Polityka Bezpieczeństwa Danych Osobowych w Środowisku IT

dla

Centrum Usług Społecznych w Opolu Lubelskim

DYREKTOR
Centrum Usług Społecznych
w Opolu Lubelskim
dr n. med. Ewelina Szkutnicka

Spis treści

Wstęp

Niniejszy dokument opisuje reguły dotyczące bezpieczeństwa systemów informatycznych, w szczególności przetwarzanych przez te systemy danych osobowych.

Cel

Celem niniejszego dokumentu jest opisanie zasad stosowanych w Centrum Usług Społecznych w Opolu Lubelskim, których zadaniem jest zapewnienie odpowiedniego bezpieczeństwa systemów informatycznych i danych w nich przetwarzanych.

Odpowiedzialności

1. Każdy użytkownik systemów w Centrum Usług Społecznych w Opolu Lubelskim jest odpowiedzialny za przestrzeganie zasad omówionych w niniejszym dokumencie.
2. Administrator systemów jest odpowiedzialny za zapewnienie odpowiedniego poziomu bezpieczeństwa systemów, konfiguracji zgodnej z wytycznymi zapisanymi w niniejszej instrukcji i rozporządzeniem Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych oraz ciągłości i poprawności działania systemów którymi zarządza.
3. IOD jest odpowiedzialny za nadzór nad przestrzeganiem zasad bezpieczeństwa systemów informatycznych i danych które są w nich przetwarzane.

Zasady użytkowania sprzętu komputerowego

1. Sprzęt komputerowy używany w Centrum Usług Społecznych w Opolu Lubelskim może być wykorzystywany tylko w celach służbowych.
2. Zabronione jest przetrzymywanie, kopiowanie, ściganie z zasobów internetowych plików w formacie mp3, divx, vawe lub innych, które naruszają Ustawę o prawie autorskim i prawach pokrewnych (Dz. U. Z 2018 poz. 1191 ze zm.) bądź inne ustawy.

Hasła w systemach informatycznych

1. Każda osoba korzystająca z systemów informatycznych w Centrum Usług Społecznych w Opolu Lubelskim musi mieć nadany swój niepowtarzalny w systemie identyfikator

oraz hasło.

2. Konto w systemie musi być przypisane jednoznacznie tylko do osoby, która z konta korzysta.
3. Dostęp dla danego użytkownika do systemów informatycznych jest możliwy wyłącznie po wprowadzeniu swojego identyfikatora i dokonaniu uwierzytelnienia w systemie.
4. Hasła dostępu użytkownika do systemów są chronione i znane wyłącznie temu użytkownikowi, w związku z tym nie mogą być ujawnione innym użytkownikom.
5. Hasła, które jednak zostały ujawnione muszą zostać niezwłocznie zmienione na nowe.
6. Przekazanie hasła przez Administratora użytkownikowi musi się odbywać w sposób bezpieczny, to znaczy uniemożliwiający poznanie tego hasła osobom postronnym.
7. Hasło przekazane przez Administratora dla nowego użytkownika, musi zostać zmienione przy pierwszym logowaniu do systemu.
8. Hasło do systemów musi spełniać następujące minimalne warunki:
   1) system musi wymusić zmianę hasła co 30 dni;
   2) hasło nie może być krótsze niż 8 znaków;
   3) hasło powinno zawierać:
      - co najmniej jedną cyfrę i jeden znak specjalny;
      - składać się z wielkich i małych liter;
   4) hasło - w miarę możliwości - nie może się powtórzyć co najmniej przez 3 razy;
   5) hasło do systemów musi być wprowadzane w sposób niewidoczny;
   6) hasło z komputera do systemów musi być przekazywane w sposób zaszyfrowany.

Zasada „czystego biurka"

1. Zgodnie z ww. zasadą niedopuszczalne jest pozostawienie informacji zawierających dane osobowe w miejscu ogólnie dostępnym.
2. Zakazane jest zapisywanie haseł na karteczkach, które są przyczepiane do klawiatury , monitora czy w jakimkolwiek innym dostępnym miejscu.
3. Zakazane jest zapisywanie haseł w zeszytach , notatnikach które mogą dostać się w ręce osób nieupoważnionych.

Logi w systemach informatycznych oraz ich ochrona

1. Każdy system operacyjny oraz baza danych musi mieć włączone audytowanie – włączony dziennik logów bezpieczeństwa.
2. Jeżeli aplikacja umożliwia włączenie logów bezpieczeństwa, to musi mieć te logi włączone.
3. Administrator danego systemu jest odpowiedzialny za systematyczne przeglądanie logów bezpieczeństwa.
4. Wszystkie stwierdzone anomalie i incydenty bezpieczeństwa muszą być udokumentowane i rozpoznane przez administratora systemu.
5. Jeżeli podczas analizy logów został stwierdzony prawdopodobny wyciek informacji a w szczególności danych osobowych o tym fakcie należy niezwłocznie powiadomić IOD, który powinien postępować zgodnie z opisanymi zasadami w sytuacji naruszenia

ochrony danych osobowych opisanych w Polityce Ochrony Danych Osobowych.
6. Zaleca się chronić aktualne logi. Logi które zostały zarchiwizowane powinny zostać zabezpieczone przed manipulacją i nieuprawnionym dostępem.

Ochrona antywirusowa

1. Wszystkie systemy informatyczne w Centrum Usług Społecznych w Opolu Lubelskim podlegają ochronie antywirusowej. Każda stacja robocza i serwer musi mieć zainstalowany odpowiedni program antywirusowy, który nie tylko sprawdza system o wyznaczonych godzinach, ale także dokonuje analizy plików na bieżąco. System antywirusowy jest uaktualniany z częstotliwością umożliwiającą pobranie najnowszych wzorców złośliwego oprogramowania na bieżąco.
2. Każdy przenośny nośnik informacji , który zostanie podłączony do komputera przez użytkownika, musi zostać sprawdzony antywirusowym programem w celu wykrycia złośliwego oprogramowania.
3. W momencie wykrycia przez program antywirusowy złośliwego oprogramowania należy postępować zgodnie ze wskazówkami programu antywirusowego. Jeżeli natomiast program antywirusowy powiadomi o niemożliwości usunięcia złośliwego oprogramowania należy niezwłocznie zaistniałą sytuację zgłosić do osoby odpowiedzialnej za opiekę nad IT. Sytuację taką należy traktować jako naruszenie bezpieczeństwa.

Synchronizacja czasu na serwerach, komputach oraz w systemach teleinformatycznych.

1. Należy wdrożyć serwer czasu w organizacji.
2. Wszystkie systemy informatyczne powinny mieć ustawiony ten sam czas, a synchronizacja powinna przebiegać automatycznie.
3. Jeżeli któryś z systemów informatycznych nie posiada synchronizacji czasu należy ją niezwłocznie uruchomić.

Zmiany w systemach informatycznych

1. Każda zmiana w systemach informatycznych musi być przygotowana i przetestowana na niezależnym od produkcji środowisku testowym.
2. System testowy nie może zawierać rzeczywistych danych osobowych.
3. Akceptacja wyników testów powinna być wykonana przez zleceniodawcę zmiany przed wdrożeniem na system produkcyjny.
4. Po pozytywnym wyniku testów można wdrożyć zmiany na produkcję.
5. W przypadku, gdy ta sama osoba przygotowuje zmianę i sama ją wdraża muszą być uruchomione mechanizmy audytu tych zmian.
6. Wszystkie zmiany muszą być rejestrowane i dokumentowane.

7. Wykrycie nieautoryzowanych zmian należy traktować jako naruszenie bezpieczeństwa.

Uprawnienia administracyjne na komputerach i systemach

1. Uprawnienia administracyjne na komputerach, przenośnych urządzeniach elektronicznych i systemach są nadawane tylko osobom upoważnionym przez ADO do takiego dostępu.
2. Normalne prace codzienne na komputerach, przenośnych urządzeniach elektronicznych i systemach nie powinny być prowadzone na koncie administratora pomimo że dana osoba ma do tego upoważnienie. Osoba taka powinna posiadać drugie niezależne konto z mniejszymi uprawnieniami.

Poczta elektroniczna

1. Poczta elektroniczna służy tylko do celów służbowych. Zabronione jest wysyłanie informacji, które w jakichkolwiek sposób mogłoby doprowadzić do uszczerbku wizerunku Centrum Usług Społecznych w Opolu Lubelskim, narazić na straty finansowe bądź łamać prawo.
2. Jeżeli otrzymana poczta nie jest związana z obowiązkami służbowymi, to użytkownik po przeczytaniu powinien niezwłocznie usunąć ją ze skrzynki pocztowej.
3. Każda przesłana informacja czy przesyłka pocztą elektroniczną jest własnością Centrum Usług Społecznych w Opolu Lubelskim, więc ADO w uzasadnionych przypadkach zastrzega sobie prawo do wglądu w pocztę elektroniczną pracownika.
4. Nie należy otwierać poczty elektronicznej , jeżeli nadawca jest nieznany. Tym bardziej nie należy otwierać załączników dołączonych do takiej wiadomości.
5. Pocztą elektroniczną dane osobowe mogą być wysyłane tylko przez osoby do tego upoważnione.
6. Jeżeli pocztą elektroniczna są przesyłane dane osobowe, to takie dane muszą być szyfrowane.

Szyfrowanie danych osobowych

1. Dane osobowe wysyłane pocztą elektroniczną muszą być szyfrowane z wykorzystaniem co najmniej standardu AES-256.
2. Dane osobowe przechowywane na przenośnych urządzeniach muszą być szyfrowane za pomocą standardu AES-256.
3. Dane osobowe wprowadzane do systemu przez Internet muszą być wprowadzane przez szyfrowany kanał SSL.

Praca na stanowisku komputerowym

1. Ustawienie monitora powinno uniemożliwić podgląd osobom nieuprawnionym do danych wyświetlanych na monitorze podczas obsługi klientów, w szczególności danych osobowych.
2. Rozpoczynając pracę na komputerze, użytkownik podaje wszystkie wymagane identyfikatory i hasła w taki sposób, aby ich nie ujawnić innym osobom.
3. W przypadku opuszczenia stanowiska pracy, użytkownik systemu obowiązany jest zaktywizować wygaszacz ekranu z hasłem lub zablokować komputer w inny sposób.
4. Po zakończeniu pracy użytkownik powinien prawidłowo wylogować się z systemu, wyłączyć komputer i zabezpieczyć stanowisko przed dostępem osób nieuprawnionych.

Stosowanie urządzeń mobilnych.

1. Zabrania się kopiowania informacji, które mogą być danymi osobowymi na urządzenia mobilne, które nie są własnością Centrum Usług Społecznych w Opolu Lubelskim.
2. Jeżeli w Centrum Usług Społecznych w Opolu Lubelskim używane są urządzenia mobilne, które są wykorzystywane do pracy takie jak tablet lub smartphone, należy zabezpieczyć je przed nieuprawnionym dostępem lub możliwością pozyskania z nich danych osobowych.
3. Aplikacje na urządzeniu mobilnym mogą zostać zainstalowane tylko za zgodą Administratora.
4. Na urządzeniach mobilnych powinien zostać zainstalowany system antywirusowy.

Tymczasowe elektroniczne nośniki informacji

1. Kopiowanie informacji, określonych jako danych osobowych na przenośne nośniki informacji takie jak Cd-Rom, pendrive i inne może być wykonane tylko za zgodą ADO.
2. Użytkownik wykonujący kopiowanie na przenośnym nośniku jest zobowiązany do zachowania szczególnej ostrożności w czasie jego transportu, przechowywania oraz użytkowania tak, aby nie mógł się dostać w niepowołane ręce.
3. Dane, o których mowa w pkt 1 na przenośnych nośnikach informacji muszą być szyfrowane (w standardzie AES-256).
4. Po zakończeniu użytkowania przenośnego nośnika, użytkownik jest zobowiązany zniszczyć lub sformatować ten nośnik w taki sposób, aby odzyskanie danych nie było możliwe.

Rejestr działań administratorów i operatorów a ochrona rejestru.

1. Wszystkie działania kont uprzywilejowanych w tym administratorów oraz operatorów systemów teleinformatycznych powinny być rejestrowane.

2. Rejestr wykonywanych czynności przez administratorów oraz operatorów systemów powinien być systematycznie przeglądany.
3. Rejestr powinien zostać również zabezpieczony w taki sposób aby uniemożliwić manipulację i dokonywanie zmian w celu zamazania zdarzeń.
4. Rejestr powinien być archiwizowany oraz przechowywany w postaci zaszyfrowanej.
5. Dostęp do rejestru powinny mieć tylko osoby upoważnione , które powinny mieć prawa tylko do odczytu.

Nadawanie, odbieranie, przegląd uprawnień do systemów

1. Zakładanie konta dla nowych użytkowników lub zmiana uprawnień w systemie przetwarzającym dane osobowe wykonywane jest przez Administratora systemu na podstawie zlecenia wysłanego drogą mailową przez ADO lub osobę wyznaczoną przez ADO na zastępcę.
2. Zlecenie założenia konta, o którym jest mowa w pkt 1 musi zawierać następujące informację:
   1) na jaki czas jest utworzone dane konto (bezterminowe, lub do określonej daty);
   2) jakie uprawnienia powinny być nadane dla danego użytkownika w systemie.
3. Administrator systemu jest zobowiązany dokonać zmian zgodnie z przesłanym zleceniem niezwłocznie po otrzymaniu informacji.
4. Administrator systemu jest zobowiązany archiwizować wszystkie zlecenia utworzenia kont.
5. Użytkownicy powinni mieć dostęp wyłącznie do tych sieci i usług sieciowych do których otrzymali uprawnienia.
6. W sytuacji rozwiązania umowy o pracę lub zakończaniu współpracy, ADO (lub osoba przez niego wskazana) musi powiadomić Administratora systemu aby konto danego użytkownika zostało zablokowane.
7. Administrator jest zobowiązany do blokady kont niezwłocznie po otrzymaniu informacji od ADO . Administrator jest zobowiązany do archiwizowania zleceń blokady.
8. Co 3 miesiące ADO na podstawie raportu z systemu musi dokonać przeglądu kont osób, na których nie odnotowano żadnej aktywności i zlecić administratorowi systemu by je niezwłocznie zablokował.
9. Co 6 miesięcy ADO na podstawie raportu musi dokonać przeglądu nadanych uprawnień w systemie dla wszystkich aktywnych kont, czy są one zgodne z ostatnimi zleceniami.
10. Uprawnienia do systemów przetwarzających dane osobowe musi być nadawana zgodnie z zasadą *„need to know”*.
11. Jeżeli zostanie zidentyfikowana sytuacja, że danemu użytkownikowi nie zostało odebrane prawo dostępu a powinno być odebrane, lub osoba która miała wgląd do danych i dokonała zmiany i/lub usunęła dane a nie była osobą upoważnioną, należy takie zdarzenie traktować jako naruszenie zasad bezpieczeństwa danych osobowych i postępować zgodnie z opisanymi zasadami w Polityce Ochrony Danych Osobowych.

Instalacja oprogramowania w systemach produkcyjnych oraz zarządzanie podatnościami technicznymi.

1. Instalacja oprogramowania w systemach produkcyjnych powinna być przeprowadzana przez osoby do tego upoważnione a także posiadające uprawnienia administratora.
2. Przed instalacją oprogramowania należy przeprowadzić ich instalacje w środowisku testowym, które jest odseparowane od środowiska produkcyjnego.
3. Przed zainstalowaniem oprogramowania w systemach produkcyjnych należy wykonać ich kopię bezpieczeństwa.
4. Oprogramowanie które jest zainstalowane w środowisku produkcyjnym powinno być systematycznie aktualizowane.
5. Aktualizacja powinna odbywać się najpierw w środowisku testowym a następnie po przeanalizowaniu poprawności działania aktualizacji należy wdrożyć ją w środowisku produkcyjnym.
6. Systemy produkcyjne powinny być systematycznie skanowane poprzez oprogramowanie weryfikujące podatności w tych systemach.
7. Znalezione podatności powinny zostać usunięte.

Udzielanie zdalnego dostępu do systemów informatycznych a także praca zdalna.

1. Zdalny dostęp do danych osobowych w Ośrodku Pomocy Społecznej w Opolu Lubelskim może być realizowany przez szyfrowany kanał VPN/SSL/SSH.
2. Każdy z użytkowników ma nadane odpowiednie konto z hasłem za pomocą którego ustanawia połączenie VPN/SSL/SSH.
3. Możliwość kopiowania plików podczas pracy zdalnej powinna zostać zablokowana.
4. Podczas pracy zdalnej powinno się zabezpieczyć ekran przed dostępem przez osoby nieupoważnione (poprzez stosowanie np. filtrów personalizujących).

Korzystanie z Internetu

1. Z Internetu można korzystać tylko do celów służbowych i edukacyjnych w zakresie swoich obowiązków służbowych.
2. Dopuszcza się użytkownie Internetu do celów prywatnych, jednakże użytkownik powinien korzystać z umiarem z tego zapisu.
3. Nie należy otwierać nieznanych stron internetowych, które mogą być źródłem zagrożenia dla danych osobowych.
4. ADO zastrzega sobie prawo do przeglądu logów dostępu do Internetu w uzasadnionych sytuacjach.

Sprzęt informatycznych oraz sieciowy.

1. Należy systematycznie prowadzić rejestr sprzętu informatycznego.
2. Należy co najmniej raz w roku przeprowadzić inwentaryzację sprzętu informatycznego.
3. Sprzęt należy chronić przed awariami zasilania oraz innymi przerwami mogącymi wpłynąć później na nieprawidłowe działanie tego sprzętu.
4. Okablowanie zasilające oraz telekomunikacyjne powinno być podłączone do sprzętu w taki sposób, by jego przesunięcie nie uszkodziło urządzenia.
5. Sprzęt powinien być prawidłowo konserwowany w celu zapewnienia jego sprawności.
6. Podczas wysyłki sprzętu do serwisów zewnętrznych należy go odpowiednio zabezpieczyć przed uszkodzeniem, a w przypadku gdy jest to komputer należy wysłać go bez dysku który może zawierać dane osobowe.
7. Powinien być prowadzony rejestr czynności i postępowania z aktywami.
8. Przed zbyciem lub przekazaniem sprzętu do ponownego użycia należy zweryfikować wszystkie jego składniki w tym zawierające nośniki informacji, dla zapewnienia, że wszystkie dane osobowe i wrażliwe oraz licencjonowane oprogramowanie zostały usunięte lub bezpiecznie nadpisane.
9. Użytkownicy sprzętu powinni zapewnić odpowiednią ochronę w czasie gdy pozostaje on bez opieki.

Zabezpieczenia komputerów przenośnych

1. Przechowywane dane osobowe na dyskach laptopów należących do Centrum Usług Społecznych w Opolu Lubelskim (na przykład w postaci raportów excelowych, formie plików pdf lub innej postaci) jest dopuszczone tylko w postaci szyfrowanej. Każdy z użytkowników komputerów przenośnych jest zobowiązany do zachowania szczególnej ostrożności w czasie jego transportu, przechowywania oraz użytkowania tak, aby nie mógł się dostać w niepowołane ręce.

Kopie zapasowe systemów informatycznych

1. Codziennie dla systemów jest wykonywana pełna kopia bezpieczeństwa.
2. Kopia bezpieczeństwa o której mowa w pkt.1 jest zapisywana na zewnętrznym dysku lub na serwerze i musi być przechowywana w zaszyfrowanej formie.
3. Dostęp do kopii bezpieczeństwa i kopii archiwalnych jest nadzorowany i zredukowany tylko i wyłącznie do koniecznego minimum poprzez mechanizmy szyfrujące.
4. Kopie danych są przechowywane przez okres 6 lat.
5. Administrator systematycznie dokonuje przeglądu logów kopii bezpieczeństwa.
6. Niemożność wykonania kopii bezpieczeństwa należy traktować jako naruszenie zasad

bezpieczeństwa i należy postępować zgodnie z określonymi zasadami w Polityce Ochrony Danych Osobowych.
7. Należy co najmniej raz w roku należy przeprowadzać próby odtworzenia systemów informatycznych z kopii bezpieczeństwa.

Wykonywanie przeglądów i konserwacji systemów i nośników

1. Sprzęt komputerowy przekazywany do serwisów zewnętrznych pozbawiony jest dysków twardych, natomiast jeżeli warunki gwarancji mówią inaczej dysk twardy podlega backupowi a następnie dane są usuwane w sposób nieodwracalny.
2. W sytuacji niemożności usunięcia danych osobowych z systemu należy podpisać umowę powierzenia przetwarzania danych osobowych oraz zebrać od serwisantów oświadczenia o zachowaniu poufności i nadać im upoważnienia do przetwarzania danych osobowych zgodnie z Polityką Ochrony Danych Osobowych.

Bezpieczeństwo prac rozwojowych oprogramowania i bezpieczeństwo w systemach informatycznych.

1. Należy identyfikować i wprowadzać bezpieczeństwo w aplikacjach na etapie projektowania systemów informacyjnych.
2. Wiadomości na temat prac rozwojowych, w szczególności te wrażliwe, powinny być wysyłane kanałem zaszyfrowanym, utrudniającym dostęp do treści osobom trzecim.
3. Dostęp do logów oprogramowania lub systemu powinien być ograniczony.
4. Powinien być prowadzony rejestr wersji oraz zmian jakie zachodziły w poszczególnych wersjach.
5. Należy systematycznie przeglądać logi systemowe.

Monitorowanie i dostosowanie zasobów w systemach informatycznych.

1. Należy na bieżąco monitorować zajętość miejsca w systemach teleinformatycznych i w odpowiedni sposób reagować tak aby zachować ciągłość pracy systemów.
2. Należy monitorować sprawność urządzeń przechowujących dane, w tym dane osobowe, aby uniknąć awarii systemów informatycznych.

Monitorowanie oraz zarządzanie siecią i usługami sieciowymi.

1. W celu podniesienia bezpieczeństwa w całej infrastrukturze powinno się wdrożyć separację sieci LAN.
2. Należy za pomocą dostępnych środków monitorować sieć a także usługi sieciowe systematycznie.

3. Sieć WiFi dla gości powinna być odseparowana od pozostałej sieci oraz zabezpieczona oraz i szyfrowana.
4. Sieć WiFi znajdująca się w Centrum Usług Społecznych w Opolu Lubelskim powinna być zabezpieczona przed dostępem z zewnątrz osób niepożądanych, a także Komunikacja powinna być szyfrowana.
5. Aby podnieść bezpieczeństwo sieci, powinno się wdrożyć rozwiązania wykrywania incydentów bezpieczeństwa w warstwie sieciowej (IDS/IPS).
6. Należy zmienić domyślne hasła wszystkich urządzeń sieciowych (routery, switche, access pointy, drukarki oraz skanery sieciowe, centrale i telefony VoIP).
7. Powinna zostać również wprowadzona blokada podłączanych urządzeń do sieci LAN/WiFi po adresach MAC.

Analiza i bezpieczeństwo usług aplikacyjnych oraz usług transakcji w sieciach publicznych.

1. Należy monitorować aplikacje oraz transakcje w sieciach publicznych.
2. Należy systematycznie przeglądać logi bezpieczeństwa a także je analizować.
3. Aplikacje powinny być aktualizowane na bieżąco.
4. Wszystkie transakcje, które są nieautoryzowane powinny zostać odnotowywane.

Rozdzielenie środowisk programistycznych, testowych oraz produkcyjnych a także przetwarzanie danych osobowych.

1. Środowisko programistyczne, testowe oraz produkcyjne powinny zostać rozdzielone i odseparowane od siebie, tak aby dostęp z każdej sieci do innej był niemożliwy.
2. W środowisku programistycznym oraz testowym dane osobowe powinny zostać zanonimizowane lub jeżeli to nie możliwe należy używać danych nierzeczywistych, które zostały odpowiednio spreparowane.

Zasady naruszenia bezpieczeństwa informacji w systemach informatycznych.

1. Incydent Bezpieczeństwa Informacji w środowisku IT to wystąpienie stanu systemu usługi lub sieci, który wskazuje na możliwe:

    1. przełamania zasad polityki bezpieczeństwa informacji;
    2. błąd zabezpieczenia;
    3. nieznaną sytuację, która może być powiązana z bezpieczeństwem informacji.

2. Incydent Bezpieczeństwa Informacji to pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które

stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji.

3. Incydent może być działaniem umyślnym, nieumyślnym, błędem lub nieznanym o charakterze faktycznym, usiłowania czy podejrzewanym w następujących kategoriach:

    1. **odmowa usługi** – incydent który uniemożliwia lub w znaczący sposób utrudnia korzystania w sposób autoryzowany z sieci, systemów czy pozostałych elementów infrastruktury (np. drukarki sieciowe);
    2. **złośliwy kod** – wirus, trojan inny złośliwy kod, który może z powodzeniem zniszczyć, zmodyfikować, upublicznić informacje zawarte w systemach;
    3. **nieautoryzowany dostęp** – incydent w którym osoba w nieautoryzowany sposób uzyskała dostęp logiczny lub fizyczny do sieci, systemów danych czy innych zasobów IT;
    4. **nieprawidłowe użytkowanie** – incydent, w którym osoba narusza zasady użytkowania sieci czy komputerów, na przykład:
        1) poprzez ściąganie czy instalację narzędzi do łamania haseł, nielegalnego oprogramowania, czy pornografii
        2) wysyłanie spamu na przykład promującego prywatny biznes;
        3) poprzez wysyłanie napastliwych e-maili do współpracowników;
        4) uruchomienie nieautoryzowanego serwisu internetowego (strona www) na komputerze Centrum Usług Społecznych w Opolu Lubelskim;
        5) wykorzystanie plików muzycznych lub ich udostępnianie dla których własność jest nie określona, lub nie zostały zakupione przez Centrum Usług Społecznych w Opolu Lubelskim, lub nie zostały dla / przez Centrum Usług Społecznych wyprodukowane, lub dystrybucja innych pirackich materiałów;
        6) nieautoryzowane wysyłanie danych osobowych do osób nieupoważnionych lub na zewnątrz;
    5. **nagłe wyłączenie systemu** – nagłe, niezaplanowane wyłączenie systemów informatycznych, czy innych urządzeń sieciowych
    6. **mieszany** – zdarzenie, które obejmuje dwa lub więcej incydentów omówionych powyżej.

4. Każdy pracownik, współpracownik Centrum Usług Społecznych w Opolu Lubelskim, który jest świadkiem naruszenia zasad bezpieczeństwa lub podejrzewa taką sytuację, jest zobowiązany zgłosić zaistniałą sytuację zgodnie z Polityką Ochrony Danych Osobowych.

Odpowiedzialność karna

1. Nieprzestrzeganie zasad zawartych w niniejszym dokumencie może skutkować sankcjami karnymi przewidzianymi w Kodeksie Karnym (art. 130, 165, 266 – 269b. 287), ustawie o prawie autorskim i prawach pokrewnych (art. 115-123) oraz ustawie o ochronie danych osobowych (art. 51,52).
2. Niezależnie od odpowiedzialności przewidzianej w tych przepisach, nieprzestrzeganie

wymienionych zasad może również być uznane za ciężkie naruszenie podstawowych obowiązków pracowniczych, co stanowi podstawę do rozwiązania stosunku pracy bez wypowiedzenia na podstawie art. 52 Kodeksu Pracy.

DYREKTOR
Centrum Usług Społecznych
w Opolu Lubelskim
dr n. med. Ewelina Szkutnicka