

REGULAMIN UŻYTKOWNIKA

Spis treści:

§ 1. Definicje	2
§ 2. Szkolenia dla użytkowników systemów teleinformatycznych	2
§ 3. Używanie autoryzowanych środków do przetwarzania informacji	3
§ 4. Wnoszenie mienia i korzystanie z urządzeń przenośnych	4
§ 5. Korzystanie z systemów teleinformatycznych Agencji oraz Internetu	5
§ 6. Korzystanie z poczty elektronicznej i innych elektronicznych systemów komunikacyjnych	6
§ 7. Ochrona haseł i kluczy kryptograficznych	7
§ 8. Zgodność oprogramowania z prawami autorskimi	8
§ 9. Korzystanie z urządzeń komunikacji głosowej, faksowej i wizyjnej	9
§ 10. Zasady „czystego biurka i czystego ekranu”	9
§ 11. Zgłaszanie zdarzeń o naruszeniu bezpieczeństwa, niewłaściwym funkcjonowaniu oprogramowania lub słabości systemu teleinformatycznego	10
§ 12. Postępowanie dyscyplinarne w przypadku naruszenia bezpieczeństwa	12

§ 1.

Definicje

Użyte w regulaminie określenia oznaczają:

1. dane uwierzytelniające – informacje wprowadzane do systemu, potwierdzające tożsamość użytkownika (np. hasła dostępu, kody zawarte w sprzętowych tokenach kryptograficznych);
2. hasło - ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie teleinformatycznym;
3. konto – część systemu teleinformatycznego (dane, oprogramowanie, zasoby sieciowe), które są powiązane z identyfikatorem użytkownika;
4. spam – niepożądaną przesyłkę poczty elektronicznej kierowaną do niezdefiniowanego adresata;
5. uwierzytelnianie - działanie, którego celem jest weryfikacja deklarowanej tożsamości osoby/podmiotu;
6. urządzenie przenośne – urządzenie mobilne takie jak laptop, notebook, netbook, palmtop, tablet, telefon komórkowy, smartfon, MDA/PDA, pendrive, odtwarzacz mp3/4, aparat cyfrowy, czytnik kart pamięci, urządzenie do nawigacji GPS itp.

§ 2.

Szkolenia dla użytkowników systemów teleinformatycznych

1. Szkolenia użytkowników systemów teleinformatycznych mają na celu uzyskanie przez nich optymalnego poziomu wiedzy i umiejętności, które pozwolą właściwie użytkować i chronić systemy teleinformatyczne.
2. Warunkiem uzyskania podstawowego dostępu do systemu teleinformatycznego Agencji (konto domenowe i konto pocztowe) przez pracownika jest odbycie szkolenia wstępnego przeprowadzanego przez bezpośredniego przełożonego potwierdzone podpisem pracownika na wniosku o przyznanie dostępu, którego wzór zawarto w Księżce Procedur KP-611-101-ARiMR – „Obsługa kont użytkowników systemów informatycznych ARiMR”.
3. Warunkiem uzyskania dostępu do zaawansowanych funkcjonalności systemów teleinformatycznych Agencji jest odbycie szkoleń i zdanie egzaminów zgodnych z wymaganiami stawianymi przez Właścicieli Zasobów teleinformatycznych.
4. Szkolenia i egzaminy sprawdzające powinny być okresowo powtarzane (częstotliwość takich szkoleń określają Właściciele Zasobów teleinformatycznych) ze szczególnym uwzględnieniem:
 - 1) zmian dokonywanych w systemach teleinformatycznych, mających wpływ na sposób korzystania z tych systemów przez użytkowników,
 - 2) zmian przepisów prawa oraz uregulowań wewnętrznych,
 - 3) wystąpienia przypadków naruszenia bezpieczeństwa, słabości systemu lub zidentyfikowanych błędów systemów teleinformatycznych.
5. Okresowo (nie rzadziej niż raz na rok) przeprowadza się szkolenia doskonalące z zakresu bezpieczeństwa informacji. Szkolenia te obejmują zagadnienia ujęte w niniejszym Regulaminie, a w szczególności dotyczą:

- 1) zapoznania z obowiązującymi regulacjami prawnymi dotyczącymi ochrony informacji, w tym z obowiązującą w Agencji polityką bezpieczeństwa informacji oraz polityką systemu zarządzania bezpieczeństwem informacji,
 - 2) przygotowania użytkowników do właściwego korzystania z powierzonych zasobów (instrukcje użytkowania sprzętu, systemów operacyjnych, aplikacji, itp.),
 - 3) sposobu postępowania w przypadku zdarzenia związanego z naruszeniem bezpieczeństwa informacji,
 - 4) sposobów postępowania w sytuacjach awaryjnych i kryzysowych.
6. Szkolenia doskonalące w zakresie obowiązujących w Agencji regulaminów związanych z bezpieczeństwem informacji mogą być przeprowadzane w zależności od zakresu obowiązków danego użytkownika przez:
- 1) Administratora Systemu,
 - 2) Inspektora Bezpieczeństwa Informacji,
 - 3) Administratora Zabezpieczeń Fizycznych,
 - 4) Właściciela Procesu / Właściciela Zasobu,
 - 5) Bezpośredniego przełożonego.
7. Szkolenia doskonalące powinny kończyć się testem sprawdzającym zrozumienie przekazanych informacji adekwatnym do poziomu i zakresu prowadzonego szkolenia.
8. Uczestnictwo w szkoleniu każdy użytkownik potwierdza podpisem na liście obecności, z wyjątkiem szkoleń, które odbywają się w formie e-learning.
9. Szkolenia i egzaminy związane z użytkowaniem systemów teleinformatycznych są odnotowywane w Systemie e-szkoleń ARiMR.
10. Nieprzystąpienie do szkolenia, o którym mowa w § 2 ust. 5 lub niezaliczenie testu, o którym mowa w § 2 ust. 7, w terminie podstawowym i dodatkowym skutkuje blokadą dostępu do systemu teleinformatycznego Agencji na wniosek dyrektora komórki właściwej ds. bezpieczeństwa informacji.
11. Przywrócenie dostępu do systemu teleinformatycznego następuje na wniosek przełożonego użytkownika, zgodnie z procedurą zawartą w KP-611-101-ARiMR, po wcześniejszym odbyciu dodatkowego szkolenia doskonalącego i pozytywnym zaliczeniu testu.

§ 3.

Używanie autoryzowanych środków do przetwarzania informacji

1. Środki do przetwarzania informacji wykorzystywane w Agencji są przeznaczone wyłącznie do wykonywania zadań służbowych.
2. Każdy środek do przetwarzania informacji podlega inwentaryzacji i autoryzacji (dopuszczenie do pracy w systemie teleinformatycznym Agencji) zgodnie z zasadami określonymi w odrębnych dokumentach Agencji.
3. Wykorzystywanie środków do przetwarzania informacji, będących własnością Agencji, w celach niezwiązanych z powierzonymi obowiązkami wymaga uzgodnienia z bezpośrednim przełożonym i, jeżeli zachodzi taka potrzeba wynikająca z zakresu ewentualnego wykorzystania urządzeń, z Administratorem Systemu.
4. Zabrania się podłączania do sieci teleinformatycznej jakichkolwiek urządzeń nie posiadających autoryzacji.

5. Użytkownicy mogą korzystać ze stacji roboczych wyłącznie na stanowiskach im przydzielonych. Korzystanie z innego stanowiska komputerowego dopuszczalne jest jedynie za zgodą i na polecenie bezpośredniego przełożonego lub w przypadkach opisanych w Planach Zapewnienia Ciągłości Działania Agencji.
6. Użytkownik ponosi odpowiedzialność za powierzony sprzęt i oprogramowanie oraz sposób jego eksploatacji.
7. W przypadku korzystania ze stacji roboczej przez kilku użytkowników, kierownik komórki bądź jednostki organizacyjnej wyznacza osobę odpowiedzialną za sprzęt, określając jednocześnie uprawnienia i obowiązki wszystkich współużytkowników tego sprzętu.
8. Użytkowników obowiązuje zakaz testowania lub podejmowania prób poznania metod zabezpieczenia systemów teleinformatycznych.
9. Użytkownicy nie mogą samodzielnie dokonywać jakiegokolwiek zmiany konfiguracji systemu teleinformatycznego.
10. Nośniki uszkodzone, wycofywane z eksploatacji lub przekazywane do ponownego użycia użytkownik przekazuje Administratorowi Systemu odpowiedzialnemu za przeprowadzenie zniszczenia lub trwałego skasowania danych, korzystając z następujących procedur:
 - 1) programowego kasowania danych na dyskach twardej – zamieszczonej w Księżce Procedur KP-611-204-ARiMR,
 - 2) niszczenia zawartości komputerowych nośników magnetycznych – zamieszczonej w Księżce Procedur KP-611-204-ARiMR,
 - 3) niszczenia nośników optycznych – zamieszczonej w Księżce Procedur KP-611-186-ARiMR.
11. Postanowienia ust. 10 nie ograniczają ani nie wykluczają stosowania obowiązujących w Agencji zasad dotyczących gospodarowania środkami trwałymi oraz wyposażeniem.

§ 4.

Wynoszenie mienia i korzystanie z urządzeń przenośnych

1. Komputery przenośne podlegają szczególnej ochronie polegającej na zabezpieczeniu dostępu do komputera hasłem (hasło na BIOS). Ich używanie poza strefą administracyjną musi mieć uzasadnienie w realizowanych przez użytkownika zadaniach.
2. Wynoszenie sprzętu komputerowego poza Agencję, w tym sposób programowego zabezpieczenia komputerów przenośnych, reguluje procedura wydawania zezwoleń na wyносzenie sprzętu komputerowego z ARiMR zawarta w Księżce Procedur KP-611-206-ARiMR.
3. Na użytkowniku urządzenia przenośnego spoczywa obowiązek jego ochrony, w szczególności zabrania się pozostawiania bez opieki tego typu urządzenia w samochodach, przedziałach wagonów, salach konferencyjnych oraz innych miejscach, gdzie użytkownik nie ma możliwości sprawowania nad nimi skutecznego nadzoru.
4. Wszelkie informacje wrażliwe nie mogą być przechowywane w urządzeniach przenośnych, które pracują poza Agencją, jeśli pozostają w postaci niezasyfrowanej.
5. Każdy użytkownik, któremu powierzono urządzenie przenośne, przed rozpoczęciem użytkowania go poza strefą administracyjną Agencji, obowiązany jest do wystąpienia do Administratora Systemu z wnioskiem o zapewnienie środków techniczno-organizacyjnych

gwarantujących poufność i integralność przetwarzanych informacji. Do środków tych zalicza się zabezpieczenia kryptograficzne określone w Polityce kryptografii oraz ochronę antywirusową.

6. W przypadku utraty powierzonego urządzenia przenośnego używanego poza Agencją użytkownik niezwłocznie powiadamia o tym fakcie Help Desk ARiMR oraz bezpośredniego przełożonego, a w przypadku kradzieży niezwłocznie zgłasza ten fakt na policję. Ponadto o kradzieży informuje osobę wydającą zgodę na wyniesienie sprzętu.

§ 5.

Korzystanie z systemów teleinformatycznych Agencji oraz Internetu

1. Przydzielanie uprawnień do korzystania z systemów teleinformatycznych realizowane jest w oparciu o następujące zasady:
 - 1) „minimalnych przywilejów” – każdy pracownik posiada prawa dostępu do zasobów ograniczone wyłącznie do tych, które są niezbędne do wykonywania powierzonych mu obowiązków,
 - 2) „wiedzy koniecznej” – pracownicy posiadają wiedzę o zasobach ograniczoną wyłącznie do zagadnień, które są niezbędne do realizacji powierzonych im zadań,
 - 3) „domniemanej odmowy” – wszystkie działania, które nie są jawnie dozwolone są zabronione.
2. Każdy użytkownik otrzymuje prawa dostępu wyłącznie w zakresie niezbędnym do realizowania powierzonych zadań na danym stanowisku pracy.
3. Prawa dostępu są przydzielone po nadaniu użytkownikowi identyfikatora i hasła dostępu lub innych danych uwierzytelniających użytkownika.
4. Każdy użytkownik ma w systemie unikalny identyfikator.
5. Przed uzyskaniem dostępu do systemów teleinformatycznych Agencji użytkownik jest informowany przez bezpośredniego przełożonego o zakresie przyznawanych mu uprawnień.
6. Użytkownik ponosi odpowiedzialność za wszelkie czynności wykonane z użyciem jego identyfikatora i hasła.
7. Jeżeli w trakcie korzystania z zasobów systemu teleinformatycznego użytkownik stwierdzi, że posiadane uprawnienia wykraczają poza przyznane, zobowiązany jest niezwłocznie zgłosić ten fakt do Help Desk ARiMR. Nie dokonanie zgłoszenia tego faktu może zostać potraktowane jako celowe i świadome naruszenie praw dostępu.
8. Po stwierdzeniu posiadania większych uprawnień zabronione jest ich testowanie i wykorzystywanie.
9. W przypadku dłuższej nieobecności na stanowisku pracy użytkownik obowiązany jest zakończyć aktywne sesje i wylogować się. Ponadto, użytkownik każdorazowo w przypadku oddalenia się od stacji roboczej obowiązany jest zablokować system.
10. Na użytkownika spoczywa obowiązek zabezpieczenia opracowywanych bądź tworzonych przez siebie danych przed utratą. Również wszelkie dane źródłowe, na których użytkownik wykonuje operacje, winny być zabezpieczone przed utratą i nieautoryzowanym użyciem bądź modyfikacją.
11. Użytkownik ma następujące możliwości zabezpieczenia danych (plików) przed utratą:

- 1) umieszczenie danych na serwerze plików (fileserv) – jest to zalecana forma zabezpieczenia danych,
 - 2) sporządzenie kopii zapasowej na wymiennym nośniku komputerowym,
 - 3) sporządzenie wydruków z wyniku pracy nad przetwarzanymi danymi.
12. Niedopuszczalne jest umieszczanie na serwerze plików danych niezwiązanych z wykonywanymi obowiązkami służbowymi.
13. W przypadku potrzeby zabezpieczenia plików o dużych rozmiarach należy skorzystać z procedury nagrywania danych na nośnikach optycznych zawartej w Księżce Procedur KP-611-186-ARiMR - „Postępowanie z optycznymi nośnikami danych”.
14. Zabronione jest:
- 1) umożliwianie dostępu do systemów teleinformatycznych osobom nieupoważnionym,
 - 2) rejestrowanie się w systemie teleinformatycznym na identyfikatorze innego użytkownika,
 - 3) korzystanie z konta innego użytkownika, chyba że część lub całość zasobów związanych z tym kontem są udostępniane zgodnie z zasadami obowiązującymi w Agencji,
 - 4) przenoszenie informacji uzyskanych w związku z wykonywanymi zadaniami służbowymi na prywatne nośniki informacji, w szczególności pamięci typu pendrive i inne pamięci zewnętrzne,
 - 5) dokonywanie prób sprawdzania, testowania i omijania zabezpieczeń systemów teleinformatycznych wewnętrznych jak również zewnętrznych, nie należących do Agencji,
 - 6) udzielanie informacji o zasadach ochrony systemów teleinformatycznych Agencji, w tym o identyfikatorach używanych w tych systemach,
 - 7) samowolne modyfikowanie ustawień związanych z bezpieczeństwem w systemach teleinformatycznych,
 - 8) świadome niszczenie danych mających znaczenie archiwalne gromadzonych w systemach teleinformatycznych,
 - 9) świadome wprowadzanie błędnych danych do systemów teleinformatycznych,
 - 10) udostępnianie danych osobom nieupoważnionym,
 - 11) włączanie urządzeń elektrycznych do wydzielonej instalacji elektrycznej przeznaczonej dla systemów teleinformatycznych,
 - 12) przeglądanie stron internetowych o treściach pornograficznych, erotycznych, rasistowskich, użytkowanych przez grupy przestępcze i terrorystyczne,
 - 13) pobieranie z Internetu, kopiowanie, instalowanie, przechowywanie lub rozpowszechnianie nieautoryzowanego przez Komitet oprogramowania i danych,
 - 14) korzystanie z list i forów dyskusyjnych, gier internetowych oraz innych usług, nie mających związku z wykonywaną pracą.

§ 6.

Korzystanie z poczty elektronicznej i innych elektronicznych systemów komunikacyjnych

1. Wszyscy pracownicy Agencji mają dostęp do wewnętrznej poczty elektronicznej.

2. Agencyjna poczta służy wyłącznie do celów służbowych. Korespondencja realizowana drogą elektroniczną z wykorzystaniem systemów teleinformatycznych Agencji podlega rejestrowaniu i filtrowaniu, o którym mowa w ust. 3.
3. Użytkownicy są świadomi, że wiadomości elektroniczne niezwiązane z działalnością Agencji, a zawierające słowa bądź temat uznane za niedozwolone, zgodnie z zasadami filtrowania komunikacji niepożądaną obowiązującymi w Agencji, będą zatrzymywane i następnie usuwane z systemu pocztowego.
4. Zalecany formatem przesyłanych wiadomości jest „zwykły tekst”. O ile nie jest to konieczne, nie należy tworzyć wiadomości w formacie HTML.
5. Użytkownicy obowiązani są do okresowego porządkowania i usuwania wiadomości zbędnych z folderów programu pocztowego tak, aby nie dopuścić do jego zablokowania z powodu przekroczenia dopuszczalnej pojemności skrzynki.
6. Zabronione jest:
 - 1) rozsyłanie z komputerów Agencji oraz przyznanym użytkownikom kont poczty wiadomości, których treść nie jest związana z wykonywaną pracą, wyjątek stanowią komunikaty niestandardowe rozsyłane zgodnie z „Zasadami świadczenia przez Departament Informatyki usługi dystrybucji komunikatów do dużych grup odbiorców”,
 - 2) wysyłanie materiałów służbowych na konta prywatne (np. celem pracy nad dokumentami w domu),
 - 3) wykorzystywanie systemu poczty elektronicznej do działań mogących zaszkodzić wizerunkowi Agencji,
 - 4) odbieranie przesyłek z nieznanymi źródłami,
 - 5) otwieranie załączników z plikami samorozpakowującymi się bądź wykonalnymi typu exe, com, itp.,
 - 6) przesyłanie pocztą elektroniczną plików wykonywalnych typu: bat, com, exe, plików multimedialnych oraz plików graficznych,
 - 7) ukrywanie lub dokonywanie zmian tożsamości nadawcy,
 - 8) czytanie, usuwanie, kopiowanie lub zmiana zawartości skrzynek pocztowych innego użytkownika,
 - 9) odpowiadanie na niezamówione wiadomości reklamowe lub wysyłane łańcuszki oraz na inne formy wymiany danych określanymi spamem; w przypadku otrzymania takiej wiadomości należy przesłać ją Administratorowi systemu poczty elektronicznej na adres e-mail: spam@arimr.gov.pl,
 - 10) posługiwanie się adresem służbowym e-mail w celu rejestrowania się na stronach handlowych, informacyjnych, chat'ach lub forach dyskusyjnych, które nie dotyczą zakresu wykonywanej pracy,
 - 11) wykorzystywanie poczty elektronicznej do reklamy prywatnych towarów lub usług, działalności handlowo-usługowej innej niż wynikającej z potrzeb Agencji lub do poszukiwania dodatkowego zatrudnienia.

§ 7.

Ochrona haseł i kluczy kryptograficznych

1. Hasła użytkowników lub inne dane uwierzytelniające podlegają szczególnej ochronie.
2. Użytkownik ponosi pełną odpowiedzialność za utworzenie hasła i jego przechowywanie.
3. Każdy użytkownik posiadający dostęp do systemów teleinformatycznych Agencji zobowiązany jest do:

- 1) zachowania w poufności wszystkich swoich haseł lub innych danych uwierzytelniających wykorzystywanych do pracy w systemie teleinformatycznym Agencji,
 - 2) niezwłocznej zmiany haseł w przypadkach zaistnienia podejrzenia lub rzeczywistego ujawnienia,
 - 3) niezwłocznej zmiany hasła tymczasowego, przekazanego przez Administratora Systemu,
 - 4) poinformowania Administratora Systemu oraz Inspektora Bezpieczeństwa Informacji o podejrzeniu lub rzeczywistym ujawnieniu hasła,
 - 5) stosowania haseł o minimalnej długości 8 znaków, zawierających kombinację małych i dużych liter oraz cyfr lub znaków specjalnych,
 - 6) zmiany wykorzystywanych haseł w regularnych odstępach czasu.
4. Zabronione jest:
- 1) zapisywanie haseł w sposób jawny i umieszczania ich w miejscach dostępnych dla innych osób,
 - 2) stosowanie haseł opartych na skojarzeniach, łatwych do odgadnięcia lub wywnioskowania z informacji dotyczących danej osoby, np. imiona, numery telefonów, daty urodzenia itp.,
 - 3) używanie tych samych haseł w różnych systemach operacyjnych i aplikacjach,
 - 4) udostępnianie haseł innym użytkownikom,
 - 5) przeprowadzanie prób łamania haseł,
 - 6) wpisywanie haseł „na stałe” (np. w skryptach logowania).
5. W zależności od funkcjonujących w Agencji systemów operacyjnych i aplikacji zasady określone w ust. 3 pkt 3, 5 i 6 oraz ust. 4 pkt 2 i 3 mogą być wymuszane ustawieniami systemu teleinformatycznego wprowadzanymi przez Administratora Systemu na podstawie zasad określonych w odrębnych dokumentach Agencji.
6. Każdy użytkownik korzystający z kluczy kryptograficznych jest zobowiązany do ich użytkowania i przechowywania z uwzględnieniem wymagań określonych w Polityce kryptografii, w sposób uniemożliwiający utratę lub dostęp osób niepowołanych.
7. W przypadku podejrzenia lub rzeczywistego naruszenia bezpieczeństwa klucza fakt ten należy niezwłocznie zgłosić Administratorowi Systemu oraz Inspektorowi Bezpieczeństwa Informacji.

§ 8.

Zgodność oprogramowania z prawami autorskimi

1. Użytkownicy nie mogą instalować oraz uruchamiać żadnych aplikacji, które nie zostały wcześniej formalnie dopuszczone do użytkowania.
2. Użytkownikowi nie wolno:
 - 1) uruchamiać jakiegokolwiek innego oprogramowania niż to, które zostało mu przydzielone na danej stacji roboczej,
 - 2) pobierać z sieci, kopiować, przechowywać lub rozprowadzać oprogramowania, utworów muzycznych i wideo oraz innych plików, których używanie może powodować naruszenie praw do własności intelektualnej,
 - 3) kopiować i rozprowadzać bez upoważnienia oprogramowania stworzonego w Agencji lub na potrzeby Agencji,
 - 4) samodzielnie usuwać oprogramowania, którego używa.

3. Każdy plik znajdujący się:
 - 1) na wymiennym nośniku komputerowym,
 - 2) otrzymany za pomocą poczty elektronicznej lub pobrany z Internetu,podlega sprawdzeniu za pomocą oprogramowania antywirusowego zainstalowanego na komputerze przypisanym do użytkownika.
4. W przypadku wykrycia jakichkolwiek plików lub oprogramowania innego niż to, które znajduje się w spisie, Administrator Systemu ma prawo do natychmiastowego ich skasowania bez uzgodnienia z użytkownikiem.
5. O przypadkach używania nieautoryzowanego oprogramowania Administrator Systemu informuje Inspektora Bezpieczeństwa Informacji.
6. Użytkownik ponosi finansowe i prawne konsekwencje posiadania nielegalnego oprogramowania w przypisanym mu komputerze, jeśli nie dopełnił obowiązków wskazanych w niniejszym Regulaminie.

§ 9.

Korzystanie z urządzeń komunikacji głosowej, faksowej i wizyjnej

1. Każdy użytkownik zobowiązany jest do przestrzegania zakazu prowadzenia rozmów, podczas których może dochodzić do wymiany informacji wrażliwych, jeśli rozmowy te odbywają się w miejscach publicznych, otwartych pomieszczeniach biurowych lub takich, które nie gwarantują zachowania poufności rozmów.
2. Odczytanie wiadomości z faksów, automatycznych sekretarek lub systemów poczty głosowej powinno być możliwe wyłącznie po wprowadzeniu indywidualnego hasła. W przypadku braku takiej możliwości urządzenia należy zabezpieczyć przed dostępem osób nieuprawnionych.
3. Zabronione jest wykorzystywanie domyślnych („fabrycznych”) haseł dla ww. urządzeń.
4. Przekazywanie za pomocą urządzeń faksowych dokumentów zawierających informacje wrażliwe jest zabronione.
5. Drukarki nie mogą być pozostawione bez kontroli, jeśli są wykorzystywane (lub wkrótce będą) do drukowania dokumentów zawierających informacje wrażliwe.

§ 10.

Zasady „czystego biurka i czystego ekranu”

1. Palenie, jedzenie oraz picie na stanowiskach komputerowych oraz w pomieszczeniach, w których znajdują się środki przetwarzania informacji (pomieszczenia serwerowni i węzłów teletechnicznych) jest zabronione.
2. W celu ograniczenia ryzyka nieuprawnionego dostępu, utraty lub uszkodzenia informacji w czasie godzin pracy i poza nimi użytkownik jest zobowiązany:
 - 1) przechowywać dokumenty papierowe i wymienne nośniki komputerowe w odpowiednio zabezpieczonych meblach biurowych,
 - 2) nie pozostawiać komputerów bez nadzoru w stanie aktywnej sesji dostępu do sieci,
 - 3) po zakończeniu pracy wylogować się z systemu i wyłączyć komputer, niedopuszczalne jest zakończenie pracy bez wykonania pełnej i poprawnej procedury zamknięcia lub przez wyłączenie napięcia zasilającego,

- 4) po zakończeniu pracy uporządkować swoje stanowisko pracy, uniemożliwiając dostęp osób nieupoważnionych do dokumentów zawierających informacje wrażliwe,
 - 5) przestrzegać zasady niepozostawiania otwartych i niezabezpieczonych drzwi i/lub okien podczas nieobecności w pomieszczeniu,
 - 6) używać wygaszaczy ekranu zabezpieczonych hasłem,
 - 7) zabezpieczać nieużywany w danym momencie komputer przed nieupoważnionym dostępem, włączając blokadę systemową; ponowny dostęp do komputera następuje po podaniu hasła,
 - 8) ustawiać monitory komputerów w taki sposób, żeby uniemożliwić osobom nieupoważnionym wgląd w zawartość ekranu,
 - 9) odpowiednio zabezpieczyć miejsca przyjmowania/wysyłania korespondencji papierowej oraz odbioru/wysyłania faksów,
 - 10) włączać blokadę urządzeń kopiujących, zabezpieczając je w ten sposób przed nieuprawnionym użyciem,
 - 11) zwracać uwagę i powodować usuwanie pozostawionych oryginałów lub kopii w pobliżu urządzeń kserograficznych,
 - 12) zwracać szczególną uwagę na pracujące drukarki pozostawione bez nadzoru,
 - 13) nie pozostawiać wymiennych nośników komputerowych w napędach, bądź ogólnie dostępnych miejscach,
 - 14) niszczyć niepotrzebne nośniki papierowe w niszczarkach, jak np. dokumenty błędnie wydrukowane, powielone kopie itp. (za wyjątkiem nośników zawierających informacje wrażliwe, których sposób niszczenia regulują odrębne przepisy, w tym przepisy kancelaryjno-archiwalne Agencji w zakresie brakowania dokumentacji nie-archiwalnej).
3. W uzasadnionych przypadkach realizacji zadań wymagających nieprzerwanego dostępu do zasobów teleinformatycznych (np. długotrwałe wgrywanie patch'y, pobieranie dużych ilości danych, odbywające się poza godzinami pracy ze względu na przepustowość łącz, wydajność baz danych, itp.) dopuszczalne jest, w porozumieniu z komórką właściwą ds. informatyki, odstępianie od wymogu podanego w ust. 2 pkt 3.

§ 11.

Zgłaszanie zdarzeń o naruszeniu bezpieczeństwa, niewłaściwym funkcjonowaniu oprogramowania lub słabości systemu teleinformatycznego

1. Przed przystąpieniem do pracy użytkownik obowiązany jest sprawdzić stację roboczą (komputer) i stanowisko pracy ze zwróceniem uwagi, czy nie zaszły okoliczności wskazujące na naruszenie lub próbę naruszenia bezpieczeństwa informacji.
2. Do przypadków mogących świadczyć lub świadczących o naruszeniu bezpieczeństwa, niewłaściwym funkcjonowaniu oprogramowania lub słabości systemu teleinformatycznego zalicza się:
 - 1) nieautoryzowany dostęp do danych,
 - 2) naruszenie lub wadliwe funkcjonowanie zabezpieczeń fizycznych w pomieszczeniach (np. wyłamane lub zacinające się zamki, naruszone plomby, nie domykające się bądź wybite okna, itp.),
 - 3) utratę usługi, urządzenia lub funkcjonalności,
 - 4) nieautoryzowaną modyfikację lub zniszczenie danych,
 - 5) udostępnienie informacji wrażliwych osobom nieupoważnionym,
 - 6) pozyskiwanie oprogramowania z nielegalnych źródeł,
 - 7) pojawianie się nietypowych komunikatów na ekranie,

- 8) niemożność zalogowania się do systemu teleinformatycznego,
 - 9) spowolnienie pracy oprogramowania,
 - 10) niestabilna praca systemu teleinformatycznego,
 - 11) brak reakcji systemu na działania użytkownika,
 - 12) ponowny start lub zawieszanie się komputera,
 - 13) ograniczenie funkcjonalności oprogramowania.
3. Za naruszenie zasad ochrony informacji wrażliwych uważa się w szczególności:
- 1) nieupoważniony dostęp, modyfikację, kopiowanie, udostępnienie lub zniszczenie /usunięcie informacji wrażliwych, zarówno w systemie teleinformatycznym, jak i na nośnikach papierowych i elektronicznych,
 - 2) udostępnianie informacji wrażliwych nieuprawnionym podmiotom,
 - 3) nieautoryzowany dostęp do danych przez połączenie sieciowe,
 - 4) niedopełnienie obowiązku ochrony informacji wrażliwych przez umożliwienie dostępu do danych (np. pozostawienie kopii danych, nie zablokowanie dostępu do systemu, brak nadzoru nad serwisantami i innymi osobami nieuprawnionymi przebywającymi w pomieszczeniach, gdzie przetwarza się informacje wrażliwe),
 - 5) stworzenie niezabezpieczonego kanału dystrybucji informacji wrażliwych,
 - 6) nielegalne bądź nieświadome ujawnienie informacji wrażliwych,
 - 7) pozyskiwanie informacji wrażliwych z nielegalnych źródeł,
 - 8) przetwarzanie informacji wrażliwych niezgodne z uprawnionym celem i zakresem,
 - 9) niepodjęcie działań zmierzających do eliminacji wirusów komputerowych lub innych programów zagrażających integralności systemu teleinformatycznego,
 - 10) ujawnienie indywidualnych haseł dostępu do informacji wrażliwych w systemie,
 - 11) przesyłanie informacji wrażliwych przez Internet bez zabezpieczenia,
 - 12) przesyłanie dokumentów papierowych i nośników elektronicznych z informacjami wrażliwymi bez zabezpieczenia,
 - 13) wykonanie nieuprawnionych kopii informacji wrażliwych,
 - 14) kradzież nośników zawierających informacje wrażliwe lub oprogramowanie,
 - 15) kradzież sprzętu służącego do przetwarzania informacji wrażliwych,
 - 16) spowodowanie utraty informacji wrażliwych w systemie teleinformatycznym, na kopiach bezpieczeństwa i na innych nośnikach,
 - 17) dopuszczenie do braku aktualnych kopii bezpieczeństwa informacji wrażliwych lub brak odpowiednich nośników do sporządzania kopii,
 - 18) niewłaściwe niszczenie nośników z informacjami wrażliwymi pozwalające na ich odczyt,
 - 19) naruszenie zasad ochrony fizycznej pomieszczeń, w których przetwarza się informacje wrażliwe,
 - 20) dopuszczenie do przetwarzania informacji wrażliwych pracowników bez odpowiednich upoważnień,
 - 21) nie przeszkolenie pracowników w zakresie zasad bezpieczeństwa informacji wrażliwych,
 - 22) inne sytuacje wskazujące lub potwierdzające naruszenie bezpieczeństwa informacji wrażliwych w Agencji.
4. Wszelkie działania użytkownika związane z samodzielnym naprawianiem, potwierdzeniem lub testowaniem potencjalnych słabości systemu są zabronione.
5. Dokonywanie zmian w miejscu naruszenia ochrony bez wiedzy i zgody Administratora Systemu lub Inspektora Bezpieczeństwa Informacji lub Administratora Zabezpieczeń Fizycznych (w zależności od rodzaju naruszenia), jest dopuszczalne jedynie w sytuacji, gdy

zachodzi konieczność ratowania życia lub zdrowia osób oraz mienia w przypadku ich bezpośredniego zagrożenia.

6. W przypadku zauważenia zdarzenia mogącego świadczyć lub świadczącego o naruszeniu bezpieczeństwa, niewłaściwym funkcjonowaniu oprogramowania, błędów lub awarii systemu użytkownik:
 - 1) zabezpiecza dostęp do miejsca lub urządzenia w sposób umożliwiający odtworzenie okoliczności naruszenia bezpieczeństwa lub niewłaściwego funkcjonowania oprogramowania,
 - 2) wstrzymuje pracę na stacji roboczej i odseparowuje komputer od sieci,
 - 3) niezwłocznie informuje Help Desk ARiMR (w przypadku wystąpienia zdarzenia związanego z systemem teleinformatycznym) lub Administratora Zabezpieczeń Fizycznych (jeżeli zdarzenie dotyczy bezpieczeństwa fizycznego i środowiskowego), a także bezpośredniego przełożonego,
 - 4) niezależnie od zapisów pkt 3) niezwłocznie informuje Inspektora Ochrony Danych oraz Inspektora Bezpieczeństwa Informacji w przypadku naruszenia zasad ochrony danych osobowych przy czym sposób poinformowania Inspektora Ochrony Danych powinien nastąpić w sposób zapewniających, iż informacja zostanie odebrana w możliwie najkrótszym czasie od jej przekazania,
 - 5) w przypadku zakwalifikowania przez IBI danego zdarzenia jako incydent, wypełnia w porozumieniu z nim część A raportu o incydencie bezpieczeństwa informacji (wzór raportu określa załącznik nr 3 do Regulaminu zarządzania incydentami).

§ 12.

Postępowanie dyscyplinarne w przypadku naruszenia bezpieczeństwa

1. Nieprzestrzeganie zasad określonych w dokumentach określających politykę bezpieczeństwa informacji stosowanych na danym stanowisku pracy przez użytkownika stanowi naruszenie podstawowych obowiązków pracowniczych i podlega odpowiedzialności dyscyplinarnej określonej w Regulaminie pracy.
2. Każdy przypadek wskazany w ust. 1 jest analizowany przez Inspektora Bezpieczeństwa Informacji, który w porozumieniu z Administratorem Systemu, Administratorem Zabezpieczeń Fizycznych oraz bezpośrednim przełożonym użytkownika, dokonuje kwalifikacji naruszenia. W szczególności umyślne działanie może zostać zakwalifikowane jako ciężkie naruszenie obowiązków pracowniczych.
3. Każdy przypadek naruszenia bezpieczeństwa informacji zgłaszany jest niezwłocznie dyrektorowi komórki właściwej ds. bezpieczeństwa informacji i opisywany zgodnie z Regulaminem zarządzania incydentami.