zał. Nr 1 do zarządzenia nr 89 z dnia 22 maja 2013r.

POLITYKA BEZPIECZEŃSTWA INFORMACJI W CENTRUM ODWYKOWYM SPZOZ

Wydanie nr 2 Stan na dzień 16-05-2013

Jest to dokument równoważny dokumentom normatywnym dotyczący:

- Polityka ochrony danych osobowych CO SPZOZ w tym szczególnie danych medycznych pacjentów,
- Polityka prywatności CO SPZOZ,
- Polityka ochrony informacji CO SPZOZ.

Podstawy prawne:

- Ustawa z dnia 29 sierpnia 1997r. o ochronie danych osobowych (tekst jednolity: Dz.U.z 2002r. Nr 101 poz.926 z późn. zmianami). Określa zasady postępowania przy przetwarzaniu danych osobowych w systemach informatycznych oraz w kartotekach, skorowidzach, księgach, wykazach i w innych zbiorach ewidencyjnych.
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. z 2004 r. Nr l00 poz.l024).
- ROZPORZĄDZENIE MINISTRA ZDROWIA1) z dnia 21 grudnia 2010 r. w sprawie rodzajów i zakresu dokumentacji medycznej oraz sposobu jej przetwarzania
- Ustawa z dnia 15 kwietnia 2011 r. o działalności leczniczej Dz.U. 2011 nr 112 poz. 654
- Ustawa z 5 grudnia 1996 o zawodzie lekarza (DU 1997 nr 28 poz.152 z póź.zm.).

1. Wstęp

1.1. Informacja jest bardzo ważnym aktywem CO SPZOZ i dlatego należy ją odpowiednio chronić.

1.2. Jakość naszej pracy zależy w dużej mierze od jakości informacji.

1.3. Chroniąc informacje zachowujemy prywatność i godność każdego pracownika oraz dbamy o interesy partnerów i klientów.

1.4. Bezpieczeństwo informacji w CO SPZOZ ma podstawowe znaczenie dla utrzymania naszej konkurencyjności, płynności finansowej, zysku, zgodności z przepisami prawa i wizerunku

1.5. Spełnienie wymagań prawnych jest celem podstawowym

1.6. Niniejszy dokument "Polityka Bezpieczeństwa CO SPZOZ" porządkuje kwestię związane z bezpieczeństwem informacji w CO SPZOZ i zawiera najważniejsze zasady postępowania z informacją w CO SPZOZ.

1.7. Obowiązkiem pracowników jest przestrzeganie postanowień niniejszej polityki bezpieczeństwa informacji CO SPZOZ, a w szczególności zasad:

- **co nie jest wyraźnie dozwolone, jest zabronione,**
- **czystego biurka –** ***praca z dokumentacją papierową tj. na biurku tylko to aktualnie konieczne***
- **czystego ekranu –** ***na ekranie tylko to co konieczne i obowiązkowy wygaszacz*****.**

Politykę bezpieczeństwa informacji zwaną także Polityką Prywatności nadzoruje osobiście Dyrektor CO SPZOZ który jest jednocześnie **ADMINISTRATOREM DANYCH OSOBOWYCH**
[ADO]

2. Organizacja bezpieczeństwa

2.1. W celu koordynacji i kontrolowania procesu zapewniania bezpieczeństwa informacji w CO SPZOZ został powołany Zespół Bezpieczeństwa Informacji w skład którego wchodzi:

- Dyrektor CO SPZOZ [DN] jednocześnie Administrator Danych Osobowych [**ADO**],
- Administrator Bezpieczeństwa Informacji [ABI],
- Administrator Sieci Teleinformatycznej [ASTI].

2.2. Zespół Bezpieczeństwa Informacji koordynuje rozwój, wdrażanie i aktualizacje niniejszego dokumentu.

2.3. Zespół Bezpieczeństwa Informacji jest jedynym organem zatwierdzającym zmiany w niniejszym dokumencie.

2.4. Zespół Bezpieczeństwa Informacji podejmuje decyzje w przypadku najpoważniejszych incydentów związanych z bezpieczeństwem informacji oraz określa sankcje za jej naruszenie

2.5. Zespół Bezpieczeństwa Informacji podejmuje decyzje w sprawie powoływania i przeprowadzania audytu (zewnętrznego lub wewnętrznego), mającego na celu zweryfikowanie efektywności wdrożonych zasad bezpieczeństwa opisanych w tym dokumencie.

2.6. Administrator Bezpieczeństwa Informacji podlega bezpośrednio Dyrektorowi CO SPZOZ który jest jednocześnie Administratorem Danych Osobowych.

2.7. Administrator Bezpieczeństwa CO SPZOZ wdraża decyzje i postanowienia określone przez Zespół Bezpieczeństwa Informacji i bezpośrednio nadzoruje wykonywanie zadań w zakresie określonym tym dokumentem.

2.8. Dyrektor .CO SPZOZ pełni obowiązki Administratora Danych zgodnie z Ustawą o Ochronie Danych Osobowych z 29.08.1997 (i późniejsze rozporządzenia do tej ustawy).

2.9. Kontakt z Zespołem Bezpieczeństwa CO SPZOZ Informacji następuje tylko i wyłącznie poprzez Dyrektora CO SPZOZ.

2.10. Dyrektor CO SPZOZ zarządza kwestią powoływania zewnętrznych / wewnętrznych konsultantów ds. bezpieczeństwa informacji.

2.11. Dyrektor CO SPZOZ utrzymuje bezpośrednie kontakty z organami ścigania, organami wydającymi przepisy, dostawcami usług informatycznych i telekomunikacyjnych jeśli chodzi o aspekty naruszenia bezpieczeństwa i dba o rodzaj przekazywanych informacji.

2.12. Administrator Sieci Teleinformatycznej podlega bezpośrednio Administratorowi Bezpieczeństwa Informacji i jest członkiem Zespołu Bezpieczeństwa Informacji.

2.13. Administrator Sieci Teleinformatycznej pełni obowiązki zgodnie z Ustawą o Ochronie Danych Osobowych z 29.08.1997 (i późniejsze rozporządzenia do tej ustawy) i ROZPORZNDZENIEM MINISTRA SPRAW WEWNĘTRZNYCH I ADMINISTRACJI z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (DU 2004r. nr 100 poz.1024)

2.14. Dokładny spis osób z nazwiska i imienia pełniących opisane funkcje znajduje się w dokumencie "**INSTRUKCJI OCHRONU DANYCH OSOBOWYCH CO SPZOZ**".

3. Inwentaryzacja, klasyfikacja i kontrola aktywów informacyjnych

3.1. CO SPZOZ musi tworzyć, zarządzać i uaktualniać bazę danych jego aktywów informacyjnych.

3.2. Wszystkie informacje, dane i dokumenty muszą być klarownie opisane, tak aby wszyscy Pracownicy i współpracownicy byli świadomi, kto jest właścicielem informacji i jaki jest jego poziom klasyfikacji.

3.3. Wszystkie informacje, dane i dokumenty muszą być przetwarzane i przechowywane zgodnie z poziomem klasyfikacji przypisanym do informacji.
3.4. Wszystkie informacje, dane i dokumenty sklasyfikowane jako wysoko wrażliwe (ściśle tajne) muszą być przechowywane w obszarach chronionych .
3.5. Wszystkie informacje, dane i dokumenty muszą być sklasyfikowane zgodnie z poziomem ich poufności, integralności i dostępności.
3.6. Za wszystkie informacje, dane i dokumenty odpowiada ich odpowiedni właściciel, lub gestor, w którego gestii są te informacje.
3.7. Proces inwentaryzacji, klasyfikacji i kontroli aktywów CO SPZOZ musi być przeprowadzany zgodnie z procedurami "**INSTRUKCJI OCHRONY DANYCH OSOBOWYCH CO SPZOZ**".
3.8. Lista zinwentaryzowanych i sklasyfikowanych informacji z przypisanymi właścicielami znajduje się w dokumencie "**INSTRUKCJI OCHRONY DANYCH OSOBOWYCH CO SPZOZ**".

4. Bezpieczeństwo osobowe

4.1. *Rekrutacja, zatrudnianie i zwalnianie pracowników*

4.1.1. Referent ds. Administracyjnych odpowiada za przeprowadzanie procesu rekrutacji nowych pracowników.
4.1.2. Proces rekrutacji musi być przeprowadzany rzetelnie i zgodnie z procedurą opisaną w dokumencie ." **Referent ds. Administracyjnych - Rekrutacja pracowników**"
4.1.3.Warunki zobowiązanie pracownika do zaznajomienia i przestrzegania aspektów zatrudnienia muszą brać pod uwagę zgodność z niniejszym dokumentem, a w szczególności bezpieczeństwa wynikających z tego dokumentu. Poza tym warunki zatrudnienia muszą dokładnie określać kwestię naruszenia bezpieczeństwa informacji i konsekwencji z tym związanych.
4.1.4. Każdy nowy pracownik musi podpisać Oświadczenie o zachowaniu poufności i ochrony danych osobowych.
4.1.5. Jeżeli nowego pracownika dotyczy przeniesienie praw autorskich na CO SPZOZ, należy spisać stosowną umowę.
4.1.6. Dokładne wymagania prawne dotyczące nowych pracowników opisane są w dokumencie " **Referent ds. Administracyjnych – Wykaz stanowisk i kwalifikacji osób zatrudnionych w CO SPZOZ- Regulamin organizacyjny CO SPZOZ"**
4.1.7.Proces zwalniania pracownika musi być przeprowadzany zgodnie z procedurą opisaną w dokumencie " **Referent ds. Administracyjnych - Zwalnianie pracowników**"

4.2. *Zasady postępowania pracowników i współpracowników CO SPZOZ*

4.2.1. Pracownicy i współpracownicy nie powinni wykorzystywać łącz internetowych do celów prywatnych nie związanych z realizacją umowy w tym umowy o pracę.

4.2.2. Pracownikom i współpracownikom nie wolno :

- nagrywać danych osobowych w tym medycznych oraz danych dotyczących umów i finansów CO SPZOZ na zewnętrzne nośniki informatyczne i nie wolno przesyłać ich pocztą elektroniczną – nie dotyczy to osób funkcyjnych prowadzących rozliczenia z NFZ za zgodą Dyrektora CO SPZOZ;
- wynosić dokumentacji osobowej w tym medycznej oraz dokumentacji dotyczącej rozliczeń finansowych i umów COSPZOZ poza obiekty COZPSOZ bez upoważnienia Dyrektora CO SPZOZ.

4.2.3. Pracownicy i współpracownicy nie mogą ujawniać informacji na temat wysokości swoich zarobków.

4.2.4. Pracownicy i współpracownicy nie mogą pożyczać sobie nawzajem kluczy i kart służących do otwierania pomieszczeń

4.2.5. Pracownicy i współpracownicy nie mogą pożyczać sobie nawzajem pieniędzy.

4.2.6. Wykorzystywanie środków służbowych, tj. telefony, samochody służbowe, poczta elektroniczna do celów prywatnych powinno być ograniczone tylko i wyłącznie do nadzwyczajnych sytuacji.

4.2.7. Wykorzystanie telefonów komórkowych i stacjonarnych jest monitorowane w stosunku do wszystkich pracowników przez Administrację CO SPZOZ i w uzasadnionych przypadkach pracownik może zostać zobowiązany do opłacenia rachunku telefonicznego, jeżeli kwestia jego użycia do celów służbowych budzi wątpliwości.

4.2.8. Firmowe karty płatnicze i wykonywanie na tych kartach operacje finansowe obciążają pracownika w przypadku, gdy charakter przeprowadzonych transakcji budzi wątpliwości.

4.2.9. Tylko upoważnieni przez dyrektora CO SPZOZ Pracownicy i współpracownicy mogą reprezentować formalnie CO SPZOZ na zewnątrz.

4.3. *Szkolenia pracowników i współpracowników*

4.3.1. Pracownicy i współpracownicy zobowiązani są do uczestnictwa w szkoleniu w zakresie polityki bezpieczeństwa i procedur obowiązujących w CO SPZOZ w tym w instruktażu wstępnym przed udzieleniem dostępu do przetwarzania informacji i danych osobowych .

4.3.2. Pracownicy i współpracownicy zobowiązani są do uczestnictwa w innych szkoleniach, jeżeli bezpośredni przełożony zleci uczestnictwo w takim szkoleniu.

5. Bezpieczeństwo fizyczne i środowiskowe

5.1. *Kontrola wejścia i wyjścia*

5.1.1. Dostęp poszczególnych osób do pomieszczeń szczególnie chronionych np. serwerownie, rejestr usług, rejestracje, archiwa, składnice akt itp. powinien być uzasadniony potrzebami funkcjonowania CO SPZOZ. Prawa dostępu powinny podlegać okresowemu przeglądowi i być bezzwłocznie odbierane w przypadku, gdy nie są już niezbędne.

5.1.2. W celu uniknięcia konieczności przydzielania praw dostępu do pomieszczeń szczególnie chronionych zbyt wielu osobom, nie należy umieszczać w nich urządzeń i materiałów ogólnodostępnych takich jak drukarki, faksy, części komputerowe lub materiały biurowe.

5.1.3. W pomieszczeniach szczególnie chronionych osoby nie zatrudnione w CO SPZOZ przebywają pod nadzorem upoważnionych pracowników. W dzienniku dostępu na obszary chronione należy zarejestrować ich dane, a także datę i godzinę ich wejścia i wyjścia. Wstęp na obszary chronione jest dozwolony wyłącznie za zgodą Administratora Bezpieczeństwa Informacji.

5.1.4. Drzwi do pomieszczeń szczególnie chronionych powinny być zawsze zamykane.

5.1.5. Przed uzyskaniem dostępu do pomieszczeń, gdzie zlokalizowano urządzenia przetwarzania informacji, użytkownicy muszą być zidentyfikowani. System dostępu do tego rodzaju pomieszczeń powinien być oparty na unikatowych identyfikatorach przydzielonych poszczególnym użytkownikom. Konieczne jest zmierzanie do wdrożenia mechanizmów rejestrowania faktu oraz czasu wejścia i wyjścia poszczególnych osób do tych pomieszczeń. Należy także rejestrować osoby wprowadzane do pomieszczeń komputerowych szczególnie chronionych przez osoby upoważnione – ten zapis dotyczy planowanych serwerowni.

5.2. *Praca* w *obszarach szczególnie chronionych tj. w planowanych do wdrożenia*

5.2.1. Informacje o istnieniu zabezpieczeń na obszarach chronionych dostępne są tylko i wyłącznie upoważnionym pracownikom.

5.2.2. .Niewykorzystywane obszary chronione powinny być zamknięte i okresowo kontrolowane.

5.2.3. Zewnętrzni dostawcy usług uzyskują ograniczony dostęp do obszarów chronionych lub urządzeń do przetwarzania informacji tylko w razie potrzeby. Tego rodzaju dostęp powinien być zatwierdzony przez Dyrektora CO SPZOZ i monitorowany przez Administratora Bezpieczeństwa Informacji .

5.2.4. Podczas wykonywania pracy na obszarach chronionych zewnętrzni dostawcy usług muszą cały czas przebywać w towarzystwie przynajmniej jednego pracownika CO SPZOZ.

5.2.5. Na obszarze chronionym nie wolno używać sprzętu fotograficznego, video, magnetofonów i innych urządzeń do rejestracji informacji, chyba że zezwoli na to Dyrektora CO SPZOZ

5.3. Zabezpieczanie sprzętu

5.3.1. Lokalizacja urządzeń do przetwarzania informacji CO SPZOZ powinna uwzględniać minimalizację ryzyka oraz potencjalnych zagrożeń takich jak na przykład kradzież, pożar, zalanie, promieniowanie elektromagnetyczne czy zanik zasilania.

5.3.2. Jeśli to możliwe, wszelkie pomieszczenia zawierające sprzęt komputerowy oraz telekomunikacyjny powinny być zlokalizowane powyżej parteru aby zminimalizować ryzyko kradzieży oraz zalania. Zasada ta powinna być szczególnie rygorystycznie przestrzegana w przypadku budynków, znajdujących się w bezpośredniej bliskości dużych cieków wodnych jak rzeki lub kanały.

5.3.3. W pomieszczeniach komputerowych obowiązuje całkowity zakaz jedzenia, picia i palenia tytoniu. Komputery powinny być także chronione przed kurzem.

5.3.4. Kluczowe wyposażenie komputerowe musi znajdować się w pomieszczeniach wyposażonych w urządzenia przeciwpożarowe oraz przeciwpożarową instalację alarmową.

5.3.5. Pomieszczenia zawierające kluczowe wyposażenie komputerowe nie mogą znajdować się w pobliżu pomieszczeń zwiększających ryzyko pożarowe (np. pomieszczeń magazynowych, transformatorowych) oraz zawierających duże instalacje wodne (np. toaleta).

5.3.6. W pomieszczeniach zawierających kluczowe wyposażenie komputerowe nie są przechowywane żadne materiały łatwopalne. Wszystkie ściany otaczające pomieszczenia, w których znajduje się kluczowe wyposażenie komputerowe powinny być niepalne oraz powinny posiadać właściwości ogniotrwałe (o wytrzymałości co najmniej godziny). Wszelkie otwory w tych ścianach takie jak drzwi, wentylacja powinny zamykać się automatycznie oraz powinny posiadać taką samą ogniotrwałość.

5.3.7. Wszystkie kluczowe urządzenia komputerowe powinny znajdować się w pomieszczeniach klimatyzowanych. Praca klimatyzacji winna być monitorowana. Klimatyzacja wyłącza się automatycznie przy jego kontroli i inwentaryzacji. Rejestry urządzeń komputerowych są regularnie aktualizowane.

5.3.8. W przypadku stwierdzenia utraty lub kradzieży jakichkolwiek urządzeń lub oprogramowania komputerowego należy natychmiast poinformować Dyrektora CO SPZOZ.

6. Kontrola dostępu do zasobów informacyjnych

6.1. Dostęp do zasobów systemów informatycznych.

6.1.1. Wyłącznie uprawnieni użytkownicy mogą uzyskać dostęp do systemów informatycznych

CO SPZOZ.

6.1.2. Dostęp musi być indywidualnie zdefiniowany dla każdego użytkownika. Użytkownik może mieć dostęp jedynie do zasobów, które są mu niezbędne do wykonywania obowiązków służbowych. Udzielanie, unieważnianie i ograniczanie dostępu użytkownikom musi przebiegać w oparciu o dalej przedstawione zasady.

6.1.3. Tożsamość każdego użytkownika systemów informatycznych CO SPZOZ musi być jednoznacznie określona i musi być sprawdzona przed rozpoczęciem pracy w systemie (uwierzytelnienie).

6.1.4. W przypadku połączeń dokonywanych z sieci wewnętrznej CO SPZOZ uwierzytelnienie użytkownika polega na sprawdzeniu identyfikatora i hasła przypisanych do profilu użytkownika.

6.1.5. W przypadku połączeń zewnętrznych uwierzytelnienie na podstawie identyfikatora użytkownika i stałego hasła jest niedostateczne i wymagane jest wykorzystanie złożonych technik uwierzytelniania (np.: połączeń zwrotnych, haseł jednokrotnego dostępu, generatorów haseł jednorazowych).

6.1.6. O ile pozwala na to oprogramowanie, na ekranie powitalnym muszą być zawarte następujące informacje:

6.1.6.1. nazwa właściciela systemu,

6.1.6.2. nazwa systemu,

6.1.6.3. pouczenie użytkownika o tym, że kontynuując pracę w systemie potwierdza uprawnienia do korzystania z zasobów systemu informatycznego CO SPZOZ,

6.1.6.4. stwierdzenie, że użytkownik zna i akceptuje zasady dotyczące bezpieczeństwa systemów informatycznych CO SPZOZ.

6.1.7. Wszystkie systemy informatyczne CO SPZOZ powinny posiadać uaktywnioną opcję wygaszacza ekranu w przypadku braku aktywności użytkownika w systemie. Czas uaktywnienia wygaszacza ekranu nie może być dłuższy niż 15 minut. Odblokowanie wygaszacza ekranu musi wymagać podania hasła. Podobnie, wszystkie sesje dostępu do zasobów informatycznych (a w szczególności do komend systemu operacyjnego) musza być zawieszane (lub zrywane) po 15 minutach bezczynności. System powinien umożliwiać uaktywnienie wygaszacza ekranu na żądanie użytkownika.

6.1.8. W systemach informatycznych CO SPZOZ nie mogą być aktywne ogólnodostępne profile domyślne typu "**gość**".

6.1.9. Ograniczanie przez CO SPZOZ dostępu do zasobów systemów informatycznych przebiega w następujący sposób:

6.1.9.1. fizyczny dostęp do sieci mogą mieć tylko takie urządzenia sieciowe, które uzyskały akceptację Administratora Systemu Teleinformatycznego (ASTI) w porozumieniu z Administratorem Bezpieczeństwa Informacji (ABI) ;

6.1.9.2. mechanizmy kontroli muszą umożliwiać wykrycie obecności nieautoryzowanych urządzeń sieciowych,

6.1.9.3. logiczny dostęp do sieci - uzyskanie dostępu do zasobów sieciowych mogą mieć tylko zarejestrowani użytkownicy jednoznacznie zidentyfikowani,

6.1.9.4. dostęp do komend systemu operacyjnego tylko użytkownicy, których zakres obowiązków wymaga dostępu do systemu operacyjnego mogą być uprawnieni do logowania się bezpośrednio na serwerach sieciowych,

6.1.9.5. -dostęp do aplikacji i baz danych - dostęp do aplikacji i baz danych CO SPZOZ wymaga uprzedniej identyfikacji i uwierzytelnienia użytkownika; przyznane użytkownikowi uprawnienia do korzystania z poszczególnych aplikacji i baz danych powinny być ograniczone wyłącznie do zakresu jego obowiązków służbowych.

6.1.10. Nadanie lub zmiana uprawnień użytkownika następuje wyłącznie na wniosek sporządzony pisemnie lub elektronicznie zgodnie z obowiązującymi procedurami. Wnioski muszą być przechowywane co najmniej przez okres 5 lat.

6.1.11. Nazwa profilu użytkownika musi być unikatowa i nie powinna zmieniać się przez cały okres jego pracy w CO SPZOZ, nie licząc przypadków takich jak np. zmiana nazwiska.

6.1.12. Osoby nie będące pracownikami lub współpracownikami CO SPZOZ nie mogą uzyskać profilu użytkownika ani uprawnień w zakresie korzystania z systemów

informatycznych CO SPZOZ bez uprzedniej, pisemnej zgody gestora i/lub Dyrektora CO SPZOZ.

6.1.13. Uprawnienia użytkowników nie będących pracownikami lub współpracownikami CO SPZOZ mogą być przyznane jedynie na czas określony potrzebami tego uprawnienia .

6.1.14. Uprawnienia specjalne mogą być przyznawane wyłącznie osobom odpowiedzialnym za administrowanie systemami za zgodą gestora oraz Dyrektora CO SPZOZ.

6.1.15. Osoby przetwarzających dane w CO SPZOZ muszą podpisać oświadczenia, że będą przestrzegać zasad dotyczących bezpieczeństwa systemów informatycznych CO SPZOZ i bezpieczeństwa danych osobowych oraz firmowych.

6.1.16. Warunki korzystania z połączenia wewnętrznej sieci CO SPZOZ z systemami zewnętrznymi regulują podpisane umowy, szczegółowo precyzujące warunki techniczne i funkcjonalne połączenia. Umowy muszą być regularnie odnawiane. Umowa musi zawierać klauzulę dotyczącą przestrzegania zasad bezpieczeństwa systemów informatycznych CO SPZOZ.

6.1.17. Liczba użytkowników mających uprawnienia specjalne do korzystania z zasobów danego systemu informatycznego CO SPZOZ powinna być ograniczona do niezbędnego minimum, jednak nie może to być mniej niż 2 osoby.

6.1.18. Uprawnienia niezbędne do przeprowadzenia testów poziomu bezpieczeństwa systemów informatycznych CO SPZOZ mogą być wydane na ściśle określony czas, niezbędny do przeprowadzenia testów i wymagają zgody Dyrektora CO SPZOZ..

6.1.19. Konto użytkownika musi być zablokowane po 30 dniach nieaktywności. Kierownicy jednostek organizacyjnych CO SPZOZ są zobowiązani informować administratorów systemów odpowiedzialnych za poszczególne konta o planowanych nieobecnościach w pracy podległych pracowników dłuższych niż 30 dni. Administratorzy mają obowiązek zablokować konto użytkownika na czas jego nieobecności w pracy ponad 30 dni.

6.1.20. Jeżeli dany podsystem kontroli dostępu do systemów informatycznych CO SPZOZ nie funkcjonuje prawidłowo, uprawnienia użytkowników powinny być zablokowane. W przypadku nieprawidłowego funkcjonowania podsystemów kontroli dostępu, decyzje o dalszych działaniach podejmuje gestor.

6.1.21. Uprawnienia nadane użytkownikom muszą być aktualizowane przez ASTI po uzgodnieniu z kierownikami jednostek organizacyjnych CO SPZOZ co 6 miesięcy.

6.1.22. Kierownicy jednostek organizacyjnych CO SPZOZ są zobowiązani informować administratorów systemów odpowiedzialnych za poszczególne konta o zmianach w zakresie obowiązków podległych pracowników skutkujących koniecznością zmiany ich uprawnień.

6.1.23. Referent ds. Administracyjnych jest zobowiązany poinformować Administratora Bezpieczeństwa Informacji o zmianach statusu pracownika. Podobnie osoby odpowiedzialne za współpracę z dostawcami zewnętrznymi są zobowiązane do informowania o zmianach statusu pracowników dostawcy zewnętrznego posiadających dostęp do systemów CO SPZOZ.

6.1.24. Administrator Bezpieczeństwa Informacji [ABI] odpowiada za poinformowanie Administratora Systemów Teleinformatycznych [ASTI] CO SPZOZ o zmianach statusu pracownika.

6.1.25. Uprawnienia posiadane przez użytkownika nie mogą być rozszerzane, o ile nie istnieje umotywowana potrzeba związana ze zmianą zakresu obowiązków użytkownika.

6.1.26. Systemy informatyczne CO SPZOZ· przetwarzające dane sklasyfikowane jako wrażliwe lub strategiczne muszą być skonfigurowane w taki sposób, aby uniemożliwić użytkownikom dostęp do zasobów systemów, do których nie są autoryzowani.

6.1.27. Systemy informatyczne CO SPZOZ przetwarzające dane sklasyfikowane.

.....