ZARZĄDZENIE nr 73/2024

Dyrektora Gminnego Ośrodka Pomocy Społecznej Gminy Michałowice

z dnia 23 grudnia 2024 r.

w sprawie zmiany zarządzenia nr 021.13.2018 Kierownika Gminnego Ośrodka Pomocy Społecznej Gminy Michałowice z dnia 1 czerwca 2018 r. w sprawie wprowadzenia Polityki ochrony danych osobowych

Na podstawie § 7 ust. 3 Regulaminu organizacyjnego Gminnego Ośrodka Pomocy Społecznej Gminy Michałowice, wprowadzonego do stosowania zarządzeniem nr 20/2024 Dyrektora Gminnego Ośrodka Pomocy Społecznej Gminy Michałowice z dnia 13 maja 2024 r., wraz ze zm., w związku z art. 24 Rozporządzenia Parlamentu europejskiego i Rady UE 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) zarządzam, co następuje:

§ 1

Wprowadzam nowe brzmienie załącznika nr 11 do Polityki ochrony danych osobowych w brzmieniu określonym w załączniku do zarządzenia.

§ 2

Zarządzenie wchodzi w życie z dniem podpisania.

Załącznik do zarządzenia nr 73/2024
Z dnia 23. 12.2024

Załącznik nr 11 do Polityki ochrony danych osobowych

ZASADY UŻYTKOWANIA ZASOBÓW KOMPUTEROWYCH

I SIECI KOMUNIKACYJNYCH

Spis treści

WSTĘP

W oparciu o aktualnie obowiązujące przepisy prawa z zakresu przetwarzania i ochrony danych osobowych wprowadza się zestaw reguł i praktycznych doświadczeń regulujących sposób zarządzania, ochrony i dystrybucji informacji wrażliwej pozwalający na zapewnienie ochrony danych osobowych.

Niniejsze zasady stanowią wyciąg najistotniejszych zapisów zawartych w Polityce Bezpieczeństwa Danych Osobowych wdrożonej do stosowania u Administratora danych (ADO). Obowiązują pracowników etatowych oraz współpracowników (użytkowników), mających upoważnienia do przetwarzania danych osobowych. Osobą nadzorującą stosowanie się do niniejszych zasad jest Administrator systemu informatycznego (ASI).

Zasady bezpiecznego użytkowania sprzętu IT

1. Za sprzęt IT uznaje się: komputery stacjonarne, komputery przenośne, tablety, telefony komórkowe i smartfony, zasilacze, telefony stacjonarne, drukarki, skanery, monitory, klawiatury, myszki komputerowe, projektory, napędy zewnętrzne np. pendrive, zasilacze awaryjne, routery, przełączniki sieciowe, faks, głośniki komputerowe, słuchawki, mikrofony komputerowe oraz niezbędne okablowanie.

2. Użytkownik zobowiązany jest korzystać ze sprzętu IT w sposób zgodny z jego przeznaczeniem i chronić go przed jakimkolwiek zniszczeniem lub uszkodzeniem.

3. Użytkownik zobowiązany jest do zabezpieczenia sprzętu IT przed dostępem osób nieupoważnionych, a w szczególności zawartości ekranów monitorów.

4. Użytkownik ma obowiązek natychmiast zgłosić uszkodzenie, zagubienie, utratę lub zniszczenie powierzonego mu sprzętu IT.

5. Użytkownik zobowiązany jest zgłosić zagrażające bezpieczeństwu użytkownika funkcjonowanie sprzętu IT (np. uszkodzony przewód zasilania, przegrzewający się sprzęt).

6. Samowolne otwieranie (demontaż) sprzętu IT, instalowanie dodatkowych urządzeń (np. twardych dysków, pamięci) lub podłączanie jakichkolwiek niezatwierdzonych urządzeń do systemu informatycznego jest zabronione.

7. Za bezpieczne użytkowanie urządzeń przenośnych typu laptop, projektor lub pendrive, szczególnie w trakcie transportu, o ile użytkownik otrzymał zgodę na ich wynoszenie poza obszar przetwarzania danych, odpowiada użytkownik.

8. Wszelkie narzędzia pracy przekazane przez pracodawcę, czyli zarówno komputer, jak i dostęp do Internetu są własnością pracodawcy i powinny być wykorzystywane zgodnie z jego wymaganiami.

9. Wykorzystywanie prywatnego sprzętu komputerowego do wykonywania zadań służbowych może mieć miejsce za zgodą pracodawcy. Warunki wykorzystywania prywatnych urządzeń oraz zasady bezpieczeństwa danych określa umowa pomiędzy pracodawcą a pracownikiem regulująca zasady korzystania ze sprzętu i aplikacji.

Zasady korzystania z oprogramowania

1. Użytkownik zobowiązuje się do korzystania wyłącznie z oprogramowania objętego prawami autorskimi.
2. Użytkownik nie ma prawa kopiować oprogramowania zainstalowanego na sprzęcie IT przez Pracodawcę - na swoje własne potrzeby ani na potrzeby osób trzecich.
3. Instalowanie jakiegokolwiek oprogramowania na sprzęcie IT może być dokonane wyłącznie przez osobę upoważnioną.
4. Użytkownicy nie mają prawa do instalowania ani używania oprogramowania innego, niż przekazane lub udostępnione im przez Pracodawcę. Zakaz dotyczy między innymi instalacji oprogramowania z zakupionych płyt CD, programów ściąganych ze stron internetowych, a także odpowiadania na samoczynnie pojawiające się reklamy internetowe.
5. Użytkownicy nie mają prawa do zmiany parametrów systemu, które mogą być zmienione tylko przez osobę upoważnioną.
6. W przypadku naruszenia któregokolwiek z powyższych postanowień Pracodawca ma prawo niezwłocznie i bez uprzedzenia usunąć nielegalne lub niewłaściwie zainstalowane oprogramowanie.

Zasady korzystania z Internetu

1. Użytkownicy mają prawo korzystać z Internetu w celu wykonywania obowiązków służbowych.
2. Przy korzystaniu z Internetu, użytkownicy mają obowiązek przestrzegać prawa własności przemysłowej i praw autorskich.
3. Użytkownicy mają prawo korzystać z Internetu dla celów prywatnych wyłącznie okazjonalnie i ograniczone do niezbędnego minimum tylko przez wskazaną przez dział IT przeglądarkę internetową.
4. Korzystanie z Internetu dla celów prywatnych nie może wpływać na jakość i ilość świadczonej przez Użytkownika pracy oraz na prawidłowe i rzetelne wykonywanie przez niego obowiązków służbowych, a także na wydajność systemu informatycznego Pracodawcy.
5. Użytkownicy nie mają prawa korzystać z Internetu w celu przeglądania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec obowiązujących zasad postępowania, a także grać w gry komputerowe w Internecie lub w systemie informatycznym Pracodawcy, ściągać z Internetu jakichkolwiek plików muzycznych lub wideo.

6. W zakresie dozwolonym przepisami prawa, Pracodawca zastrzega sobie prawo kontrolowania sposobu korzystania przez Użytkownika z Internetu pod kątem wyżej opisanych zasad. Ponadto, w uzasadnionym zakresie, Pracodawca zastrzega sobie prawo kontroli czasu spędzanego przez Użytkownika w Internecie. Pracodawca może również blokować dostęp do niektórych treści dostępnych przez Internet.

Zasady korzystania z poczty elektronicznej

1. System Poczty Elektronicznej jest przeznaczony wyłącznie do wykonywania obowiązków służbowych
2. Przy korzystaniu z Systemu Poczty Elektronicznej, Użytkownicy mają obowiązek przestrzegać prawa własności przemysłowej i prawa autorskiego
3. Użytkownicy mają prawo korzystać z Systemu Poczty Elektronicznej dla celów prywatnych wyłącznie okazjonalnie i powinno być to ograniczone do niezbędnego minimum poprzez przeglądarkę internetową.
4. Korzystanie z Systemu Poczty Elektronicznej dla celów prywatnych nie może wpływać na jakość i ilość świadczonej przez Użytkownika pracy oraz na prawidłowe i rzetelne wykonywanie przez niego obowiązków służbowych, a także na wydajność Systemu Poczty Elektronicznej.
5. Użytkownik jest świadomy, że wszelkie wiadomości o charakterze prywatnym utworzone lub odebrane za pośrednictwem Systemu Poczty Elektronicznej Pracodawcy przetwarzane są wyłącznie na jego własną odpowiedzialność. Użytkownik jest świadom możliwości prowadzenia kontroli tych wiadomości przez Pracodawcę. Pracodawca nie będzie w tej sytuacji odpowiadać za przypadkowe naruszenie dóbr osobistych Użytkownika w postaci naruszenia tajemnicy korespondencji.
6. Użytkownicy nie mają prawa korzystać z Systemu Poczty Elektronicznej w celu przeglądania lub rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec powszechnie obowiązujących zasad postępowania
7. Użytkownik nie ma prawa wysyłać wiadomości zawierających informacje poufne w rozumieniu tajemnicy przedsiębiorstwa, jego pracowników, klientów, dostawców lub kontrahentów za pośrednictwem Internetu, w tym przy użyciu prywatnej elektronicznej skrzynki pocztowej.
8. Zakazuje się uczestnictwa w tzw. „łańcuszkach szczęścia”.
9. Użytkownicy nie powinni otwierać przesyłek od nieznanych sobie osób, których tytuł nie sugeruje związku z wypełnianymi przez nich obowiązkami służbowymi.
10. Użytkownicy nie powinni uruchamiać wykonywalnych załączników dołączonych do wiadomości przesyłanych pocztą elektroniczną.

11. Użycie systemów teleinformatycznych i zasobów systemowych Pracodawcy dla własnych celów komercyjnych jest zakazane.
12. Zakazane jest wygłaszanie prywatnych opinii, jako oficjalnego stanowiska Pracodawcy.
13. W przypadku przesyłania plików danych osobowych do podmiotów zewnętrznych, Użytkownik zobowiązany jest do ich spakowania i opatrzenia hasłem (8 znaków: wielkie i małe litery i cyfry lub znaki specjalne). Hasło należy przesłać odrębnym mailem, sms-em lub przekazać w innej bezpiecznej formie.
14. Cała korespondencja wpływająca na służbową skrzynkę jest korespondencją służbową.
15. Użytkownik odpowiadając lub przekazując wiadomość do innych osób zobowiązany jest zabezpieczyć dane osobowe zawarte w przekazywanej wiadomości (np. listy e-mail)
16. Użytkownik wysyłając wiadomości do wielu odbiorów powinien korzystać z pola UDW – ukryte do wiadomości.

Ochrona antywirusowa

1. Użytkownicy zobowiązani są do skanowania plików wprowadzanych z zewnętrznych nośników programem antywirusowym,
2. Zakazane jest wyłączanie systemu antywirusowego podczas pracy systemu informatycznego przetwarzającego dane osobowe,
3. W przypadku stwierdzenia zainfekowania systemu, użytkownik obowiązany jest poinformować niezwłocznie o tym fakcie Informatyka lub osobę upoważnioną.
4. W przypadku stwierdzenia braku ochrony antywirusowej na komputerze stacjonarnym lub przenośnym, użytkownik obowiązany jest poinformować niezwłocznie o tym fakcie Informatyka lub osobę upoważnioną.

Nadawanie upoważnień i uprawnień do przetwarzania danych osobowych

1. Konto użytkownika w systemie IT i odpowiedni poziom uprawnień zakłada Administrator systemu informatycznego (ASI)
2. ASI jest niezwłocznie informowany o zatrudnieniu nowego pracownika lub współpracownika jak i o zakończeniu stosunku pracy lub umowy zlecenia.
3. Każdy użytkownik systemu przed nadaniem upoważnienia musi:

3.1. zapoznać się z niniejszym regulaminem;

3.2. odbyć szkolenie z zasad ochrony danych osobowych (np.: karta szkolenia odo);

3.3. podpisać Oświadczenie o poufności.

4. Upoważnienie nadawane jest do zbiorów w wersji papierowej i elektronicznej.

5. W przypadku, gdy upoważnienie udzielane jest do zbioru w wersji elektronicznej, nadawany jest użytkownikowi identyfikator w systemie.

6. W przypadku anulowania upoważnienia, identyfikator użytkownika jest blokowany w systemie.

7. Szczegółowa procedura nadawania i blokowania uprawnień w systemie opisana jest w załączniku do Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych.

Polityka haseł

1. Ustala się następujące zasady tworzenia haseł dostępu:
   1) Zaleca się używanie długich haseł, 16 znakowych lub dłuższych, minimalna długość hasła wynosi 12 znaków;
   2) Złożoność haseł uzyskuje się stosując „zasadę pełnych zdań" omówioną w części II procedury (lub stosując hasła wygenerowane losowo) oraz dodatkowo aby wykluczyć stosowanie haseł trywialnych, hasła:
      a. nie mogą być identyczne z identyfikatorem użytkownika, ani kombinacją jego imienia lub nazwiska, nie mogą zawierać części tych kombinacji dłuższej niż dwa kolejne znaki,
      b. Musza być wykluczone z listy haseł zakazanych[1] , tj. listy haseł które wyciekły, listy haseł trywialnych, listy haseł niezgodnych z niniejszą polityką itp. a w przypadku braku możliwości technicznych implementacji takiej listy muszą zawierać znaki z trzech spośród następujących czterech kategorii:
         - wielkie litery alfabetu łacińskiego (od A do Z),
         - małe litery alfabetu łacińskiego (od a do z),
         - cyfry systemu dziesiętnego (od 0 do 9),
         - znaki niealfabetyczne (na przykład !, $, #, %).
   3) Zaprzestaje się wymuszania okresowej zmiany hasła, hasło zmieniane jest jeśli:
      a. systemy wykryły jego obecność na listach haseł trywialnych,

[1] Listę haseł publikuje np. CERT Polska: https://cert.pl/uploads/2022/01/hasla/resources/wordlist_pl.zip za stroną cert.pl Rekomendacje techniczne CERT Polska dla systemów uwierzytelniania https://cert.pl/posts/2022/01/rekomendacje-techniczne-systemow-uwierzytelniania/

b. systemy wykryły jego obecność w publicznie dostępnych słownikach haseł,
c. zachodzi podejrzenie, że aktualne hasło zostało przejęte,
d. przypadku podejrzenia jego odkrycia przez osobę nieupoważnioną,
e. na polecenie przełożonego nadzorującego pracę użytkownika;

2. Bezwzględnie zabrania się udostępniania swojego identyfikatora i hasła innym osobom, w tym współpracownikom mającym wgląd do prowadzonych przez użytkownika spraw i realizowanych zadań;
3. Po otrzymaniu pierwszego hasła, użytkownik zobowiązany jest niezwłocznie zalogować się do systemu i zmienić przydzielone hasło zgodnie z zasadami określonymi w pkt. 1 podpunkt 1) i 2);
4. Hasła nie mogą być nigdzie zapisywane (wyjątek stanowią menadżery haseł o których mowa w pkt.5), z wyjątkiem zarchiwizowanych haseł umożliwiających administracyjny dostęp (tj. zapewniających pełne uprawnienia do zarządzania systemem).
5. Dopuszcza się do stosowania i zapisywania haseł - menadżery haseł:
   1) wbudowane w wymienione przeglądarki internetowe posiadające zainstalowane najnowsze aktualizacje oraz będące zabezpieczone głównym hasłem dostępowym godnie z zasadami określonymi w pkt. 1: Google Chrome, Microsoft Edge, Firefox
   2) w postaci zewnętrznych programów i innych rozwiązań, zatwierdzone przez Informatyka i co do wersji i konfiguracji.
6. W przypadku aplikacji instalowanych na stacjach roboczych stosuje się uwierzytelnianie domenowe (użytkownik podaje tylko raz hasło przy logowaniu do komputera), w przypadku oprogramowania które nie obsługuje logowania domenowego, hasło użyte do dostępu do programu musi być inne niż hasło logowania do komputera.

Procedura rozpoczęcia, zawieszenia i zakończenia pracy

1. Użytkownik rozpoczyna pracę z systemem informatycznym przetwarzającym dane osobowe z użyciem identyfikatora i hasła.

2. Użytkownik jest zobowiązany do uniemożliwienia osobom niepowołanym (np. klientom, innym pracownikom) wglądu do danych wyświetlanych na monitorach komputerowych – tzw. Polityka czystego ekranu.

3. Przed czasowym opuszczeniem stanowiska pracy, użytkownik zobowiązany jest wywołać blokowany hasłem wygaszacz ekranu lub wylogować się z systemu (np.:  + L).

4. Po zakończeniu pracy, użytkownik zobowiązany jest:

   4.1. wylogować się z systemu informatycznego, a następnie wyłączyć sprzęt komputerowy,

   4.2. zabezpieczyć stanowisko pracy, w szczególności wszelką dokumentację oraz nośniki magnetyczne i optyczne, na których znajdują się dane osobowe.

Postępowanie z elektronicznymi nośnikami zawierającymi dane osobowe

1. Elektroniczne nośniki, to: np. wymienne twarde dyski, pen-drive, płyty CD, DVD, pamięci typu Flash.

2. Użytkownicy nie mogą wynosić na zewnątrz firmy wymiennych elektronicznych nośników informacji z zapisanymi danymi osobowymi bez zgody Administratora danych.

3. Dane osobowe wynoszone poza firmę muszą być chronione, np.: zaszyfrowane.

4. W przypadku uszkodzenia lub zużycia nośnika zawierającego dane osobowe należy fizycznie zniszczyć nośnik np. przez rozdrobnienie.

5. Przekazywanie nośników z danymi osobowymi powinno być przeprowadzane z uwzględnieniem zasad bezpieczeństwa. Adresat powinien zostać powiadomiony o przesyłce, zaś nadawca powinien sporządzić kopię przesyłanych danych. Adresat powinien powiadomić nadawcę o otrzymaniu przesyłki. Jeżeli nadawca nie otrzymał potwierdzenia, zaś adresat twierdzi, że nie otrzymał przesyłki, użytkownik będący nadawcą powinien poinformować o zaistniałej sytuacji ADO.

Postępowanie z danymi osobowymi w wersji papierowej

1. Za bezpieczeństwo dokumentów i wydruków zawierających dane osobowe odpowiedzialne są osoby upoważnione (użytkownicy).

2. Dokumenty i wydruki zawierające dane osobowe przechowuje się w pomieszczeniach zabezpieczonych fizycznie przed dostępem osób nieupoważnionych.

3. Pomieszczenia w których są przetwarzane dane osobowe muszą być zamykane na klucz. Dostęp do kluczy posiadają tylko upoważnieni pracownicy.

4. Dostęp do pomieszczeń możliwy jest tylko i wyłącznie w godzinach pracy. W wypadku gdy jest wymagany poza godzinami pracy – możliwy jest tylko na podstawie zezwolenia ADO.

5. Dostęp do pomieszczeń w których są przetwarzane dane osobowe mogą mieć tylko upoważnieni pracownicy.

6. W przypadku pomieszczeń do których dostęp mają również osoby nieupoważnione, mogą przebywać w tych pomieszczeniach tylko w obecności osób upoważnionych i tylko w czasie wymaganym na wykonanie niezbędnych czynności.

7. Użytkownicy są zobowiązani do stosowania „polityki czystego biurka". Polega ona na zabezpieczaniu dokumentów np. w szafach, biurkach, pomieszczeniach przed kradzieżą lub wglądem osób nieupoważnionych.

8. Użytkownicy zobowiązani są do przewożenia dokumentów w sposób zapobiegający ich kradzieży, zagubieniu lub utracie.

9. Użytkownicy zobowiązani są do niszczenia dokumentów i tymczasowych wydruków w niszczarkach niezwłocznie po ustaniu celu ich przetwarzania.

Zapewnienie poufności danych osobowych

1. Użytkownik zobowiązany jest do zachowania w tajemnicy danych osobowych, do których ma lub będzie miał/a dostęp w związku z wykonywaniem zadań służbowych lub obowiązków pracowniczych lub zadań zleconych przez Pracodawcę.

2. Użytkownik zobowiązany jest do niewykorzystywania danych osobowych w celach pozasłużbowych bądź niezgodnych ze zleceniem, o ile nie są one jawne.

3. Użytkownik zobowiązany jest do zachowania w tajemnicy sposobów zabezpieczenia danych osobowych, o ile nie są one jawne.

4. Zabrania się przekazywania bezpośrednio lub przez telefon danych osobowych osobom nieupoważnionym.

Skrócona instrukcja postępowania w przypadku naruszenia ochrony danych osobowych

1. Użytkownik zobowiązany jest do powiadomienia ADO w przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych.

2. Typowe sytuacje, które użytkownik powinien zgłosić:

   2.1. ślady na drzwiach, oknach i szafach wskazują na próbę włamania;

   2.2. dokumentacja jest niszczona bez użycia niszczarki;

   2.3. fizyczna obecność w budynku lub pomieszczeniach osób zachowujących się podejrzanie;

2.4. otwarte drzwi do pomieszczeń, szaf, gdzie przechowywane są dane osobowe;

2.5. ustawienie monitorów pozwala na wgląd osób postronnych na dane osobowe;

2.6. wynoszenie danych osobowych w wersji papierowej i elektronicznej na zewnątrz firmy bez upoważnienia;

2.7. udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej i ustnej;

2.8. telefoniczne próby wyłudzenia danych osobowych;

2.9. kradzież komputerów lub CD, twardych dysków, Pen-drive z danymi osobowymi;

2.10. maile zachęcające do ujawnienia identyfikatora i/lub hasła, zawierające podejrzane załączniki lub linki;

2.11. pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów;

2.12. hasła do systemów przechowywane są w pobliżu komputera.

Prawo Własności Intelektualnej

1. Całkowity udział Pracownika w jakiejkolwiek formie Prawa Własności Intelektualnej (zdefiniowanego poniżej) staje się, w stosunkach pomiędzy Pracownikiem a Pracodawcą, własnością Pracodawcy, który jest jej pełnym właścicielem, a Pracownikowi nie przysługuje jakakolwiek zapłata z tego tytułu.

2. Pracownik, na żądanie i na koszt Pracodawcy, sporządzi dokumenty oraz wykona wszelkie czynności, które mogą okazać się niezbędne w celu uzyskania przez Pracodawcę ochrony jakiegokolwiek Prawa Własności Intelektualnej, oraz wykorzystania przez Pracodawcę jakiegokolwiek Prawa Własności Intelektualnej.

3. W niniejszym regulaminie "Prawo Własności Intelektualnej" oznacza jakikolwiek wzór, proces, wynalazek, ulepszenie, model, znak handlowy, znak usługowy, firmę, prawa do projektu, patent, know-how, tajemnicę handlową, prawo autorskie oraz wszelkie inne prawa własności intelektualnej jakiejkolwiek natury (zastrzeżone czy też nie, włączając w to zastosowania oraz prawa do stosowania wszelkich elementów wymienionych powyżej) wynalezione, rozwinięte, stworzone lub nabyte przez Pracownika w trakcie trwania stosunku pracy Pracownika, włączając w to, bez ograniczeń, wszelkie prawa do jakiegokolwiek oprogramowania, sprzętu, materiałów pisemnych lub innych elementów stworzonych, zaprojektowanych, rozwiniętych lub napisanych przez Pracownika w trakcie stosunku pracy Pracownika.

Konsekwencje w przypadku naruszenia niniejszych zasad

1. Przypadki, nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także, gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, można wszcząć postępowanie dyscyplinarne.

2. Kara dyscyplinarna, orzeczona wobec osoby uchylającej się od powiadomienia nie wyklucza odpowiedzialności karnej tej osoby zgodnie z obowiązującymi przepisami o ochronie danych osobowych oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.

3. ASI ma prawo do monitorowania systemów, sieci i zasobów komputerowych, tak by zapewnić poprawne funkcjonowanie tych systemów i śledzić ewentualne nieprawidłowości. Informacja o zakresie i celu kontroli zostanie przekazana przed rozpoczęciem działań kontrolnych

4. ASI ma prawo do ograniczenia/zabrania dostępu do systemów, sieci i zasobów komputerowych w przypadku uzasadnionych podejrzeń naruszenia warunków niniejszego regulaminu.

5. ASI jest zobowiązany do raportowania każdego naruszenia niniejszego dokumentu, włączając w to warunki zawarte w dokumentach wymienionych wyżej do ADO i/lub organów ścigania, co może prowadzić do wdrożenia postępowania dyscyplinarnego i/lub prawnego i w rezultacie do zawieszenia w prawach dostępu do systemów, sieci i zasobów komputerowych, rozwiązania umowy o pracę i/lub postępowania sądowego.