobów SGSP

.....

imię i nazwisko

.....

nazwa przedsiębiorcy

OŚWIADCZENIE

W związku z zawartą z Szkołą Główną Służby Pożarniczej (SGSP) umową nr ....., w imieniu przedsiębiorcy działającego pod firmą .....

z siedzibą w ....., pod adresem .....

.....

NIP ..... Regon ..... oświadczam, że:

1. Pracownikami, którzy prowadzić będą zdalne prace wynikające z umowy nr są:

1) ....., tel. kontaktowy ……..

2) ....., tel. kontaktowy ……..

2. wymienione wyżej osoby, które z racji wykonywania obowiązków wynikających z powołanej umowy dokonywać będą zdalnych prac w sieci wewnętrznej SGSP zostały zapoznane z obowiązującymi w SGSP zasadami pracy zdalnej.

W załączeniu wypełnione przez wyżej wymienione osoby oświadczenia zawierające zobowiązanie do przestrzegania zasad pracy zdalnej w SGSP zgodnie z obowiązującym w SGSP wzorem.

Przedsiębiorca ponosi wszelką i nieograniczoną odpowiedzialność, w tym za wszelkie szkody lub starty faktyczne lub prawne jakie poniesie SGSP w przypadku naruszenia przez wymienione wyżej osoby lub jakichkolwiek naszych innych pracowników lub współpracowników obowiązujących w SGSP zasad pracy zdalnej.

....., dnia ....

(miejsce) (data) (pieczęć i podpis)

Załącznik Nr 2

Rejestr awarii i naruszeń bezpieczeństwa

Rejestr awarii i naruszeń bezpieczeństwa /p*rzykład*/							
Data zdarzenia w formacie dd:mm:rr	**Czas wystąpienia zdarzenia zdarzenia** hh:mm	**Kod zdarzenia:** A - awaria, N - naruszenie bezpieczeństwa	**Nazwa urządzenia/ adres IP**	**Opis zdarzenia**	**Poziom istotności zdarzenia**	**Opis podjętych działań**	**Osoby zaangażowane w obsługę zdarzenia**
12.01.2022	10:20	N	stacje robocze LAN	rozprzestrzenianie się wirusa	poważny	usunięcie wirusa, aktualizacja programów antywirusowych	
19.01.2022	10:00	A	serwer bazy danych	brak miejsca na dysku	krytyczny	usunięcie starych kopii danych, przywrócenie funkcjonalności	

Poziom istotności awarii:

- KRYTYCZNY - trwały brak możliwości prawidłowego funkcjonowania systemu informatycznego w wyniku katastrofy, awarii lub naruszenia bezpieczeństwa, w konsekwencji uniemożliwiający realizowanie zadań SGSP jako uczelni państwowej oraz jednostki organizacyjnej PSP, uzależnionych od usług właściwych dla danego systemu

- POWAŻNY - awaria komponentu pomocniczego systemu mogąca mieć wpływ na prawidłową realizację zadań SGSP jako uczelni państwowej oraz jednostki organizacyjnej PSP

- NISKI - faktyczne zakłócenie lub podejrzenie zagrożenia niemające bezpośredniego wpływu na prawidłowe działanie systemu, bezpieczeństwo przetwarzanych informacji lub poprawność wykonywania czynności/procesów, uzależnionych od usług właściwych dla danego systemu

Poziom istotności naruszenia bezpieczeństwa:

- KRYTYCZNY - jeżeli przewidywane skutki zdarzenia mogą uniemożliwić realizację zadań SGSP jako uczelni państwowej oraz jednostki organizacyjnej PSP lub doprowadzić do utraty poufności, dostępności lub integralności danych (w szczególności danych osobowych)

- POWAŻNY - jeżeli przewidywane skutki zdarzenia mogą w istotny sposób utrudnić realizację zadań SGSP jako uczelni państwowej oraz jednostki organizacyjnej PSP w związku z obniżoną jakością usług dostarczanych przez systemy informatyczne

- NISKI - jeżeli przewidywane skutki zdarzenia są ograniczone w skali i zasięgu oraz jest mało prawdopodobne, aby negatywnie wpływały na działalność SGSP