BARTEX	BARTEX – Bartol WINIARNIA	
	Procedura systemu zarządzania **Polityka Bezpieczeństwa informacji**	**Ps.4.3 /2**

1. Cel

Polityka Bezpieczeństwa informacji jest dokumentem opisującym zasady ochrony danych elektronicznych w celu spełnienia zapewnienia cyberbezpieczeństwa i wymagań prawnych. Polityka bezpieczeństwa informacji jest poddawana przeglądom w zaplanowanych odstępach czasu lub wtedy, gdy wystąpią istotne zmiany, aby zapewnić, że jest właściwa, adekwatna i skuteczna. Przegląd obejmuje szacowanie możliwości udoskonalenia Polityki Bezpieczeństwa informacji w organizacji oraz podejścia do zarządzania bezpieczeństwem informacji, z uwzględnieniem zmian środowiska organizacyjnego, warunków biznesowych, prawnych lub środowiska technicznego.

2. Zakres

Zakres Polityki obejmuje:

- Inwentaryzacja danych - wykaz zbiorów danych
- Role i odpowiedzialność za bezpieczeństwo informacji - upoważnienie do przetwarzania danych
- Umowa powierzenia przetwarzania danych
- Opis zdarzeń naruszających ochronę danych
- Bezpieczeństwo fizyczne w obszarach przetwarzania danych
- Polityka kluczy
- Zabezpieczenie sprzętu
- Systemy wspomagające- zasilanie, łączność i inne media
- Konserwacja sprzętu
- Wynoszenie aktywów poza siedzibę organizacji
- Bezpiecznie zbywanie lub przekazywanie do ponownego użycia
- Polityka czystego biurka i czystego ekranu
- Bezpieczeństwo systemów informatycznych i danych. Kopie zapasowe
- Zasady korzystania z Internetu
- Zasady korzystania z poczty elektronicznej
- Zarządzanie nośnikami wymiennymi
- Dostęp do sieci i usług sieciowych
- Zarządzanie identyfikatorami użytkowników
- Nadawanie, odbieranie lub dostosowywanie praw dostępu
- Stosowanie poufnych informacji uwierzytelniających
- Zabezpieczenie przed szkodliwym oprogramowaniem
- Polityka bezpieczeństwa informacji w relacjach z dostawcami
- Zasady monitoringu wizyjnego
- Zapewnienie ciągłości działania

3. Terminologia

„dane osobowe” oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

„przetwarzanie” oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką

jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

„zbiór danych” oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;

„administrator” oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania;

„podmiot przetwarzający” oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;

„**aktywa”** - wszystko, co ma wartość dla organizacji

„**analiza ryzyka”** - systematyczne wykorzystywanie informacji do zidentyfikowania źródeł ryzyka i jego oszacowania

„**analiza zagrożeń”** - badanie działań i zdarzeń, które mogą szkodliwie wpływać na system przetwarzania danych,

„**audyt bezpieczeństwa”** - niezależny przegląd i sprawdzenie zapisów oraz funkcji systemu przetwarzania danych w celu sprawdzenia prawidłowości kontroli systemowej, zapewnienia zgodności z przyjętą polityką bezpieczeństwa i procedurami działania w celu wykrycia przełamania bezpieczeństwa oraz zalecenia określonych zmian w kontroli, polityce bezpieczeństwa i procedurach,

„**autentyczność”** - właściwość zapewniająca, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana; autentyczność dotyczy takich podmiotów, jak użytkownicy, procesy, systemy i informacja

„badanie zgodności” - przeprowadzenie testów i dokonanie ocen bezpieczeństwa w celu ustalenia zgodności ze specyfikacją i z wymaganiami systemu bezpieczeństwa,

„**bezpieczeństwo”** - stan lub ochrona przed niekontrolowanymi stratami lub skutkami, kombinacja usług zapewniających poufność, integralność i dostępność,

„**bezpieczeństwo informacji”** - zachowanie poufności, integralności i dostępności informacji; dodatkowo mogą być brane pod uwagę inne właściwości, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność

„**bezpieczeństwo systemu informatycznego”** - wszystkie aspekty związane z definiowaniem, osiąganiem i utrzymywaniem poufności, integralności, dostępności, rozliczalności, autentyczności i niezawodności systemu informatycznego,

„**ciągłość działania”** - utrzymanie niezbędnych usług systemu informatycznego po poważnej awarii w centrum informatycznym, która może być spowodowana przyczynami naturalnymi, takimi jak pożar lub trzęsienie ziemi, lub zdarzeniami wywołanymi umyślnie, np. sabotażem,

„dokumentacja” - pisemna lub zarejestrowana w innej formie informacja o przedmiocie oceny, wymagana do jego oceny,

„**dostępność”** - oznacza zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią aktywów wtedy, gdy jest to potrzebne [ISO/IEC 17799:2005] ,

„**incydent związany z bezpieczeństwem informacji”** - pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji [ISO/IEC TR 18044:2004],

„**integralność”** - właściwość polegająca na zapewnieniu dokładności i kompletności aktywów

„**ocena ryzyka**” - proces porównywania oszacowanego ryzyka z określonymi kryteriami w celu określenia znaczenia ryzyka
„**podatność**” - słabość zasobu lub grupy zasobów, która może być wykorzystana przez zagrożenie,
„**polityka bezpieczeństwa**” - zestaw praw, reguł i praktycznych doświadczeń regulujących sposób zarządzania, ochrony i dystrybucji informacji wrażliwej wewnątrz określonego systemu,
„**poufność**”– właściwość wskazująca, że informacja nie jest udostępniana lub wyjawiana nieupoważnionym osobom, podmiotom lub procesom [ISO/IEC 13335-1:2004],
„**rozliczalność**” - właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi (ISO 7498-2:1989),
„**ryzyko**” - prawdopodobieństwo, że określone zagrożenie wykorzysta podatność zasobu lub grupy zasobów, aby spowodować straty lub zniszczenie zasobów
„**System Zarządzania Bezpieczeństwem Informacji (SZBI)** - z ang. ISMS (Information Security Management System) - część całościowego systemu zarządzania oparta na podejściu wynikającym z ryzyka biznesowego, odnosząca się do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia bezpieczeństwa informacji
„**szacowanie ryzyka**” - szacowanie zagrożeń, ich wpływu, podatności informacji i urządzeń do przetwarzania informacji oraz prawdopodobieństwa ich wystąpienia,
„**zabezpieczenie**” - praktyka, procedura lub mechanizm redukujący ryzyko,
„**zagrożenie**” - potencjalna przyczyna niepożądanego incydentu, którego skutkiem może być szkoda dla systemu lub instytucji,
„**zdarzenie związane z bezpieczeństwem informacji**” - jest określonym stanem systemu, usługi lub sieci, który wskazuje na możliwe przełamanie polityki bezpieczeństwa informacji, błąd zabezpieczenia lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem.

4. Opis działania

4.1. Role i odpowiedzialność za bezpieczeństwo informacji/Upoważnienia

4.1.1. Zarząd odpowiada za nadawanie i anulowanie upoważnień do przetwarzania danych w zbiorach papierowych, systemach informatycznych. Każda osoba upoważniona musi przetwarzać dane wyłącznie na polecenie Zarządu.

4.1.2. Uprawnienia nadawane do zbiorów na wniosek kierowników działów wysłanych pocztą elektroniczną e-mail.

4.1.3. Osoby obecnie zatrudnione podpisują oświadczenia o poufności danych w dziale Kadr Osoba oświadczenia o poufności danych zobowiązuję się do:

- przetwarzania danych wyłącznie w zakresie i celu przewidzianym w powierzonych przez Zarząd zadaniach
- zachowania w tajemnicy danych do których mam lub będę miał/a dostęp w związku z wykonywaniem zadań powierzonych przez Zarząd
- niewykorzystywania danych w celach niezgodnych z zakresem i celem powierzonych zadań przez Zarząd
- zachowania w tajemnicy sposobów zabezpieczenia danych
- ochrony danych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją danych, nieuprawnionym ujawnieniem danych, nieuprawnionym dostępem do danych oraz przetwarzaniem.

4.2. Procedura napraw w serwisach zewnętrznych

- W przypadku naprawy sprzętu z danymi na nośniku - rekomendowane jest przekazywanie do naprawy uszkodzonego sprzętu z danymi zaszyfrowanymi na dysku / karcie pamięci. Sprzęt przekazywany jest do serwisu bez podania hasła
- Rekomendowane jest korzystanie z serwisu, który dokonuje napraw u klienta (umowy gwarancyjne on-site)

4.3. Opis zdarzeń naruszających ochronę danych

Podział zagrożeń:

1) zagrożenia losowe zewnętrzne (np. klęski żywiołowe, przerwy w zasilaniu), ich występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu, ciągłość systemu zostaje zakłócona - nie dochodzi do naruszenia poufności danych;

2) zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki operatorów, administratora, awarie sprzętowe, błędy oprogramowania), może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu - może nastąpić naruszenie poufności danych;

3) zagrożenia zamierzone, świadome i celowe - najpoważniejsze zagrożenia, naruszenia poufności danych, (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy), zagrożenia te możemy podzielić na:

- nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu),
- nieuprawniony dostęp do systemu z jego wnętrza,
- nieuprawniony przekaz danych,
- pogorszenie jakości sprzętu i oprogramowania,
- bezpośrednie zagrożenie materialnych składników systemu.
- przechwycenie sygnałów na skutek zjawiska interferencji
- szpiegostwo zdalne
- podsłuch
- kradzież nośników lub dokumentów lub urządzenia
- odtworzenie z powtórnie wykorzystanych lub wyrzuconych nośników
- ujawnienie
- manipulowanie urządzeniem
- sfałszowanie oprogramowania

Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są dane to głównie:

1) sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.;

2) niewłaściwe parametry środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych;

3) awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie serwisu, a w tym sam fakt pozostawienia serwisantów bez nadzoru;

4) pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu;

5) jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie;

6) nastąpiło naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie,
7) stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji);
8) nastąpiła niedopuszczalna manipulacja danymi w systemie;
9) ujawniono osobom nieupoważnionym dane lub objęte tajemnicą procedury ochrony przetwarzania albo inne strzeżone elementy systemu zabezpieczeń;
10) praca w systemie lub jego sieci komputerowej wykazuje nieprzypadkowe odstępstwa od założonego rytmu pracy wskazujące na przełamanie lub zaniechanie ochrony danych - np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu, itp.;
11) ujawniono istnienie nieautoryzowanych kont dostępu do danych lub tzw. "bocznej furtki", itp.;
12) podmieniono lub zniszczono nośniki z danymi bez odpowiedniego upoważnienia lub w sposób niedozwolony skasowano lub kopiowano dane
13) rażąco naruszono dyscyplinę pracy w zakresie przestrzegania procedur bezpieczeństwa informacji, tj. nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych w drukarce, na ksero, nie zamknięcie pomieszczenia z komputerem, nie wykonanie w określonym terminie kopii bezpieczeństwa, prace na danych w celach prywatnych, itp. Za naruszenie ochrony danych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania danych, w tym także (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych, tj. na papierze (wydrukach), kliszy, folii, zdjęciach, dyskietkach, pendrive, czy przenośnych dyskach HD w formie niezabezpieczonej itp.

4.4. Bezpieczeństwo fizyczne w obszarach przetwarzania danych

4.4.1. W zakresie ochrony fizycznej należy rozważyć wyznaczenie obszarów bezpiecznych oraz podział na strefy w zależności od ich dostępności zarówno dla personelu, jak oraz przedstawicieli podmiotów współpracujących.
Podział na strefy umożliwia dobór stosowanych zabezpieczeń fizycznych:
1. Identyfikatory gości
2. System kontroli dostępu,
3. Zarządzanie kluczami tradycyjnymi–wszystkie klucze powinny być przechowywane w zabezpieczonym miejscu, do którego dostęp mają wyłącznie osoby upoważnione,
5. Systemy przeciwwłamaniowe,
7. Służba ochrony całodobowa
8. Systemy przeciwpożarowe lub gaśnice,

4.4.2. Zabezpieczenia na poziomie wysokim w zakresie bezpieczeństwa fizycznego, powinny zapewniać co najmniej aby:
1. Obszar, w którym przetwarzane są dane, zabezpieczony był przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych
2. Przebywanie osób nieuprawnionych w obszarze, w którym przetwarza się dane, było dopuszczalne za zgodą administratora danych lub w obecności osoby upoważnionej do przetwarzania danych
3. Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych jest w czasie nieobecności zatrudnionych tam pracowników nadzorowany przez służbę ochrony.
4. Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych przez cała dobę jest nadzorowany przez służbę ochrony.
5. Zbiór danych w postaci papierowej przechowywany jest w zamkniętej

szafie.
6. Kopie zapasowe/archiwalne zbioru danych przechowywane są w zamkniętej szafie, sejfie lub półkach zamkniętej serwerowni
7. Pomieszczenie, w którym przetwarzane są zbiory danych zabezpieczone jest przed skutkami pożaru za pomocą systemu przeciwpożarowego i/lub wolnostojącej gaśnicy.
8. Dokumenty zawierające dane po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.

4.4.3. Fizyczne zabezpieczenie wejść

a. rejestrowanie daty i godziny wejścia i wyjścia gości przez ochronę, sekretariat, nadzorowanie ich pobytu w obszarach bezpiecznych, chyba że ich dostęp został wcześniej zaakceptowany;
b. ograniczenia dostępu do obszarów, gdzie są przetwarzane lub przechowywane informacje poufne tylko dla uprawnionego personelu, poprzez wdrożenie właściwych zabezpieczeń dostępu,
c. prowadzenia, bezpiecznego przechowywania i nadzorowania, książki rejestracji gości lub elektronicznego śladu, w których na potrzeby audytu umieszczane są zapisy wszystkich wejść;
d. przyznawania personelowi pomocniczemu reprezentującemu podmiot zewnętrzny ograniczonego dostępu do obszarów bezpiecznych lub środków przetwarzania informacji poufnych tylko wtedy, gdy jest to wymagane; autoryzowanie i monitorowanie takiego dostępu;
e. regularnego przeglądania praw dostępu do obszarów bezpiecznych i, jeśli zachodzi taka potrzeba, uaktualniania ich lub odbierania.

4.4.4. Praca w obszarach przetwarzania danych

Zaleca się uświadomienie personelu w zakresie istnienia obszaru bezpiecznego oraz prowadzonych w nim działań zgodnie z zasadą wiedzy koniecznej. W obszarach przetwarzania danych prace wykonywane przez osoby nieupoważnione powinny być prowadzone wyłącznie pod nadzorem z powodów bezpieczeństwa, jak i z uwagi na uniemożliwienie złośliwych działań.

4.5. Inwentaryzacja i zabezpieczenie sprzętu

4.5.1 Informatyk wykonuje i prowadzi na bieżąco inwentaryzację sprzętu wykorzystywanego do przetwarzania informacji mogących stanowić dane (inwentaryzacja zasobów informatycznych) oraz oprogramowania. Inwentaryzacja sprzętu komputerowego prowadzona jest w systemie finansowo-księgowym FK Ferrodo środki trwałe przez księgowość, nadto ewidencja wydań/zdań notebooków i telefonów komórkowych prowadzone na zlecenie zarządu przez wyznaczonego pracownika.

4.5.2. Celem zabezpieczenia sprzętu jest zapobieżenie utracie, uszkodzeniu, kradzieży lub utracie integralności aktywów oraz zakłóceniom w działaniu organizacji. Zaleca się umieszczenie i ochronę sprzętu w taki sposób, aby zminimalizować ryzyka wynikające z zagrożeń i niebezpieczeństw środowiskowych oraz okazje do nieuprawnionego dostępu.

4.5.3. W celu ochrony sprzętu zaleca się rozważenie ulokowania sprzętu w taki sposób, aby zminimalizować niepotrzebny dostęp do obszarów pracy, takiego ulokowania środków przetwarzania wrażliwych informacji, aby podczas ich użycia minimalizować ryzyko podglądu przez nieuprawnione osoby, urządzenia przechowujące informacje powinny być zabezpieczone w sposób uniemożliwiający nieuprawniony dostęp, wprowadzenie zabezpieczeń minimalizujących ryzyko związane z potencjalnymi zagrożeniami fizycznymi i środowiskowymi, np. kradzieżą, pożarem, środkami wybuchowymi, dymem, zalaniem (lub

awarią zaopatrzenia w wodę), kurzem, wibracjami, środkami chemicznymi, interferencjami linii zasilających, linii komunikacyjnych, promieniowaniem elektromagnetycznym i wandalizmem. Zaleca się wprowadzenie procedur związanych ze spożywaniem posiłków, napojów oraz paleniem tytoniu w bliskim sąsiedztwie środków przetwarzania informacji.

4.5.4. Strefy przetwarzania danych, przede wszystkim serwerownie powinny być monitorowe pod względem takich warunków środowiska, jak temperatura i wilgotność, w celu wykrycia ich niekorzystny wpływ na działanie środków przetwarzania informacji. Zaleca się wyposażenie wszystkich budynków w instalację odgromową oraz stosowania filtrów odgromowych na liniach zasilających i komunikacyjnych.

4.6. Bezpieczeństwo okablowania

4.6.1. Zaleca się, aby okablowanie zasilające i telekomunikacyjne, przenoszące dane lub wspomagające usługi informacyjne, było chronione przed przechwyceniem, zakłóceniem lub uszkodzeniem.

4.6.2. W kwestii bezpieczeństwa okablowania zaleca się rozważenie wdrożenia tam, gdzie jest to możliwe, prowadzenie linii zasilających i telekomunikacyjnych do środków przetwarzania informacji pod ziemią lub zabezpieczenie ich w inny stosowny sposób, oddzielenie kabli zasilających od okablowania komunikacyjnego w celu uniknięcia interferencji.

4.6.3. Zaleca się aby dla systemów wrażliwych lub krytycznych rozważyć dodatkowe zabezpieczenia obejmujące instalację zbrojonych rur kablowych i zamykanych pomieszczeń lub szafek w punktach kontrolnych i zakończeń, korzystanie z ekranów elektromagnetycznych do ochrony kabli, prowadzanie przeglądów technicznych oraz fizycznych inspekcji pod kątem nieautoryzowanych urządzeń podłączonych do kabli oraz kontrolowanie dostępu do paneli połączeniowych i pomieszczeń z okablowaniem.

4.7. Konserwacja sprzętu komputerowego

4.7.1. W celu zapewnienia ciągłej dostępności i integralności sprzętu zaleca się jego prawidłową konserwację zgodnie z zaleceniami dostawcy, w zakresie częstotliwości i zakresu, naprawianie lub serwisowanie sprzętu tylko przez autoryzowany personel.

4.7.2. Zaleca się wdrożenie odpowiednich zabezpieczeń na czas czynności konserwacyjnych, z uwzględnieniem działań przeprowadzanych przez personel na miejscu lub poza siedzibą organizacji; jeśli zachodzi taka potrzeba, usuwanie poufnych informacji ze sprzętu lub nadanie personelowi utrzymującemu odpowiednich uprawnień, zapewnienie zgodności z wszystkimi wymaganiami dotyczącymi konserwacji, nakładanymi przez polisy ubezpieczeniowej. Należy pamiętać o skontrolowaniu urządzenia przed jego ponownym uruchomieniem, po przeprowadzeniu jego konserwacji, w celu zapewnienia, że sprzęt nie został zmanipulowany i nie realizuje szkodliwych funkcji.

4.8. Wynoszenie aktywów poza siedzibę organizacji

4.8.1. Zaleca się rozważenie zabezpieczeń w postaci wskazania pracowników i użytkowników reprezentujących podmioty zewnętrzne, którzy mają prawo wynoszenia aktywów, jeśli to potrzebne i właściwe, rejestrowanie kiedy aktywa są wynoszone i kiedy są zwracane, dokumentowanie tożsamości, stanowiska i przynależności każdego, kto obsługuje lub wykorzystuje aktywa oraz zwrotu tej dokumentacji z urządzeniem, informacją lub oprogramowaniem.

4.8.2. Wyrywkowe kontrole, podejmowane w celu wykrycia aktywów wynoszonych bez zezwolenia, mogą być też wykorzystywane do wykrycia nieautoryzowanych urządzeń rejestrujących oraz chronić przed ich wniesieniem lub wyniesieniem z siedziby. Zaleca się przeprowadzanie takich kontroli zgodnie z odpowiednimi przepisami prawa i regulacjami. Jeśli kontrole są przeprowadzane, to należy o nich poinformować, a ich wykonanie autoryzować zgodnie z wymaganiami prawa i regulacjami.

4.9. Bezpieczeństwo sprzętu i aktywów poza siedzibą - urządzenia mobilne i telepraca

4.9.1. Zaleca się zabezpieczenie aktywów wynoszonych poza siedzibę organizacji przed wystąpieniem różnych ryzyk związanych z pracą poza siedzibą.

4.9.2. W kwestii ochrony sprzętu znajdującego się poza siedzibą, zaleca się nie pozostawiać w miejscach publicznych bez nadzoru urządzeń lub nośników wynoszonych poza siedzibę, przestrzegać instrukcji producenta dotyczących ochrony sprzętu, np. ochrony przed wystawieniem na działanie silnego pola elektromagnetycznego.

4.9.3. Zaleca się stosować odpowiednie zabezpieczenia określone w czasie procesu szacowania ryzyka, niezbędne podczas pracy poza siedzibą, np. w domu, pracując zdalnie, w tymczasowych lokalizacjach, takie jak zamykane szafki, polityka czystego biurka, zabezpieczenia dostępu do komputerów oraz bezpieczne połączenie z biurem. Ważnym elementem jest dokumentacja, w której odnotowywany jest łańcuch posiadaczy odpowiedzialnych za sprzęt, w tym co najmniej ich dane oraz nazwy organizacji, jeśli sprzęt znajdujący się poza siedzibą jest przenoszony pomiędzy różnymi osobami lub podmiotami zewnętrznymi.

4.9.5. Zaleca się, aby wybierając właściwe zabezpieczenia uwzględnić fakt, że ryzyka np. uszkodzeń, kradzieży lub podsłuchu, mogą znacząco różnić się w zależności od miejsca. W przypadku wystąpienia ryzyka kradzieży, utraty sprzętu na którym przechowywane są istotne dane np. dane wrażliwe, informacje na sprzęcie powinny być przechowywane w formie zaszyfrowanej. Nie niweluje to ryzyka kradzieży ale uniemożliwia dostęp do informacji osobom nieuprawnionym w przypadku utraty kontroli nad urządzeniem.

4.9.6. Zaleca się wprowadzenie polityki oraz wspierających ją zabezpieczeń w celu zarządzania ryzykami wynikającymi z użytkowania urządzeń mobilnych.
a) rejestrację urządzeń mobilnych;
b) wymagania dotyczące ochrony fizycznej;
c) ograniczenia instalacji oprogramowania;
d) wymagania dotyczące wersji oprogramowania urządzenia mobilnego i stosowania uaktualnień;
e) ograniczenia w połączeniach do usług informacyjnych;
f) kontrolę dostępu;
g) techniki kryptograficzne;
h) ochronę przed szkodliwym oprogramowaniem;
i) zdalne wyłączanie, usuwanie danych lub blokowanie;

j) kopie zapasowe;
k) korzystanie z usług internetowych i aplikacji internetowych

4.9.7. Zaleca się zachowanie ostrożności podczas korzystania z urządzeń mobilnych w miejscach publicznych, salach konferencyjnych i innych niezabezpieczonych obszarach. Zaleca się stosowanie środków ochrony, aby uniknąć nieautoryzowanego dostępu do tych urządzeń lub ujawnienia informacji przechowywanych i przetwarzanych przez te urządzenia, na przykład poprzez zastosowanie technik kryptograficznych i wymuszanie wykorzystania poufnych informacji uwierzytelniających.

4.9.8. Zaleca się również fizycznie zabezpieczenie urządzeń mobilnych przed kradzieżą, zwłaszcza pozostawionych na przykład w samochodach oraz innych środkach transportu, pokojach hotelowych, centrach konferencyjnych i miejscach spotkań. Na okoliczność kradzieży lub utraty urządzeń mobilnych zaleca się opracowanie odpowiedniej procedury uwzględniającej prawne, ubezpieczeniowe i inne wymagania związane z bezpieczeństwem organizacji. Nie zaleca się pozostawiania urządzeń zawierających ważne, wrażliwe lub krytyczne informacje biznesowe bez nadzoru i w miarę możliwości zaleca się fizyczne ich zablokowanie lub zastosowanie specjalnych zamknięć.

4.10. Bezpiecznie zbywanie lub przekazywanie do ponownego użycia

4.10.1. Przed zbyciem lub przekazaniem sprzętu do ponownego użycia zaleca się sprawdzanie wszystkich jego składników zawierających nośniki informacji, dla zapewnienia, że wszystkie wrażliwe dane i licencjonowane programy zostały usunięte lub bezpiecznie nadpisane.

4.10.2. Zaleca się aby nośniki danych były usuwane z urządzeń zbywanych lub przekazywanych do ponownego użycia. Zaleca się fizyczne niszczenie nośników informacji zawierających informacje wrażliwe lub chronione prawem autorskim; zamiast standardowego kasowania lub formatowania zaleca się zniszczenie, skasowanie lub nadpisanie informacji za pomocą technik uniemożliwiających ich odtworzenie.

4.10.3. Uszkodzone urządzenia zawierające nośniki informacji mogą wymagać szacowania ryzyka określającego, czy należy je fizycznie zniszczyć, wysłać do naprawy, czy też wyrzucić. Nieostrożne zbycie lub przekazanie urządzenia do ponownego użycia może bowiem spowodować nieautoryzowane ujawnienie informacji.

4.10.4. Gdy sprzęt jest usuwany lub przeznaczony do ponownego użycia, to w celu zmniejszenia ryzyka ujawnienia poufnych informacji można zastosować dodatkowo, zamiast bezpiecznego wyczyszczenia dysku, jego zaszyfrowanie, pod warunkiem że proces szyfrowania jest wystarczająco silny i obejmuje cały dysk (w tym przestrzeń nieużywaną, pliki wymiany itp.), klucze szyfrowania są wystarczająco długie, aby zapewnić odporność na ataki wyczerpujące, same klucze szyfrowania są poufne (np. nigdy nie są przechowywane na tym samym dysku).

4.10.5. Techniki bezpiecznego nadpisywania nośników informacji różnią się w zależności od technologii tych nośników. Zaleca się przeglądanie narzędzi nadpisywania w celu upewnienia się, że mogą mieć one zastosowanie do danej technologii nośnika informacji.

4.10.6. Zaleca się, aby użytkownicy zapewniali odpowiednią ochronę sprzętu pozostawianego bez opieki. Zaleca się, aby wszyscy użytkownicy byli świadomi wymagań i procedur ochrony wyposażenia pozostawianego bez opieki, jak również odpowiedzialności związanej z wdrożeniem tej ochrony. Zaleca się użytkownikom, aby:

a) zamykali aktywne sesje po zakończeniu pracy, chyba że są one zabezpieczane przez odpowiedni mechanizm blokujący, np. wygaszacz ekranu chroniony hasłem;
b) wyrejestrowywali się z aplikacji lub usług sieciowych, kiedy nie są już więcej potrzebne;
c) zabezpieczali nieużywane w danym momencie komputery osobiste lub urządzenia mobilne przed nieupoważnionym dostępem poprzez blokadę klawiatury lub w inny równoważny sposób, np. dostęp do komputera po podaniu hasła.

4.11. Polityka czystego biurka i czystego ekranu

4.11.1. Zaleca się wprowadzenie polityki czystego biurka dla dokumentów papierowych i przenośnych nośników pamięci oraz polityki czystego ekranu dla środków przetwarzania informacji.
4.11.2. Zaleca się, aby polityka czystego biurka i czystego ekranu brała pod uwagę klasyfikację informacji, wymagania prawne i umowne oraz odpowiednie rodzaje ryzyka i uwarunkowania kulturowe organizacji.
Zaleca się rozważenie wprowadzenia następujących rozwiązań organizacyjnych:
a) przechowywania pod zamknięciem (najlepszym rozwiązaniem jest sejf, szafa lub inna forma zabezpieczenia) nieużywanych, wrażliwych lub krytycznych informacji biznesowych, np. umieszczonych na nośnikach elektronicznych lub w postaci dokumentów papierowych, szczególnie jeśli pomieszczenie biurowe jest opuszczane;
b) zamykania sesji lub blokowanie komputerów i terminali pozostawionych bez opieki za pomocą mechanizmu blokowania ekranu i klawiatury zabezpieczanego hasłem, tokenem lub z użyciem innego podobnego mechanizmu uwierzytelnienia użytkownika; ochrony komputerów i terminali mechanicznym zamkiem, hasłem lub za pomocą innego zabezpieczenia jeśli nie są używane;
c) wprowadzenia zakazu korzystania z kopiarek lub innych technik kopiowania (np. skanerów, aparatów cyfrowych) bez autoryzacji;
d) niezwłoczne usuwanie z drukarek wydruków zawierających wrażliwe lub klasyfikowane informacje.
Polityka czystego biurka i czystego ekranu ogranicza ryzyko nieautoryzowanego dostępu, utraty lub uszkodzenia informacji w czasie normalnych godzin pracy i poza normalnymi godzinami pracy. Ponadto, sejfy lub inne formy bezpiecznych urządzeń przechowujących mogą chronić przechowywane informacje przed takimi katastrofami, jak: pożar, trzęsienie ziemi, zalanie czy eksplozja.
Należy rozważyć korzystanie z drukarek chronionych cyfrowym kodem osobistym (PIN), aby tylko właściciele wydruku mogli otrzymać swoją kopię i tylko wtedy, gdy stoją obok drukarki.

4.12. Bezpieczeństwo systemów informatycznych i danych . Kopie zapasowe

4.12.1. W systemie informatycznym służącym do przetwarzania danych zastosowane były mechanizmy kontroli dostępu do tych danych, a w przypadku, kiedy dostęp do danych przetwarzanych w systemie informatycznym posiadają co najmniej dwie osoby, zapewnione było, aby:
a) w systemie tym rejestrowany był dla każdego użytkownika odrębny identyfikator;
b) dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia.
Jednocześnie zapewnić należy aby identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie mógł być przydzielony innej osobie.

W przypadku gdy do uwierzytelniania użytkowników do systemów operacyjnych komputera lub serwera używa się hasła, jego zmiana następuje
nie rzadziej niż co 30 dni. Hasło składa się co najmniej z 8 znaków, zawiera małe i wielkie litery

oraz cyfry lub znaki specjalne.

4.12.2. System informatyczny służący do przetwarzania danych zabezpieczony był, w szczególności przed:
a) działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego;
b) utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.

4.12.3. Zaleca się ustanowienie polityki kopii zapasowych, określającej wymagania organizacji w zakresie zapasowych kopii informacji, oprogramowania i systemów.
Zaleca się, aby polityka kopii zapasowych definiowała wymagania w zakresie retencji i ochrony. W celu zapewnienia, że wszystkie niezbędne informacje i oprogramowanie można będzie odzyskać po katastrofie lub awarii nośników zaleca się dostarczenie odpowiednich urządzeń do kopii zapasowych.
Podczas opracowywania planu kopii zapasowych zaleca się:
a) utworzenie dokładnego i kompletnego spisu kopii zapasowych oraz procedur odtwarzania;
b) aby zakres (np. pełny lub przyrostowy) i częstotliwość kopii zapasowych odzwierciedlały wymagania biznesowe organizacji, wymagania związane z bezpieczeństwem informacji oraz krytyczność informacji dla ciągłości działalności organizacji;
c) przechowywanie kopii zapasowych w odległości pozwalającej uniknąć uszkodzeń spowodowanych katastrofą, która dotknęła ośrodek podstawowy
d) odpowiednie fizyczne zabezpieczenie kopii zapasowych oraz zabezpieczenie ich przed wpływem środowiska
e) testowanie nośników kopii zapasowych, aby można było na nich polegać w przypadku awaryjnego odtwarzania; zaleca się łączenie powyższego z testami procedur odtwarzania i sprawdzaniem wymaganego czasu odtworzenia. Badanie zdolności do przywracania danych z kopii zapasowej zaleca się wykonać na dedykowanych testowych nośnikach, a nie poprzez nadpisanie oryginalnego nośnika, gdyby utworzenie kopii zapasowej lub przywrócenie danych nie powiodło się i spowodowało nieodwracalne uszkodzenie lub utratę danych;
f) w sytuacjach, gdy ważna jest poufność, szyfrowanie kopii zapasowych.
Zaleca się, aby procedury utrzymaniowe monitorowały wykonywanie kopii zapasowych i kierowały błędy w tym zakresie do obsługi, w celu zapewnienia kompletności kopii zapasowych zgodnie z polityką kopii zapasowych.
Zaleca się regularne testowanie planów kopii zapasowych pojedynczych systemów i usług, aby spełniały wymagania planów ciągłości działania. W przypadku systemów i usług krytycznych zaleca się, aby plany te obejmowały wszystkie informacje systemowe, aplikacje oraz dane niezbędne do odtworzenia całego systemu na wypadek awarii.

4.12.4. Dane przetwarzane w systemie informatycznym zabezpieczone muszą być przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych. Kopie zapasowe muszą być:
a) przechowywane w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem;
b) przechowywane jeżeli to możliwe w formie zaszyfrowanej;
c) usuwane niezwłocznie po ustaniu ich użyteczności.

4.12.5. Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:
a) likwidacji - muszą zostać pozbawione wcześniej zapisu tych danych, a w przypadku

gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;
b) przekazania podmiotowi nieuprawnionemu do przetwarzania danych - muszą zostać pozbawione wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;
c) naprawy — powinny zostać pozbawione wcześniej zapisu tych danych, jeżeli to jest możliwe, w sposób uniemożliwiający ich odzyskanie

4.12.6. Systemy informatyczne służące do przetwarzania danych muszą być chronione przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem. W przypadku zastosowania logicznych zabezpieczeń, o których mowa powyżej, muszą one obejmować:
a) kontrolę przepływu informacji pomiędzy systemem informatycznym administratora danych a siecią publiczną;
b) kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego administratora danych.

4.12.7. Administrator danych musi stosować środki kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej, które uniemożliwiają uzyskanie dostępu do danych przez osoby nieuprawnione nawet w przypadku, gdy zostaną one przez nie przejęte.

4.12.8. Osoba użytkująca komputer przenośny zawierający dane musi zachowywać szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem, w którym dane są przetwarzane, w tym muszą zostać zastosowane środki ochrony kryptograficznej wobec przetwarzanych danych.

4.12.9. Urządzenia i nośniki zawierające dane, przekazywane poza obszar, w którym dane są przetwarzane, zabezpiecza się w sposób zapewniający poufność i integralność tych danych m.in. poprzez przechowywanie ich na tych urządzeniach i nośnikach w formie zaszyfrowanej.

4.12.10. Standardem jest stosowanie wygaszaczy ekranowych ze zwłoką czasową oraz koniecznością wprowadzenia hasła przy wznowieniu pracy w systemie informatycznym.

4.12.11. Dobrą praktyka jest okresowy przegląd uprawnień i identyfikatorów użytkowników, który może być realizowany przez porównanie anulowanych upoważnień z kontami aktywnymi w systemie informatycznym. Przegląd taki należy wykonywać regularnie, co najmniej raz w roku. Przegląd taki może być częścią sprawdzenia prowadzonego przez administratora bezpieczeństwa informacji.

4.13. Procedura niszczenia danych na nośnikach elektronicznych

4.13.1. W odniesieniu do nośników przenośnych oraz nośników danych zainstalowanych w komponentach informatycznych – złomowanych stosowane są mechanizmy bezpiecznego kasowania informacji:

- za pomocą specjalistycznego oprogramowania
- przy użyciu demagnetyzacji
- poprzez fizyczne niszczenie (pocięcie, spalenie) nośników

Wyznaczony administrator dokonuje kontroli prawidłowości usunięcia informacji.
4.12.2. Nośniki usuwalne, które nie mogą być ponownie wykorzystane, są niszczone.
Za właściwe skasowanie informacji zawartej na nośniku przenośnym lub w pamięci masowej stacji roboczej odpowiada użytkownik.

Za kasowanie informacji z pamięci masowych serwerów oraz nośników kopii archiwalnych i zapasowych odpowiada informatyk

4.15. Zasady korzystania z Internetu

4.15.1. Użytkownik zobowiązany jest do korzystania z internetu wyłącznie w celach służbowych. Zabrania się zgrywania na dysk twardy komputera oraz uruchamiania jakichkolwiek programów nielegalnych oraz plików pobranych z niewiadomego źródła. Pliki takie powinny być ściągane tylko za każdorazową zgodą osoby upoważnionej do administrowania infrastrukturą IT i tylko w uzasadnionych przypadkach.

4.15.2. Zabrania się wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, hackerskim, pornograficznym, lub innym zakazanym przez prawo (na większości stron tego typu jest zainstalowane szkodliwe oprogramowanie infekujące w sposób automatyczny system operacyjny komputera szkodliwym oprogramowaniem).

4.15.3. Nie należy w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł. W przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, należy zwracać uwagę na pojawienie się odpowiedniej ikonki (kłódka) oraz adresu www rozpoczynającego się frazą ”https:”. Dla pewności należy „kliknąć” na ikonkę kłódki i sprawdzić, czy właścicielem certyfikatu jest wiarygodny właściciel.

4.15.4. Należy zachować szczególną ostrożność w przypadku podejrzanego żądania lub prośby zalogowania się na stronę (np. na stronę banku, portalu społecznościowego, e-sklepu, poczty mailowej) lub podania naszych loginów i haseł, PIN-ów, numerów kart płatniczych przez Internet. Szczególnie tyczy się to żądania podania takich informacji przez rzekomy bank.

4.16. Zasady korzystania z poczty elektronicznej

4.16.1. Przesyłanie danych z użyciem maila poza organizację może odbywać się tylko przez osoby do tego upoważnione.

4.16.2. W przypadku przesyłania danych poza organizację zaleca się wykorzystywać mechanizmy kryptograficzne (hasłowanie wysyłanych dokumentów lub plików zzipowanych, lub podpis elektroniczny)

4.16.3. W przypadku zabezpieczenia plików hasłem, obowiązuje minimum 12 znaków: duże i małe litery i cyfry lub znaki specjalne a hasło należy przesłać odrębnym mailem lub inną metodą, np. telefonicznie lub SMS-em.

4.16.4. Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu. Zaleca się, aby użytkownik podczas przesyłania danych mailem zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata

4.16.5. Nie należy otwierać załączników (plików) w mailach nawet od rzekomo znanych nam nadawców bez weryfikacji tegoż nadawcy. Tego typu maile większości przypadków zawierają załączniki ze szkodliwymi programami, które po „kliknięciu” infekują komputer użytkownika oraz często pozostałe komputery w sieci. W wyniku działania takiego szkodliwego oprogramowania może dojść do poważnych incydentów, łącznie z pełną utratą danych lub zaszyfrowanie przez kryptowirusy.

4.16.6. Bez weryfikacji wiarygodności nadawcy, nie należy „klikać" na hiperlinki w mailach, gdyż mogą to być hiperlinki do stron zainfekowanych lub niebezpiecznych. Użytkownik „klikając" na taki hiperlink bezwiednie infekuje swój komputer oraz często pozostałe komputery w sieci. W wyniku takiej infekcji może dojść do poważnych incydentów, łącznie z pełną utratą danych osobowych lub zaszyfrowanie m przez kryptowirusy

4.16.7. Zakazuje się wysyłania korespondencji służbowej na prywatne skrzynki pocztowe pracowników lub innych osób. Użytkownicy mają prawo korzystać z poczty mailowej dla celów prywatnych wyłącznie okazjonalnie i powinno być to ograniczone do niezbędnego minimum.
Korzystanie z maila dla celów prywatnych nie może wpływać na jakość i ilość świadczonej przez użytkownika pracy oraz na prawidłowe i rzetelne wykonywanie przez niego obowiązków służbowych.

4.16.8. Przy korzystaniu z maila, Użytkownicy mają obowiązek przestrzegać prawa własności przemysłowej, tajemnicy przedsiębiorstwa i prawa autorskiego. Użytkownicy nie mają prawa korzystać z maila w celu rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec powszechnie obowiązujących zasad postępowania

4.16.9. Użytkownik bez zgody Pracodawcy nie ma prawa wysyłać wiadomości zawierających dane dotyczące Pracodawcy / Zleceniodawcy, jego pracowników, klientów, dostawców lub kontrahentów za pośrednictwem Internetu, w tym przy użyciu prywatnej elektronicznej skrzynki pocztowej.

4.16.10. Jeżeli jest to niezbędne do zapewnienia organizacji pracy umożliwiającej pełne wykorzystanie czasu pracy oraz właściwego użytkowania udostępnionych pracownikowi narzędzi pracy, Administrator może wprowadzić kontrolę służbowej poczty elektronicznej pracownika (monitoring poczty elektronicznej).
Monitoring poczty elektronicznej nie może naruszać tajemnicy korespondencji oraz innych dóbr osobistych pracownika.

4.17. Zarządzanie nośnikami wymiennymi

4.17.1. Wytyczne w zakresie zarządzania nośnikami wymiennymi:
a) jeśli zawartość usuwanych z organizacji nośników, które mogą być ponownie użyte, nie jest już potrzebna, zaleca się usunięcie ich w sposób uniemożliwiający ich odtworzenie;
b) tam, gdzie jest to niezbędne i praktyczne, zaleca się autoryzowanie usunięcia nośników z organizacji, a dla potrzeb audytu prowadzenie rejestru takich czynności;
c) zaleca się przechowywanie wszystkich nośników w bezpiecznym środowisku, zgodnie z zaleceniami producenta;
d) jeżeli poufność lub integralność jest istotna, zaleca się wykorzystywane technik kryptograficznych do ochrony danych na nośnikach wymiennych;
e) w celu zmniejszenia ryzyka związanego z pogorszeniem się stanu nośnika, podczas gdy przechowywane dane są nadal potrzebne, zaleca się przeniesienie danych na nowy nośnik, zanim aktualny stanie się nieczytelny;
f) zaleca się przechowywanie na oddzielnych nośnikach wielokrotnych kopii cennych danych w celu zmniejszenia ryzyka przypadkowego zniszczenia danych lub ich utraty;
g) w celu ograniczenia możliwości utraty informacji zaleca się uwzględnienie rejestrowania nośników wymiennych;
h) czytniki nośników wymiennych należy udostępniać tylko w przypadkach uzasadnionych biznesowo;

i) tam, gdzie jest niezbędne użycie nośników wymiennych, zaleca się monitorowanie kopiowania informacji na takie nośniki.

4.18. Dostęp do sieci i usług sieciowych

4.18.1. Zaleca się zapewnienie użytkownikom dostępu wyłącznie do tych sieci i usług sieciowych, do których otrzymali wyraźne uprawnienia:
a) sieci i usługi sieciowe, do których dostęp jest dozwolony;
b) procedury autoryzacji, określające kto jest uprawniony do dostępu do sieci i usług sieciowych;
c) nadzór kierownictwa oraz procedury ochrony dostępu do połączeń sieciowych i usług sieciowych;
d) środki wykorzystywane do realizacji dostępu do sieci lub usług sieciowych (np. używanie VPN lub sieci bezprzewodowych);
e) wymagania uwierzytelnienia użytkownika w celu dostępu do różnych usług sieciowych;
f) monitorowanie korzystania z usług sieciowych.

4.19. Zarządzanie dostępem użytkowników

4.19.1 Zarządzanie identyfikatorami użytkowników

Zaleca się, aby proces zarządzania identyfikatorami użytkowników obejmował:
a) używanie unikatowego identyfikatora użytkownika, aby można było przypisać poszczególnym użytkownikom określone działania oraz odpowiedzialność za nie; zaleca się, aby użycie identyfikatorów grupowych było dozwolone tylko wtedy, gdy uzasadniają to potrzeby biznesowe; ponadto zaleca się, zatwierdzenie i udokumentowanie powyższego;
b) niezwłoczne usuniecie lub zablokowanie identyfikatorów użytkownikom, którzy opuścili organizację
c) okresowe sprawdzanie i usuwanie lub blokowanie zbędnych identyfikatorów użytkowników;
d) zapewnienie, że uprzednio użyty identyfikator nie zostanie przydzielony innemu użytkownikowi.

4.19.2. Nadawanie, odbieranie lub dostosowywanie praw dostępu

4.19.2.1 Przed zatrudnieniem zaleca się zweryfikowanie historii wszystkich kandydatów do pracy, zgodnie z odpowiednimi przepisami prawnymi, regulacjami i zasadami etycznymi oraz proporcjonalnie do wymagań biznesowych, klasyfikacji informacji, do których będzie potrzebny dostęp oraz dostrzeżonych ryzyk.

4.19.2.2. Zaleca się, aby weryfikacja uwzględniała wszystkie istotne przepisy prawne dotyczące prywatności, ochrony danych identyfikujących osobę i zatrudnienia oraz, tam gdzie jest to dozwolone, obejmowała:
a) dostępność satysfakcjonujących referencji, np. jednego świadectwa pracy i jednej referencji osobistej;
b) sprawdzenie (kompletności i dokładności) przedstawionego życiorysu;
c) potwierdzenie deklarowanego wykształcenia i kwalifikacji zawodowych;
d) niezależną weryfikację tożsamości (paszport lub podobny dokument);
e) bardziej szczegółową weryfikację,

4.19.2.3. W przypadku, gdy osoba jest zatrudniana na stanowisko związane z bezpieczeństwem informacji, zaleca się, aby organizacja upewniła się, że kandydat:
a) posiada uprawnienia niezbędne do pełnienia roli związanej z bezpieczeństwem;
b) sprosta powierzonej mu roli, zwłaszcza, gdy jest ona kluczowa dla organizacji.
Jeśli stanowisko zajmowane początkowo lub uzyskane w wyniku awansu wymaga przyznania dostępu do środków przetwarzania informacji, zwłaszcza jeśli przetwarzane są informacje

poufne. Zaleca się, aby procedury określały kryteria i ograniczenia postępowania sprawdzającego, np. kto odpowiada za przeprowadzenie postępowania, jak, kiedy i dlaczego postępowanie sprawdzające jest przeprowadzane.

4.19.2.4. Zaleca się, aby postępowaniu sprawdzającemu byli poddawani także kontrahenci. Zaleca się, aby w tych przypadkach umowa między organizacją a kontrahentem określała odpowiedzialność za przeprowadzenie postępowania sprawdzającego oraz procedury powiadamiania, które należy zastosować, jeśli sprawdzenie nie zostało zakończone lub wyniki postępowania są niepewne lub budzą obawy.
Zaleca się, aby informacje o wszystkich branych pod uwagę kandydatach na stanowiska w organizacji były gromadzone i przetwarzane zgodnie z odpowiednimi przepisami prawa. W zależności od uwarunkowań prawnych zaleca się uprzedzanie kandydatów o przeprowadzaniu postępowania sprawdzającego.

4.19.2.5. Zaleca się, aby w zakresie odpowiedzialności kierownictwa uwzględniono zapewnienie, że pracownicy oraz kontrahenci:
a) są odpowiednio wprowadzani w swoje obowiązki i odpowiedzialność związaną z bezpieczeństwem informacji przed przyznaniem im dostępu do poufnych informacji lub systemów informacyjnych;
b) otrzymują wytyczne określające wymagania w zakresie bezpieczeństwa informacji związane z ich obowiązkami w organizacji;
c) są motywowani do stosowania polityk bezpieczeństwa informacji w organizacji;
d) osiągają poziom świadomości bezpieczeństwa informacji odpowiedni do swoich ról i obowiązków w organizacji
e) wypełniają zalecenia i warunki zatrudnienia, które uwzględniają politykę bezpieczeństwa informacji organizacji oraz właściwe metody pracy;
f) dbają o odpowiednie umiejętności i kwalifikacje i są na bieżąco szkoleni;
g) mają możliwość anonimowego zgłaszania naruszeń polityki bezpieczeństwa informacji lub procedur („anonimowe informowanie”).

4.19.2.6. W chwili zakończenia stosunku pracy zaleca się odebranie lub zawieszenie praw dostępu osoby do informacji oraz aktywów związanych ze środkami przetwarzania informacji i usługami.
Zaleca się, aby zmiany w zatrudnieniu odzwierciedlały odebranie wszystkich praw nieuzasadnionych w związku z nowymi obowiązkami.

4.19.2.7.Zalecane do odebrania lub dostosowania prawa dostępu obejmują dostęp fizyczny i logiczny. Odebranie lub dostosowanie można zrealizować poprzez odebranie lub wymianę kluczy, kart identyfikacyjnych, środków przetwarzania informacji lub subskrypcji.
Zaleca się, aby dokumentacja opisująca prawa dostępu pracowników i kontrahentów odzwierciedlała fakty odebrania lub dostosowania ich praw dostępu. Jeśli odchodzący pracownik lub użytkownik reprezentujący podmiot zewnętrzny zna hasła do kont, które pozostają aktywne, zaleca się zmianę haseł w momencie ustania stosunku pracy, umowy lub porozumienia.

4.19.2.8. Przed zakończeniem lub zmianą zatrudnienia zaleca się ograniczenie lub odebranie praw dostępu do informacji i aktywów związanych ze środkami przetwarzania informacji, na podstawie oceny takich czynników ryzyka, jak:
a) stwierdzenie, czy zakończenie lub zmiana zatrudnienia jest inicjowana przez pracownika, użytkownika reprezentującego podmiot zewnętrzny, czy przez kierownictwo oraz jakie są tego przyczyny;

b) aktualny zakres odpowiedzialności pracownika, użytkownika reprezentującego podmiot zewnętrzny lub każdego innego użytkownika;
c) wartość aktualnie dostępnych aktywów.

4.19.3. Stosowanie poufnych informacji uwierzytelniających

4.19.3.1 Zaleca się opracowanie wskazówek dla wszystkich użytkowników, aby:
a) utrzymywali poufne informacje uwierzytelniające w tajemnicy, w celu zapewnienia, że nie będą ujawnione innym podmiotom, w tym osobom nadzorującym;
b) unikali zapisywania (np. na papierze, w pliku lub urządzeniu przenośnym) poufnych informacji uwierzytelniających, chyba że mogą być one przechowywane w sposób bezpieczny, a metoda przechowywania została zatwierdzona (np. hasła zabezpieczone kryptograficznie);
c) niezwłocznie zmieniali poufne informacje uwierzytelniające, gdy cokolwiek mogłoby wskazywać na możliwość ich ujawnienia;
d) jeśli w charakterze poufnych Informacji uwierzytelniających są stosowane hasła, to należy wybierać hasła dobrej jakości o wystarczającej minimalnej długości, które:
1) nie są łatwe do zapamiętania;
2) nie opierają się na prostych skojarzeniach, łatwych do odgadnięcia lub wywnioskowania z informacji dotyczących danej osoby, np. imiona, numery telefonów, daty urodzenia itp.;
3) nie są podatne na atak słownikowy (tzn. nie zawierają słów zamieszczonych w słownikach);
4) nie zawierają ciągu jednakowych znaków ani grup znaków złożonych z samych cyfr lub samych liter;
5) jeśli są tymczasowe, to są zmieniane przy pierwszym logowaniu;
e) nie współdzielili indywidualnych poufnych informacji uwierzytelniających;
f) zapewnili właściwą ochronę haseł, jeśli są one stosowane, jako poufne informacje uwierzytelniające w zautomatyzowanych procesach logowania i tam przechowywane;
g) nie korzystali z takiego samego hasła w celach biznesowych i niezwiązanych z biznesem.

4.19.3.2 Zaleca się, aby system zarządzania hasłami:
a) wymuszał użycie indywidualnych identyfikatorów użytkownika i haseł, aby zapewnić zachowanie rozliczalności;
b) zezwalał użytkownikom na wybór i zmianę ich własnych haseł oraz zawierał procedurę potwierdzania zmian haseł dla unikania błędów w ich wprowadzaniu;
c) wymuszał wybór haseł odpowiedniej jakości;
d) wymuszał na użytkownikach zmianę ich haseł przy pierwszym logowaniu;
e) wymuszał okresowe zmiany haseł oraz zmiany w razie potrzeby;
f) prowadził spis poprzednio używanych haseł użytkowników oraz zapobiegał ponownemu ich użyciu;
g) uniemożliwiał wyświetlanie haseł na ekranie podczas ich wprowadzania;
h) przechowywał pliki z hasłami w innym miejscu niż dane systemu aplikacji;
i) przechowywał i przesyłał hasła w formie zabezpieczonej.

4.19.4. Procedura bezpiecznego logowania

4.19.4.1. Tam, gdzie polityka kontroli dostępu tego wymaga, zaleca się kontrolowanie dostępu do systemów i aplikacji z zastosowaniem procedury bezpiecznego logowania.
Do potwierdzenia deklarowanej tożsamości użytkownika zaleca się wybranie odpowiedniej techniki uwierzytelnienia.
W przypadku, gdy wymagane jest silne uwierzytelnianie i weryfikacja tożsamości, zaleca się stosowanie alternatywnych do haseł metod uwierzytelniania, takich jak: środki kryptograficzne, karty elektroniczne, tokeny lub środki biometryczne.

4.19.4.2. Zaleca się zaprojektowanie procedury logowania do systemu lub aplikacji w sposób pozwalający minimalizować możliwość nieautoryzowanego dostępu. Z tego względu zaleca się, aby procedura ta ujawniała minimum informacji o systemie lub aplikacji, tak by nie pozwolić nieuprawnionemu użytkownikowi na uzyskanie dodatkowych wskazówek. Zaleca się, aby dobra procedura logowania:
a) nie wyświetlała identyfikatorów systemu lub aplikacji, aż do chwili pomyślnego zakończenia procedury logowania się do systemu;
b) powodowała wyświetlenie ogólnego ostrzeżenia, że dostęp do komputera jest dozwolony jedynie dla uprawnionych użytkowników;
c) nie powodowała wyświetlenia, w trakcie trwania procedury logowania się, komunikatów pomocniczych, które mogłyby pomóc nieuprawnionemu użytkownikowi;
d) zatwierdzała jedynie kompletne informacje wejściowe, niezbędne do zalogowania. Jeżeli wystąpi błąd, to zaleca się, aby system nie wskazywał, która część danych jest poprawna lub niepoprawna;
e) chroniła przed próbami zalogowania się poprzez podanie wszystkich możliwych kombinacji;
f) jeżeli to możliwe, wykonywała zapis nieudanych i udanych prób;
g) generowała zdarzenie związane z bezpieczeństwem, jeśli została wykryta potencjalna próba lub wykryto udane przełamanie zabezpieczeń logowania;
h) wyświetlała następujące informacje po pomyślnym zakończeniu procedury:
1) jeżeli to możliwe - datę i czas ostatniego pomyślnego logowania się do systemu;
2) jeżeli to możliwe - szczegółowe dane dotyczące nieudanych prób logowania się, jakie zdarzyły się od chwili ostatniej udanej próby;
i) jeżeli to możliwe, blokowała wyświetlanie wprowadzanego hasła;
j) jeżeli to możliwe, uniemożliwiała przesyłanie haseł przez sieć tekstem otwartym;
k) jeżeli to możliwe zamykała nieaktywne sesje po określonym czasie nieaktywności, szczególnie w lokalizacjach wysokiego ryzyka, takich jak obszary publiczne lub zewnętrzne poza obszarem zarządzania bezpieczeństwem organizacji lub na urządzeniach mobilnych;
l) ograniczała czas połączenia w celu zapewnienia dodatkowego bezpieczeństwa dla aplikacji wysokiego ryzyka i redukowała możliwość nieautoryzowanego dostępu.

4.19.4.3. Hasła są powszechnym sposobem zapewnienia identyfikacji i uwierzytelnienia opartym na tajemnicy znanej tylko użytkownikowi. To samo można osiągnąć za pomocą metod kryptograficznych i protokołów uwierzytelniających. Zaleca się, aby siła mechanizmu uwierzytelnienia użytkownika była odpowiednia do klasyfikacji informacji, która jest udostępniana.
Jeśli w czasie sesji logowania hasła są transmitowane w sieci tekstem otwartym, to mogą być przechwycone przez sieciowy program typu „sniffer”.

4.20. Zabezpieczenie przed szkodliwym oprogramowaniem
4.20.1. Zaleca się oparcie ochrony przed szkodliwym oprogramowaniem na oprogramowaniu wykrywającym i naprawiającym, na świadomości w zakresie bezpieczeństwa informacji oraz właściwych mechanizmach kontroli dostępu oraz zarządzania zmianami. Zaleca się następujące rekomendacje:
a) zabrania się korzystania z nieautoryzowanego oprogramowania
b) wdrożenie zabezpieczeń wykrywających lub zapobiegających użyciu nieautoryzowanego oprogramowania (np. białe listy aplikacji);
c) wdrożenie zabezpieczeń wykrywających lub zapobiegających użyciu znanych szkodliwych stron webowych lub podejrzewanych o to (np. czarne listy);

d) ustanowienie formalnej polityki ochrony przed ryzykami związanymi z otrzymywaniem plików lub oprogramowania z sieci zewnętrznych albo za pośrednictwem innych mediów, określającej jakie środki ochrony należy wdrożyć;
e) redukowanie podatności, które mogą być wykorzystane przez szkodliwe oprogramowanie, np. poprzez zarządzanie podatnościami technicznymi
f) przeprowadzanie regularnych przeglądów oprogramowania i danych zawartych w systemach obsługujących krytyczne procesy biznesowe; zaleca się przeprowadzenie formalnego dochodzenia w przypadku stwierdzenia obecności niezatwierdzonych plików lub nieautoryzowanych poprawek;
g) zainstalowanie i regularne uaktualnianie oprogramowania do wykrywania oraz usuwania szkodliwego oprogramowania poprzez skanowanie komputerów i nośników informacji, jako zabezpieczenie prewencyjne lub na bieżąco; zaleca się, aby przeprowadzane skanowania obejmowały:
1) skanowanie wszystkich plików odbieranych poprzez sieci lub na innych nośnikach pamięci pod kątem obecności szkodliwego oprogramowania;
2) skanowanie załączników poczty elektronicznej oraz ściąganych danych pod kątem obecności szkodliwego oprogramowania; zaleca się, aby skanowanie prowadzone było w różnych miejscach, np. na serwerach poczty elektronicznej, stacjach roboczych oraz podczas łączenia się z siecią organizacji;
3) sprawdzanie stron internetowych pod kątem obecności szkodliwego oprogramowania;
h) określenie procedur i odpowiedzialności za ochronę systemów przed szkodliwym oprogramowaniem, szkoleń w zakresie stosowania tych mechanizmów, raportowania i odtwarzania po atakach zrealizowanych za pomocą szkodliwego oprogramowania;
i) opracowanie właściwych planów ciągłości działania w celu odtwarzania po ataku szkodliwego oprogramowania, zawierających wszystkie niezbędne dane oraz zestawy procedur związane z wykonywaniem kopii zapasowych oprogramowania i ich odtwarzaniem
j) wdrożenie procedur dotyczących regularnego zbierania informacji, takiego jak subskrypcja list mailowych lub sprawdzanie stron webowych, udostępniających informacje dotyczące szkodliwego oprogramowaniem

4.21. Polityka bezpieczeństwa informacji w relacjach z dostawcami

4.21.1. Zaleca się uzgodnienie z dostawcą i udokumentowanie wymagań związanych z bezpieczeństwem informacji celem zmniejszenia ryzyk związanych z dostępem dostawcy do aktywów organizacji.

4.21.2. Zaleca się, aby organizacja w swojej polityce zidentyfikowała i wdrożyła zabezpieczenia informacji, uwzględniające określony dostęp dostawców do informacji organizacji. Zaleca się, aby zabezpieczenia te uwzględniały procesy i procedury realizowane przez organizację, a także te procesy i procedury, których realizacji organizacja powinna wymagać od dostawcy, w tym:
a) identyfikację i dokumentowanie rodzajów dostawców, np. usługi teleinformatyczne, wsparcie logistyczne, usługi finansowe, informatyczne elementy infrastruktury teleinformatycznej, którym organizacja pozwoli na dostęp do jej informacji;
b) znormalizowany proces i cykl życia zarządzania relacjami z dostawcami;
c) określenie rodzaju dostępu do informacji, do których będą miały uprawnienia różne rodzaje dostawców oraz monitorowanie i kontrolę tego dostępu;
d) minimalne wymagania w zakresie bezpieczeństwa informacji dla każdego rodzaju informacji i rodzaju dostępu, służące jako podstawa dla indywidualnych porozumień z dostawcami w oparciu o potrzeby biznesowe organizacji, wymagania i profil ryzyka;

4.22. Zasady monitoringu wizyjnego

4.22.1. Dla zapewnienia bezpieczeństwa pracowników lub ochrony mienia lub kontroli produkcji lub zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić Administratora na szkodę, wprowadzono szczególny nadzór nad terenem zakładu pracy i terenem wokół zakładu pracy w postaci środków technicznych umożliwiających rejestrację obrazu (monitoring). Monitoring nie obejmuje pomieszczeń sanitarnych, szatni, stołówek.

4.22.2. Nagrania obrazu Administrator przetwarza wyłącznie do celów, dla których zostały zebrane i przechowuje przez okres nieprzekraczający 3 miesięcy od dnia nagrania. Na rejestratorach monitoringu włączona jest opcja nadgrania najstarszych zapisów, okres zapisów zależy od przestrzeni dyskowej rejestratora, trybu zapisu i ilości kamer. W przypadku, w którym nagrania obrazu stanowią dowód w postępowaniu prowadzonym na podstawie prawa lub Administrator powziął wiadomość, iż mogą one stanowić dowód w postępowaniu, termin ulega przedłużeniu do czasu prawomocnego zakończenia postępowania. Po upływie okresów, uzyskane w wyniku monitoringu nagrania obrazu zawierające dane, podlegają zniszczeniu.

4.22.3. Administrator informuje pracowników o wprowadzeniu monitoringu, nie później niż 2 tygodnie przed jego uruchomieniem. Administrator przed dopuszczeniem pracownika do pracy przekazuje mu na piśmie informacje, o prowadzonym monitoringu.

4.22.4. Administrator oznacza pomieszczenia i teren monitorowany w sposób widoczny i czytelny, za pomocą odpowiednich znaków nie później niż jeden dzień przed jego uruchomieniem.

4.23. Plan ciągłości działania na wypadek dysfunkcji systemu informatycznego

4.23.1. Zaleca się, aby organizacja zapewniła, że:

a) istnieje odpowiednia struktura zarządzania, do przygotowywania, zmniejszania skutków oraz reagowania na zdarzenia zakłócające, korzystająca z pracowników posiadających niezbędne uprawnienia, doświadczenie i kompetencje;

b) powołano personel reagujący na incydenty z niezbędnym zakresem obowiązków, uprawnień i kompetencji do zarządzania incydentami i utrzymania bezpieczeństwa informacji

c) opracowano i zatwierdzono udokumentowane plany oraz procedury reagowania i odtwarzania, opisujące szczegółowo, w jaki sposób organizacja będzie zarządzać destrukcyjnymi zdarzeniami i utrzymywać bezpieczeństwo informacji na ustalonym z góry poziomie, na podstawie zatwierdzonych przez kierownictwo celów ciągłości bezpieczeństwa informacji.

Zgodnie z wymaganiami ciągłości bezpieczeństwa informacji zaleca się ustanowienie, udokumentowanie, wdrożenie i utrzymywanie przez organizację:

a) zabezpieczeń informacji w ramach procesów, procedur oraz systemów wspierających i narzędzi ciągłości działania i odzyskiwania po katastrofie;

b) procesów, procedur i zmian w zakresie wdrożenia, w celu utrzymania istniejących zabezpieczeń informacji w czasie niekorzystnej sytuacji;

c) zabezpieczeń kompensujących dla tych zabezpieczeń informacji, które nie mogą być utrzymane w czasie krytycznej sytuacji.

Zaleca się, aby organizacja weryfikowała ustanowione i wdrożone zabezpieczenia ciągłości bezpieczeństwa informacji w regularnych odstępach czasu celem zapewnienia ich aktualności i skuteczności w niekorzystnych sytuacjach.

Zaleca się, aby weryfikować ciągłość zarządzania bezpieczeństwem informacji poprzez:

a) ćwiczenie i testowanie możliwości wykonania procesów, procedur i zabezpieczeń ciągłości bezpieczeństwa informacji w celu zapewnienia, że są one zgodne z celami ciągłości bezpieczeństwa informacji;

b) ćwiczenie i testowanie wiedzy i trybu utrzymania procesów, procedur i zabezpieczeń ciągłości bezpieczeństwa informacji w celu zapewnienia, że ich realizacja jest zgodna z celami ciągłości bezpieczeństwa informacji;
c) przeglądanie poprawności i skuteczności miar ciągłości bezpieczeństwa informacji, gdy podlegają zmianom systemy informatyczne, zabezpieczenia, procesy, procedury związane z bezpieczeństwem informacji lub zarządzanie ciągłością działania/odtwarzaniem po katastrofie.
Został zakupiony nowy serwer do replikacji maszyn wirtualnych, każda maszyna wirtualna zostanie zreplikowana na inną maszynę fizyczną. Mamy kopię zapasową systemu wykonywalną raz dziennie, ponadto raz w tygodnie zostanie wykonana kopia wszystkich maszyn wirtualnych na nowy serwer ftp w osobnym zamkniętym budynku na terenie firmy
4.23.2. Kierownicy działów raz w kwartale prowadzą kontrolę komputerów podległych pracowników - zapisy z kontroli na formularzu: **F1 Ps 4.3./2 Karta stanowiska komputerowego**

l.p.	Funkcja	Opis działań	Potrzebne zasoby
1	Zweryfikować zasadność zgłoszenia od użytkownika	Sprawdzić, czy zgłoszenie dotyczy zdarzenia spowodowanego awarią systemu informatycznego	Zapewnić: dostęp do infrastruktury informatycznej na stanowisku, skąd pochodzi zgłoszenie
2	Ustalić źródła awarii	Ustalić, co jest przyczyną awarii: □ przerwa w zasilaniu prądem, □ brak połączenia z siecią Internet, □ wadliwe działanie sprzętu, □ wadliwe działanie aplikacji, □ wadliwe działanie systemu, na którym uruchomiona jest aplikacji	Zapewnić: □ dostęp do serwerowni oraz do sprzętu, który uległ awarii, □ w przypadku awarii zasilania elektrycznego wezwać pogotowie ENERGETYCZNE-24h
3	Określić skalę awarii	Ustalić, czy awaria powoduje zatrzymanie pracy	Zapewnić: kontakt z kluczowymi pracownikami
4	Ustalić czy wznawianie usługi może odbywać się w dotychczasowej lokalizacji	Działanie ma na celu zweryfikowanie, czy wznawiane usługi uruchamiane będą w dotychczasowej lokalizacji, czy w lokalizacjach alternatywnych.	Zapewnić: □ możliwość uruchomienia dowolnych usług w lokalizacji: □ infrastrukturę sieciową, zasilanie prądem

5	Zakupić niezbędne Elementy wyposażenia, dokonać naprawy (wymiany) urządzeń, uruchomić aplikację	W przypadku braku możliwości zakupu należy znaleźć rozwiązanie alternatywne (np. zdecydować o przeniesieniu aplikacji na stałe na inny serwer).	Zapewnić: środki na zakup elementów niezbędnych do ponownego uruchomienia systemu.
6	Zweryfikować możliwość przeniesienia aplikacji na inny serwer lub komputer	Sprawdzić, czy aplikacja może być uruchomiona na którymś z działających poprawnie komputerów	
7	Przygotować serwer zastępczy,	Jako serwer zastępczy można wykorzystać np. Komputer typu desktop, który należy odpowiednio skonfigurować. Po uruchomieniu aplikacji na serwerze zastępczym należy przetestować jej działanie.	Zapewnić: komputer dowolnego typu, która w podstawowym zakresie pozwoli na uruchomienie podstawowych usług
8	Przywrócić funkcjonowanie aplikacji / system	Spróbować usunąć przyczynę nieprawidłowego działania. W razie konieczności należy odtworzyć aplikację korzystając z kopii zapasowych.	Zapewnić: □ dostęp do najbardziej aktualnej wersji aplikacji, □ dostęp do aktualnej bazy danych.
9	Sprawdzenie aplikacji / Systemu	Po przeniesieniu / uruchomieniu należy zweryfikować prawidłowe funkcjonowanie aplikacji /systemów zainstalowanych na serwerze	Zapewnić: kontakt z kluczowymi pracownikami mogącymi przetestować prawidłowość funkcjonowania systemów i aplikacji.

4.24. Bezpieczeństwo zasobów ludzkich w zakresie ochrony danych osobowych

4.24.1. Zaleca się, aby weryfikacja uwzględniała wszystkie istotne przepisy prawne dotyczące prywatności, ochrony danych identyfikujących osobę i zatrudnienia oraz obejmowała:

a) dostępność świadectwa pracy

b) sprawdzenie (kompletności i dokładności) przedstawionego życiorysu;

c) potwierdzenie deklarowanego wykształcenia i kwalifikacji zawodowych;
d) niezależną weryfikację tożsamości (paszport lub podobny dokument);

4.24.2. Zaleca się, aby zobowiązania wynikające z umowy z pracownikami lub kontrahentami odzwierciedlały politykę ochrony danych w organizacji oraz dodatkowo zawierały wyjaśnienia i deklaracje w zakresie:
a) zaleceń, aby pracownicy którym przyznaje się dostęp do danych informacji poufnych, podpisywali porozumienia o zachowaniu poufności i nieujawnianiu informacji przed uzyskaniem dostępu do środków przetwarzania informacji
b) praw i obowiązków pracowników w odniesieniu do ochrony danych identyfikujących osobę
c) obowiązku klasyfikacji informacji i zarządzania informacjami organizacji, innymi aktywami związanymi z informacją, środkami przetwarzania informacji i usługami informacyjnymi obsługiwanymi przez pracownika
d) odpowiedzialności pracowników w zakresie przetwarzania informacji otrzymywanej z innych firm lub podmiotów zewnętrznych;
e) działań podejmowanych, jeśli pracownik nie przestrzega wymagań Polityki ochrony danych

4.24.3. Zaleca się, aby organizacja zapewniła, że pracownicy oraz kontrahenci akceptują zasady i warunki związane z ochrona danych odpowiednio do rodzaju i zakresu przyznanego im dostępu do aktywów organizacji powiązanych z systemami informacyjnymi.

4.24.4. Zaleca się, aby w zakresie zarzadzania zasobami ludzkimi uwzględniono zapewnienie, że pracownicy:
a) są odpowiednio wprowadzani w swoje obowiązki i odpowiedzialność związaną z bezpieczeństwem informacji i ochroną danych przed przyznaniem im dostępu do poufnych informacji lub systemów informacyjnych;
b) otrzymują wytyczne określające wymagania w zakresie bezpieczeństwa informacji związane z ich obowiązkami w organizacji;
c) są motywowani do stosowania polityki ochrony danych w organizacji;
d) osiągają poziom świadomości bezpieczeństwa informacji i ochrony danych odpowiedni do swoich ról i obowiązków w organizacji
e) wypełniają zalecenia i warunki zatrudnienia, które uwzględniają polityki ochrony danych organizacji oraz właściwe metody pracy;
f) dbają o odpowiednie umiejętności i kwalifikacje i są na bieżąco szkoleni;
g) mają możliwość anonimowego zgłaszania naruszeń polityki ochrony danych („anonimowe informowanie”).

4.24.5. Zaleca się, aby kształcenie i szkolenia w zakresie ochrony danych obejmowało również ogólne aspekty, takie jak:
a) zaangażowanie pracowników w bezpieczeństwo informacji w całej organizacji;
b) potrzebę zapoznania się i przestrzegania stosownych zasad ochrony danych i bezpieczeństwa informacji oraz obowiązków określonych w politykach, normach, przepisach prawnych,
c) osobistą odpowiedzialność pracowników za ich działania i zaniechania oraz ogólne obowiązki w kwestii zabezpieczenia lub ochrony danych
d) podstawowe procedury ochrony danych oraz podstawowe zabezpieczenia (takie, jak bezpieczeństwo haseł, zabezpieczenia przed szkodliwym oprogramowaniem i czyste biurka);
e) dodatkowe informacje i porady w sprawach związanych z ochroną danych i bezpieczeństwem informacji, w tym dalsze kształcenie w zakresie ochrony danych

4.24.6. Zaleca się, aby formalne postępowanie dyscyplinarne zapewniało poprawne i obiektywne traktowanie pracowników, którzy podejrzani są o naruszenie zasad ochrony danych i bezpieczeństwa informacji. Zaleca się stopniowanie postępowania, uwzględnienie takich czynników, jak: rodzaj i waga naruszenia, jego wpływ na biznes, czy jest to pierwsze, czy kolejne naruszenie, czy winny został prawidłowo przeszkolony, właściwe przepisy prawne.
Zaleca się stosowanie procesu dyscyplinarnego jako środka odstraszającego, aby zapobiec naruszaniu przez pracowników polityki ochrony danych organizacji i procedur oraz naruszaniu wszelkich innych zabezpieczeń informacji. Umyślne naruszenie może wymagać natychmiastowego działania.

5. ODPOWIEDZIALNOŚĆ I UPRAWNIENIA

Czynność	Odpowiedzialny
Ustanowienie odpowiedzialności za bezpieczeństwo informacji – upoważnienie do przetwarzania danych osobowych	Prezes
Nadzorowanie umów powierzenia przetwarzania danych osobowych	Prezes
Zabezpieczenie sprzętu do przetwarzania danych osobowych	Informatyk
Konserwacja sprzętu do przetwarzania danych osobowych	Informatyk
Nadzorowanie wynoszenia aktywów poza siedzibę organizacji	Kierownicy komórek organizacyjnych firmy
Bezpiecznie zbywanie lub przekazywanie nośników do ponownego użycia	Informatyk
Nadzorowanie przestrzegania Polityki czystego biurka i czystego ekranu	kierownicy komórek organizacyjnych firmy
Nadzorowanie bezpieczeństwa systemów informatycznych i danych osobowych oraz kopi zapasowych	Informatyk
Nadzorowanie przestrzegania zasad korzystania z Internetu	kierownicy komórek organizacyjnych firmy
Nadzorowanie przestrzegania zasad korzystania z poczty elektronicznej	kierownicy komórek organizacyjnych firmy
Nadzorowanie przestrzegania zarządzania nośnikami wymiennymi	Informatyk
Nadzorowanie dostępu do sieci i usług sieciowych	Informatyk
Zarządzanie identyfikatorami użytkowników	Informatyk, Analityk, Kierownik działu floty
Nadawanie, odbieranie lub dostosowywanie praw dostępu	Informatyk, Analityk, Kierownik działu floty
Stosowanie poufnych informacji uwierzytelniających	Informatyk
Zabezpieczenie przed szkodliwym oprogramowaniem	Informatyk
Nadzorowanie przestrzegania Polityki bezpieczeństwa informacji w relacjach z dostawcami	Kierownicy działu handlowego, marketingu i księgowości, Informatyk

Przeprowadzenie testowania planu ciągłości działania na wypadek dysfunkcji systemu informatycznego.	Informatyk
Kontrola komputerów pracowników	Kierownicy działów

6. DOKUMENTY ZWIĄZANE

- PS A2/1 Nadzór nad dokumentacją
- PS A3/1 Nadzór nad zapisami
- ROZPORZĄDZENIA ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)
- USTAWA z dnia 10 maja 2018 r. o ochronie danych osobowych
- USTAWA z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa

7. ZAŁĄCZNIKI

F1 Ps 4.3./2 Karta stanowiska komputerowego