DZIENNIK URZĘDOWY

Głównego Inspektoratu Transportu Drogowego

Warszawa, dnia 12 lutego 2015 r.

Poz. 8

Z A R Z Ą D Z E N I E N R 8 / 2 0 1 5

G Ł Ó W N E G O I N S P E K T O R A T R A N S P O R T U D R O G O W E G O

z dnia 12 lutego 2015 r.

w sprawie wprowadzenia Polityki Bezpieczeństwa Systemów Informatycznych w Głównym Inspektoracie Transportu Drogowego

Na podstawie art. 36 ust. 1 i ust. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r. poz. 1182 i 1662) oraz art. 52 ust. 1 ustawy z dnia 6 września 2001 r. o transporcie drogowym (Dz. U. z 2013 r. poz. 1414 oraz z 2014 r. poz. 486, 805, 915 i 1310), zarządza się, co następuje:

§ 1. W Głównym Inspektoracie Transportu Drogowego wprowadza się Politykę Bezpieczeństwa Systemów Informatycznych, stanowiącą załącznik do niniejszego zarządzenia.

§ 2. Traci moc zarządzenie nr 45/2011 Głównego Inspektora Transportu Drogowego z dnia 4 października 2011 r. w sprawie wprowadzenia zasad przetwarzania danych osobowych, zasad dotyczących kont użytkowników, sprzętu komputerowego i systemu teleinformatycznego, Polityki Bezpieczeństwa i Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

§ 3. Zarządzenie wchodzi w życie z dniem 15 lutego 2015 r.

Główny Inspektor Transportu Drogowego**:** *wz. M. Maksimiuk*

Załącznik do zarządzenia nr 8/2015
Głównego Inspektora Transportu Drogowego
z dnia 12 lutego 2015 r.

POLITYKA BEZPIECZEŃSTWA SYSTEMÓW INFORMATYCZNYCH W GŁÓWNYM INSPEKTORACIE TRANSPORTU DROGOWEGO

Spis treści:

Załączniki:

Rozdział 1

Postanowienia ogólne

§ 1. Polityka Bezpieczeństwa Systemów Informatycznych określa zasady zarządzania systemami i sieciami teleinformatycznymi w Głównym Inspektoracie Transportu Drogowego. Dokument jest przeznaczony dla wszystkich pracowników GITD.

§ 2. Użyte w niniejszej Polityce Bezpieczeństwa Systemów Informatycznych pojęcia i skróty oznaczają:

1) ASI – Administratora Systemu Informatycznego wyznaczonego przez Dyrektora Generalnego Głównego Inspektoratu Transportu Drogowego;
2) BIŁ – Biuro Informatyki i Łączności;
3) DIT – dyrektora Biura Informatyki i Łączności;
4) GITD - Główny Inspektorat Transportu Drogowego;
5) pracownik – osobę pozostającą z GITD w stosunku pracy na podstawie umowy o pracę lub na podstawie mianowania;
6) użytkownik – osobę w jakikolwiek sposób użytkującą systemy informatyczne w GITD;
7) incydent bezpieczeństwa – każde potwierdzone naruszenie przez pracowników GITD (lub osoby trzecie), bezpieczeństwa informacji przetwarzanych w systemie informatycznym lub zasad użytkowania systemów informatycznych określonych w niniejszym dokumencie;
8) KKO – kierownika komórki organizacyjnej;
9) PBSIT – Politykę Bezpieczeństwa Systemów Informatycznych.

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. Pracownicy mogą korzystać wyłącznie z tych systemów informatycznych, programów i zasobów informatycznych, do korzystania z których zostały nadane im uprawnienia.

3. 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.

4. Zabrania się pracownikom wykorzystywania do celów służbowych, prywatnych urządzeń informatycznych, w szczególności ich podłączania do sieci informatycznej GITD, jeżeli nie zostały one skonfigurowane i zabezpieczone przez ASI.

5. Zabrania się pracownikom instalowania oraz zmiany konfiguracji jakiegokolwiek oprogramowania, urządzenia i służbowego sprzętu informatycznego bez uzyskania zgody ASI, chyba że działanie takie wynika z zakresu obowiązków pracownika.

6. Potrzebę instalacji dodatkowego oprogramowania lub sprzętu informatycznego należy zgłaszać w systemie QDesk.

7. Za umożliwienie wykorzystania powierzonego sprzętu informatycznego przez inną osobę (pracownika, gościa itp.) w szczególności uzyskanie przez nią nieautoryzowanego dostępu do plików zapisanych lokalnie na urządzeniu oraz w zasobach sieciowych odpowiada pracownik, któremu sprzęt przydzielono.

8. Wszystkie pochodzące z zewnątrz nośniki lub inne media z danymi muszą być sprawdzane przy pomocy aktualnego oprogramowania antywirusowego.

9. 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.

10. Zabrania się przekazywania informacji o wykorzystywanym w GITD sprzęcie komputerowym, oprogramowaniu, sieci, kartach dostępowych, procedurach oraz
o wszelkich stosowanych środkach bezpieczeństwa. Informacji tych mogą udzielać jedynie pracownicy BIŁ.

11. Utrata lub kradzież sprzętu muszą być niezwłocznie zgłaszane do BIŁ.

§ 4. Zasady korzystania z haseł

1. Otrzymane przez pracownika 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. Pracownicy muszą stosować hasła zgodne z polityką tworzenia haseł przyjętą w GITD.

3. Jeżeli system informatyczny z powodów technologicznych nie ma możliwości wymuszenia odpowiednio silnego hasła lub wymuszenia jego zmiany co 30 dni; pracownicy 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) zmiany hasła co 30 dni i nie używania starego hasła lub hasła o strukturze zbliżonej do starego hasła;
3) niezwłocznej zmiany hasła, gdy istnieje uzasadnione podejrzenie naruszenia bezpieczeństwa systemu lub ujawnienia hasła;
4) zmiany hasła tymczasowego 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 usług internetowych i poczty elektronicznej

1. Pracownicy mogą przeglądać zasoby sieci Internet wyłącznie w celach związanych z wykonywaną pracą. Zabrania się w szczególności przeglądania treści o charakterze pornograficznym, rozrywkowym itp. 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 pracownikom wykorzystywania prywatnych skrzynek pocztowych do celów służbowych. Do celów służbowych pracownikowi przydzielana jest firmowa skrzynka pocztowa. Wszelka korespondencja służbowa musi odbywać się za pośrednictwem firmowych skrzynek pocztowych.

5. Korzystanie z firmowej 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 użytkownikom otwierania załączników do poczty elektronicznej, jeżeli pochodzi ona z niewiadomego źródła (np. od nieznanych osób, zwłaszcza spoza GITD).

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 poza sieć GITD muszą być zabezpieczane kryptograficznie (np. hasło do pliku lub inna forma szyfrowania wskazana przez ASI).

10. Wszelkie działania pracownika na służbowym sprzęcie komputerowym, w tym działania w sieci Internet wykonywane z sieci wewnętrznej GITD oraz wiadomości znajdujące się w skrzynce służbowej poczty elektronicznej mogą być monitorowane przez pracodawcę lub upoważnionych przez niego pracowników.

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.

§ 6. Rozpoczęcie, zakończenie, zawieszenie pracy w systemach informatycznych

1. Przed przystąpieniem do pracy z systemem informatycznym, użytkownik 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 QDesk.

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 klawisz ⊞ + L).

8. Kończąc pracę, użytkownik 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 komputerów przenośnych

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

2. Użytkownicy komputerów przenośnych mają prawo do samodzielnej zmiany konfiguracji kart sieciowych oraz instalacji aktualizacji zainstalowanego oprogramowania.

3. 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.

4. Komputer przenośny nie może być pozostawiony bez opieki osoby, której został powierzony.

5. Komputer przenośny użytkowany poza siedzibą GITD musi być przechowywany w miejscach minimalizujących ryzyko przypadkowego uszkodzenia oraz kradzieży.

6. Komputery przenośne, które są użytkowane poza siedzibą GITD powinny być transportowane w specjalnie do tego celu przeznaczonych torbach, chroniących je przed uszkodzeniami mechanicznymi.

7. Podczas transportu komunikacją publiczną zaleca się unikać umieszczania komputera przenośnego w ogólnodostępnych bagażnikach, do których dostęp mają inni pasażerowie.

§ 8. Zasady pracy zdalnej

1. Przetwarzanie przez pracowników danych osobowych w związku z wykonywaniem przez nich obowiązków służbowych następuje wyłącznie w siedzibie GITD.

2. Poza siedzibą GITD lub w ramach telepracy pracownicy mogą przetwarzać:

1) informacje zawierające dane osobowe, zgodnie z obowiązującymi w GITD zasadami przetwarzania danych osobowych;

2) informacje będące tajemnicą pracodawcy za uprzednią zgodą KKO

wyłącznie z wykorzystaniem połączeń VPN/IPSec, na służbowych komputerach przenośnych.

3. W trakcie trwania połączenia VPN/IPSec pomiędzy komputerem pracownika, a siedzibą GITD na komputerze pracownika automatycznie blokowana jest wszelka pozostała łączność Internetowa. Ma to za zadanie dodatkowe podniesienie poziomu zabezpieczeń.

4. Niedozwolone jest samodzielne dokonywanie jakichkolwiek ingerencji w strukturę oraz konfigurację oprogramowania klienta VPN.

5. Wszelkie prace prowadzone za pomocą zdalnego dostępu do sieci muszą przebiegać w taki sposób by w ich wyniku nie doszło do uszkodzeń bądź nieplanowanych przerw w działaniu infrastruktury informatycznej GITD.

6. Obowiązkiem użytkownika jest zapewnienie, by w wyniku jego działań nie doszło do nieuprawnionych modyfikacji danych znajdujących się w systemach teleinformatycznych GITD.

7. Użytkownikom nie wolno wykorzystywać uzyskanych praw dostępu do innych celów niż określone we wniosku o nadanie uprawnień.

8. Użytkownika obowiązuje zakaz udostępniania utworzonego zdalnego połączenia innym osobom.

9. Zabrania się samodzielnego testowania zabezpieczeń sieci wewnętrznej GITD. Wszelkie działania w tym zakresie wymagają wcześniejszej zgody DIT oraz muszą obywać się pod kontrolą wyznaczonego ASI.

10. Użytkownicy ponoszą pełną odpowiedzialność za wszelkie czynności wykonane podczas zdalnej pracy w sieci wewnętrznej GITD z użyciem ich danych uwierzytelniających.

11. Użytkownik, 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.

12. W trakcie pracy użytkownicy zobowiązani są do posługiwania się licencjonowanym oprogramowaniem z zainstalowanymi aktualnymi, krytycznymi aktualizacjami.

13. Użytkownicy uzyskujący uprawnienia zdalnego dostępu mają obowiązek dołożenia starań w zakresie zagwarantowania bezpieczeństwa połączenia. Podstawowym wymogiem jest stosowanie właściwie skonfigurowanego systemu zabezpieczającego typu „firewall”.

14. Przed przystąpieniem do zdalnej pracy, użytkownik jest zobowiązany do sprawdzenia systemu informatycznego programem antywirusowym z zainstalowanymi aktualnymi definicjami wirusów oraz do sprawdzenia systemu pod kątem obecności oprogramowania szpiegującego.

15. Użytkownicy zobligowani są do niezwłocznego pisemnego lub elektronicznego zgłaszania ASI wszelkich zaobserwowanych nieprawidłowości w funkcjonowaniu oprogramowania VPN oraz podejrzeń przejęcia hasła dostępu do służbowego konta użytkownika.

16. Użytkownicy zobowiązani są wskazać numer telefonu, pod którym można będzie uzyskać bieżące informacje dotyczące aktualnie prowadzonych przez nich prac.

17. Wszystkie zdalne połączenia do sieci wewnętrznej GITD będą rejestrowane.

18. BIŁ jest uprawnione 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.

19. W przypadku ujawnienia przez BIŁ przypadków korzystania z uprawnień zdalnego dostępu w sposób niezgodny z zasadami lub przyznanym zakresem uprawnień BIŁ może:

1) cofnąć przyznane uprawnienia do korzystania z sieci;
2) wnioskować do właściwego KKO o:
   a) zastosowanie wobec pracownika kary porządkowej przewidzianej w regulaminie pracy GITD,
   b) rozwiązanie umowy o współpracy w przypadku współpracownika,
   c) obciążenie karami wynikającymi w umowy, w przypadku gdy użytkownikiem był podmiot zewnętrzny.

§ 9. Zgłaszanie incydentów i podatności

1. Pracownicy mają obowiązek zgłaszać do ASI wszelkiego rodzaju zdarzenia, które w ich ocenie mają lub mogą mieć negatywny wpływ na bezpieczeństwo informacji przetwarzanych w systemach informatycznych.

2. Wszyscy pracownicy, a w szczególności ASI, powinni 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 GITD poza siedzibą GITD.

3. Zgłoszeń można dokonywać w systemie QDesk, telefonicznie lub za pośrednictwem poczty elektronicznej.

4. W przypadku zdarzeń związanych z systemami informatycznymi **zabrania się** pracownikom podejmowania jakichkolwiek działań w systemie informatycznym bez wcześniejszej konsultacji z ASI.

5. Niezgłoszenie przez pracownika zaistniałego zdarzenia, odmowa udzielenia wyjaśnień dotyczących zaistniałych incydentów lub próba samodzielnego potwierdzenia występowania podatności systemu informatycznego może być podstawą do wyciągnięcia wobec pracownika sankcji porządkowych, dyscyplinarnych lub karnych.

§ 10. Odpowiedzialność użytkownika

Umyślne lub nieumyślne naruszenie przedstawionych zasad bezpieczeństwa systemów informatycznych lub niestosowanie się do poleceń służbowych w tym zakresie może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych.

Rozdział 3

Zarządzanie sprzętem i oprogramowaniem

§ 11. 1. W GITD sprzęt informatyczny oraz oprogramowanie mogą być wdrażane i użytkowane jedynie po uzyskaniu akceptacji DIT.

2. BIŁ prowadzi Wykaz eksploatowanych systemów informatycznych oraz Wykaz licencjonowanego oprogramowania.

3. Systemy informatyczne mogą być dopuszczone do produkcyjnego użytkowania po ich skonfigurowaniu przez ASI, zatwierdzeniu ich konfiguracji przez DIT oraz wpisaniu na Wykaz eksploatowanych systemów informatycznych.

4. W przypadku wykrycia użytkowania przez pracowników GITD nieautoryzowanego sprzętu lub oprogramowania, DIT powinien poinformować o tym KKO wraz z wnioskiem o podjęcie odpowiednich działań porządkowych.

5. Szczegółowe zasady dotyczące wydawania/odbierania sprzętu informatycznego użytkownikom zawiera wewnętrzna Instrukcja BIŁ.

Rozdział 4

Zarządzanie dokumentacją systemów informatycznych

§ 12. 1. Podstawowym dokumentem regulującym zasady zarządzania bezpieczeństwem systemów informatycznych jest PBSIT. Za jej opracowanie i aktualizację odpowiada DIT.

2. DIT określa systemy informatyczne, dla których muszą zostać opracowane dodatkowe dokumenty: instrukcje użytkowania systemów (dla użytkowników) i instrukcje zarządzania systemami (dla administratorów).

3. Za opracowanie instrukcji, o których mowa w ust. 2, dla wskazanych systemów informatycznych odpowiadają ASI.

4. W instrukcjach uwzględniane są następujące zagadnienia:

1) w instrukcji użytkowania systemu informatycznego - 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,
   c) procedury tworzenia kopii zapasowych,
   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.

5. ASI uzupełnia **Wykaz eksploatowanych systemów informatycznych** o tytuły opracowanych instrukcji dla poszczególnych systemów.

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 DIT jest zobowiązany do przeglądu PBSIT oraz pozostałej dokumentacji systemów informatycznych i potwierdzenia jej kompletności oraz aktualności przez złożenie podpisu w metrykach poszczególnych dokumentów.

Rozdział 5

Analiza ryzyka i dobór zabezpieczeń dla systemów informatycznych

§ 13. 1. DIT określa w niniejszym dokumencie **podstawowy poziom zabezpieczeń systemów informatycznych** obowiązujący w GITD. Jeśli w wyniku przeprowadzanej szczegółowej analizy ryzyka nie ustalono stosowania innych zabezpieczeń, należy stosować zabezpieczenia poziomu podstawowego. Za konfigurację zabezpieczeń odpowiadają ASI.

2. Analiza ryzyka dla bezpieczeństwa informacji jest prowadzona przez wszystkie jednostki organizacyjne GITD, zgodnie z ustaloną metodyką.

3. W procesie analizy ryzyka dla bezpieczeństwa informacji pracownicy BIŁ 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.

Za określenie skutków utraty poufności, dostępności i integralności danych przetwarzanych w systemach informatycznych oraz akceptowalnego poziomu ryzyka odpowiadają KKO.

4. Działania BIŁ 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.

5. 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.

6. Analiza ryzyka dla istniejących systemów informatycznych powinna prowadzić do potwierdzenia lub zaprzeczenia skuteczności istniejących zabezpieczeń oraz ewentualnego przedstawienia rekomendacji dla podniesienia poziomu bezpieczeństwa.

7. Przeprowadzenie analizy ryzyka przez BIŁ jest dokumentowane w raportach z analizy ryzyka opracowywanych zgodnie z ustaloną metodyką szacowania ryzyka.

8. Dyrektor Generalny GITD jest odpowiedzialny za zatwierdzenie proponowanych zabezpieczeń poziomu podstawowego oraz zabezpieczeń i działań korygujących wynikających z analizy ryzyka.

Rozdział 6

Podstawowy poziom zabezpieczeń infrastruktury informatycznej GITD

§ 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 GITD zaleca się stosować kryptograficzne zabezpieczenia transmisji danych lub fizycznego zabezpieczenia trasy;
3) szafy krosownicze muszą znajdować się w pomieszczeniach zapewniających kontrolę dostępu;
4) niewykorzystywane gniazdka sieci informatycznej powinny być wyłączone;
5) 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 GITD 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 GITD;
3) ruch sieciowy pomiędzy poszczególnymi podsieciami i vlanami sieci wewnętrznej GITD powinien być filtrowany za pomocą list kontroli dostępu (ACL) konfigurowanych na przełącznikach sieciowych;
4) adresy sprzętowe MAC poszczególnych urządzeń sieci wewnętrznej muszą być przypisywane do poszczególnych portów przełączników sieciowych;

5) systemy informatyczne GITD 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;
6) utworzenie połączeń sieci GITD z siecią innego podmiotu lub siecią publiczną wymaga zgody DIT określającej wymagane zabezpieczenia, zakres i czas połączenia;
7) konfiguracja urządzeń sieciowych musi zapewniać, że połączenia użytkowników z sieciami publicznymi lub sieciami innych podmiotów są kontrolowane i realizowane wyłącznie przez infrastrukturę zarządzaną przez BIŁ;
8) 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 GITD;
9) 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 DIT.

4. Dostęp do zasobów sieci wewnętrznej GITD:

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 GITD do zasobów sieci publicznych wyłącznie do usług i protokołów, które są im niezbędne do wykonywania pracy;
2) jeśli nie zostanie to określone we wniosku o nadanie uprawnień należy przyjmować, że użytkownicy mogą mieć dostęp wyłącznie do zasobów udostępnianych za pośrednictwem protokołów HTTP (port 80), HTTPS (port 443). Jako usługi udostępniane za pośrednictwem

wymienionych protokołów należy rozumieć dostęp wyłącznie do serwerów WWW z wykluczeniem innych usług, które mogą być udostępniane na wymienionych portach (np. komunikatory, serwery proxy lub inne usługi mogące być wykorzystane do tworzenia ukrytych kanałów wymiany/przesyłu informacji);

3) użytkownicy sieci wewnętrznej, chcący uzyskać dostęp do usług i zasobów sieci publicznych muszą poprawnie przejść proces uwierzytelnienia wymuszany przez elementy infrastruktury informatycznej GITD;

4) 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) zmianę haseł co 30 dni,
   c) tworzenie hasła różnego od co najmniej 12 poprzednich,
   d) blokowanie dostępu na 15 minut po 5 nieudanych próbach logowania;

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 GITD 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 DIT.

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) wszystkie serwery muszą być wyposażone w macierze dyskowe;
4) na serwerach sieciowych muszą być wydzielane dedykowane zasoby na których użytkownicy będą mogli przechowywać swoje pliki;
5) dla wszystkich serwerów produkcyjnych muszą być wykonywane kopie bezpieczeństwa;
6) DIT 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;
3) maksymalna akceptowalna zwłoka w instalacji poprawki bezpieczeństwa powinna wynosić 7 dni od jej publikacji przy jednoczesnym zastosowaniu rozwiązań zastępczych minimalizujących ryzyko naruszeń bezpieczeństwa w tym okresie.

§ 16. Zabezpieczenia stacji roboczych

1. Stacje robocze muszą być podłączone do domeny Active Directory GITD 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) zmianę haseł co 30 dni;
3) tworzenie hasła różnego od co najmniej 12 poprzednich;
4) blokowanie dostępu na 15 minut po 5 nieudanych próbach logowania.

3. Użytkownicy nie mogą posiadać na stacjach roboczych lokalnych kont z uprawnieniami administracyjnymi.

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. Aktualizacja oprogramowania antywirusowego i skanowanie muszą następować przynajmniej raz dziennie w sposób automatyczny.

6. Stacje robocze muszą posiadać włączone mechanizmy 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;

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) przyznawane pracownikom 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 GITD należy w miarę możliwości 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 GITD jest wymagane należy rozumieć:

1) Systemy awaryjnego zasilania (generatory prądotwórcze lub alternatywne linie zasilające);

b) Systemy podtrzymywania zasilania (UPS);

3) Systemy klimatyzacji;

4) Systemy gaszenia;

5) Systemy alarmowe.

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.

3. Protokoły z testów i przeglądów systemów wspomagających są przechowywane przez DIT lub osobę przez niego wyznaczoną.

Rozdział 7

Zarządzanie kopiami bezpieczeństwa

§ 20. 1. DIT ustala w porozumieniu z właściwymi KKO sposób wykonywania kopii bezpieczeństwa poszczególnych systemów informatycznych z uwzględnieniem potrzeb biznesowych 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 zapasowych.

3. Wymagane jest przechowywanie kopii bezpieczeństwa poza lokalizacją w której znajduje się system informatyczny dla którego wykonuje się kopię bezpieczeństwa.

4. Zatwierdzone podpisem właściwego KKO zasady wykonywania kopii bezpieczeństwa dla systemu informatycznego są przechowywane przez BIŁ.

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 GITD muszą być zapisywane przez użytkowników na dedykowanych zasobach sieciowych wskazanych przez DIT.

7. Odtwarzanie kopii bezpieczeństwa następuje w wyniku:

1) działań realizowanych przez BIŁ związanych z obsługą awarii lub rekonfiguracją systemu informatycznego;
2) okresowego sprawdzania możliwości odtworzenia kopii bezpieczeństwa przez BIŁ;
3) na wniosek KKO skierowany do BIŁ.

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

Rozdział 8

Zarządzanie uprawnieniami użytkowników

§ 21. 1. Nadawanie uprawnień

1. DIT ustala i udostępnia w sieci wewnętrznej GITD wzór Wniosku o nadanie lub odebranie uprawnień do systemów informatycznych.

2. Uprawnienia do systemu informatycznego mogą być nadawane, odbierane lub modyfikowane wyłącznie na podstawie wypełnionego wniosku w postaci elektronicznej lub papierowej skierowanego do BIŁ i zaakceptowanego przez właściwego KKO.

3. KKO akceptujący wniosek, jest zobowiązany do jego weryfikacji pod kątem zgodności wnioskowanych uprawnień z zakresem obowiązków podległego pracownika lub pracownika podmiotu zewnętrznego.

4. Wniosek, który wpłynął do BIŁ, jest akceptowany przez DIT i przekazywany do realizacji właściwym ASI.

5. ASI realizują wniosek oraz prowadzą rejestr identyfikatorów przyznanych użytkownikom w poszczególnych systemach informatycznych.

6. Wnioski o nadanie lub odebranie uprawnień do systemów informatycznych są archiwizowane przez BIŁ.

7. BIŁ przekazuje informacje o przyznanych identyfikatorach i hasłach bezpośrednio użytkownikowi.

§ 22. 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 KKO i skierowanego do BIŁ.

2. 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.

3. DIT 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.

4. Jeżeli zmiana uprawnień użytkownika wiąże się ze zmianą komórki organizacyjnej, KKO, z której użytkownik odchodzi, ma obowiązek wnioskować o odebranie uprawnień użytkownika zaznaczając, że użytkownik przechodzi do innej komórki organizacyjnej.

5. W przypadku zakończenia zatrudnienia KKO, któremu podlegał pracownik, ma obowiązek wnioskować o całkowite odebranie uprawnień użytkownika do systemów informatycznych.

6. Postępowanie z zasobami sieciowymi (zgromadzonymi plikami, wiadomościami poczty elektronicznej) użytkownika, którego zatrudnienie w GITD ustało, jest każdorazowo uzgadniane pomiędzy DIT a właściwym KKO.

§ 23. Dostęp podmiotów zewnętrznych

1. Podmioty zewnętrzne mogą otrzymać dostęp do systemów informatycznych GITD tylko jeżeli przewidują to zawarte z nimi umowy.

2. KKO 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 KKO nadzorujący realizację umowy. Czas ten nie może być jednak dłuższy niż 3 miesiące lub czas realizacji zadań wynikających z umowy.

4. Niezwłocznie po ustaniu potrzeby dostępu pracowników podmiotu zewnętrznego do systemów informatycznych GITD, KKO nadzorujący realizację umowy ma obowiązek wnioskować o odebranie im uprawnień.

§ 24. Zdalny dostęp do zasobów sieci wewnętrznej GITD

1. Przyznanie zdalnego dostępu do zasobów sieci wewnętrznej GITD odbywa się zgodnie z § 21 (lub § 23 – w przypadku podmiotów zewnętrznych) na podstawie wypełnionego wniosku o nadanie lub odebranie uprawnień do systemów informatycznych, skierowanego do BIŁ i zaakceptowanego przez właściwego KKO.

2. W przypadku zdalnego dostępu do zasobów sieci wewnętrznej GITD podmiotów zewnętrznych, KKO 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 GITD, DIT może odmówić umożliwienia zdalnego dostępu do zasobów sieci wewnętrznej GITD.

4. BIŁ 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 BIŁ.

6. Jakiekolwiek rozszerzenia zakresu prac wymagają wcześniejszego pisemnego zgłoszenia i zaakceptowania przez BIŁ.

7. BIŁ każdorazowo określa rodzaj danych uwierzytelniających, zakres ich złożoności jak i sposób ich przekazania użytkownikowi.

§ 25. Przegląd uprawnień

1. Przegląd uprawnień użytkowników w systemach informatycznych jest realizowany raz na 6 miesięcy.

2. ASI wysyłają do KKO listy kont użytkowników w poszczególnych systemach informatycznych.

3. KKO mają obowiązek weryfikacji przesłanych list i potwierdzenia aktualności każdego konta użytkownika na przesłanej liście. KKO wysyłają zwrotnie do ASI potwierdzone listy w ciągu 5 dni roboczych od daty ich otrzymania.

4. Konta, których konieczności istnienia KKO nie potwierdzili, są niezwłocznie blokowane przez ASI.

5. Raz na 6 miesięcy komórka organizacyjna właściwa do spraw kadr przesyła do BIŁ listę pracowników, którzy zakończyli pracę w GITD.

6. ASI na podstawie otrzymanej listy, o której mowa w ust. 5, mają obowiązek zweryfikowania i ewentualnego zablokowania kont użytkowników których zatrudnienie w GITD ustało.

Rozdział 9

Pozyskiwanie i rozwój systemów informatycznych

§ 26. Umowy dotyczące systemów informatycznych

1. DIT jest odpowiedzialny za przekazanie:

1) wymagań technologicznych;
2) wymagań bezpieczeństwa;
3) wymagań dotyczących jakości świadczonych usług (SLA).

Wymagania funkcjonalne nowego systemu informatycznego muszą być sformułowane przez właściwych KKO i przekazane do komórki organizacyjnej właściwej do spraw pomocy prawnej GITD.

2. 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.

3. Każda umowa, której realizacja wiąże się z możliwością dostępu podmiotów zewnętrznych do danych GITD, musi zawierać postanowienia zobowiązujące podmiot zewnętrzny do zachowania poufności informacji do których będzie miał dostęp.

4. Umowa musi być parafowana przez DIT oraz właściwych KKO.

§ 27. Planowanie systemów

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

2. Na podstawie analizy wyników monitorowania DIT szacuje zasoby systemów, które zapewnią ich prawidłowe funkcjonowanie.

3. DIT zobowiązany jest wnioskować o zakupy urządzeń i systemów zapewniających wymaganą wydajność ze względu na potrzeby biznesowe GITD, uwzględniając plany rozwojowe komórek organizacyjnych.

§ 28. Dopuszczenie systemów informatycznych do eksploatacji

1. O dopuszczeniu systemu informatycznego do użytkowania w środowisku produkcyjnym decyduje DIT.

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 DIT dokumentację umożliwiającą bieżącą eksploatację zarówno użytkownikom jak i pracownikom BIŁ;

4) posiada ustalone procedury odtwarzania po awarii.

3. Testy wydajnościowe i bezpieczeństwa są prowadzone przez pracowników BIŁ lub podmioty zewnętrzne.

4. Testy funkcjonalne są prowadzone przez pracowników komórek 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 przechowuje DIT.

§ 29. Zarządzanie podatnościami

1. Każde wykorzystywane w GITD 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 GITD 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. Maksymalna akceptowalna zwłoka w instalacji poprawki bezpieczeństwa wynosi 7 dni od daty jej publikacji. Brak instalacji poprawki po tym czasie musi być uzasadniony przez ASI w notatce kierowanej do DIT.

6. W przypadku braku możliwości instalacji poprawki bezpieczeństwa ASI wraz z DIT 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.

§ 30. Przeglądy i konserwacja systemów informatycznych

1. Bieżące monitorowanie i aktualizacja systemów informatycznych odbywa się zgodnie z zasadami opisanymi w § 29 oraz § 31.

2. Okresowe przeglądy mające na celu weryfikację stanu zabezpieczeń systemów informatycznych są realizowane zgodnie z ustalonym wewnętrznie w BIŁ 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 „Polityce Bezpieczeństwa Danych Osobowych”.

Rozdział 10

Monitorowanie bezpieczeństwa systemów informatycznych

§ 31. 1. Monitorowanie bezpieczeństwa systemów informatycznych jest realizowane w sposób ciągły przez ASI co najmniej poprzez przegląd 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 DIT.

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 11

Audyty bezpieczeństwa systemów informatycznych

§ 32. 1. Systemy informatyczne GITD muszą przynajmniej raz do roku przechodzić wewnętrzne audyty bezpieczeństwa.

2. Za ustalenie zakresu i harmonogramu audytu odpowiada komórka organizacyjna właściwa do spraw audytu wewnętrznego.

3. Audyt jest przeprowadzany zgodnie z procedurami komórki organizacyjnej właściwej do spraw audytu wewnętrznego.

Rozdział 12

Szkolenia dla pracowników

§ 33. 1. Szkolenia z zakresu bezpieczeństwa i zasad użytkowania systemów informatycznych są organizowane:

1) dla każdego nowego pracownika GITD w terminie ustalanym przez komórkę organizacyjną właściwą do spraw szkoleń;
2) okresowo dla wszystkich pracowników GITD w terminie ustalonym przez komórkę organizacyjną właściwą do spraw szkoleń, nie rzadziej niż raz na trzy lata;
3) dla wszystkich pracowników GITD na wniosek BIŁ w związku z istotnymi zmianami zasad użytkowania systemów informatycznych.

2. W ramach szkoleń przedstawiane są zagadnienia wymienione w rozdziale 2.

Rozdział 13

Reakcja na incydenty

§ 34. 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, wg poniższych wytycznych:

1) KRYTYCZNY – jeżeli przewidywane skutki zdarzenia mogą uniemożliwić działanie procesów biznesowych GITD 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 procesów biznesowych GITD 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 GITD.

3. ASI przyjmujący zgłoszenie dotyczące systemu informatycznego jest odpowiedzialny za:

1) zarejestrowanie zgłoszenia w systemie QDesk;
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 BIŁ.

5. W przypadku potwierdzenia naruszenia bezpieczeństwa informacji przetwarzanych w systemie informatycznym tj. wystąpienia incydentu bezpieczeństwa, ASI ma obowiązek powiadomić DIT w celu ustalenia dalszego sposobu postępowania. Postępowanie to obejmuje:

1) w przypadkach zaklasyfikowanych jako „Poważne” i „Krytyczne”-powiadomienie Dyrektora Generalnego GITD i 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 do Polityki Bezpieczeństwa Systemów Informatycznych

Oświadczenie podmiotu zewnętrznego w związku uzyskaniem zdalnego dostępu do zasobów GITD

.....
imię i nazwisko

.....
nazwa przedsiębiorcy

OŚWIADCZENIE

W związku z zawartą z Głównym Inspektoratem Transportu Drogowego 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) ……. …….
   2) ……. …….
2. wymienione wyżej osoby, które z racji wykonywania obowiązków wynikających z powołanej umowy dokonywać będą zdalnych prac w sieci wewnętrznej Głównego Inspektoratu Transportu Drogowego zostały zapoznane z obowiązującymi w Głównym Inspektoracie Transportu Drogowego zasadami pracy zdalnej I.

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

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

……..……., dnia ....
(miejsce) (data) (pieczęć i podpis)

Załącznik nr 2 do Polityki Bezpieczeństwa Systemów Informatycznych

Rejestr awarii i naruszeń bezpieczeństwa

Rejestr awarii i naruszeń bezpieczeństwa /Przykład/							
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
12.01.2014	10:20	N	stacje robocze LAN	rozprzestrzenianie się wirusa	poważny	usunięcie wirusa, aktualizacja programów antywirusowych	
19.01.2014	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 procesów biznesowych, uzależnionych od usług właściwych dla danego systemu
- **POWAŻNY** – awaria komponentu pomocniczego systemu mogąca mieć wpływ na prawidłową realizację procesów biznesowych
- **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 działanie procesów biznesowych GITD, lub doprowadzić do utraty poufności, dostępności lub integralności danych (w szczególności danych osobowych)

- **POWAŻNY** – jeżeli przewidywane skutki zdarzenia mogą w istotny sposób utrudnić realizację procesów biznesowych GITD 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 GITD