ZARZĄDZENIE Nr 7639 /VIII/21
PREZYDENTA MIASTA ŁODZI
z dnia 2 lipca 2021 r.

w sprawie wdrożenia Polityki Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi.

Na podstawie art. 33 ust. 1 i 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2020 r. poz. 713 i 1378 oraz z 2021 r. poz. 1038) w związku z art. 92 ust. 1 pkt 2 i ust. 2 ustawy z dnia 5 czerwca 1998 r. o samorządzie powiatowym (Dz. U. z 2020 r. poz. 920 oraz z 2021 r. poz. 1038), § 20 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r. poz. 2247) oraz art. 24 ust. 1 i 2 rozporządzenia 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) (Dz. Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.[1])

zarządzam, co następuje:

§ 1. 1. Wdrażam Politykę Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi, zwaną dalej Polityką SZBI, stanowiącą załącznik do niniejszego zarządzenia.

2. Na Politykę SZBI składają się:

1) Deklaracja stosowania, stanowiąca załącznik Nr 1 do Polityki SZBI;
2) Procedura monitorowania i nadzoru nad dokumentacją związaną z bezpieczeństwem informacji w Systemie Zarządzania Bezpieczeństwem Informacji Urzędu Miasta Łodzi, stanowiąca załącznik Nr 2 do Polityki SZBI;
3) Polityka Ochrony Danych w Urzędzie Miasta Łodzi, stanowiąca załącznik Nr 3 do Polityki SZBI;
4) Polityka Bezpieczeństwa Systemów Informatycznych w Urzędzie Miasta Łodzi, stanowiąca załącznik Nr 4 do Polityki SZBI;
5) Polityka Bezpieczeństwa Fizycznego i Środowiskowego w Urzędzie Miasta Łodzi, stanowiąca załącznik Nr 5 do Polityki SZBI.

§ 2. 1. Jawność załączników do Polityki SZBI, z wyjątkiem Deklaracji stosowania, stanowiącej załącznik Nr 1 do Polityki SZBI, podlega wyłączeniu na podstawie art. 28 ust. 3 lit. b i art. 38 ust. 5 oraz motywu 39 rozporządzenia 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).

2. Decyzję o udostępnieniu załączników wskazanych w § 1 ust. 2 pkt 2-5 podejmuje kierownik komórki organizacyjnej Urzędu Miasta Łodzi właściwej w sprawach bezpieczeństwa informacji i ochrony danych osobowych w porozumieniu z administratorem bezpieczeństwa systemu lub kierownikiem komórki organizacyjnej Urzędu Miasta Łodzi właściwej w sprawach administrowania budynkami.

---

[1] Zmiana wymienionego rozporządzenia została ogłoszona w Dz. Urz. UE L 127 z 23.05.2018, str. 2

§ 3. Zobowiązuję kierowników komórek organizacyjnych Urzędu Miasta Łodzi do podjęcia działań w zakresie dostosowania zasad funkcjonowania komórek organizacyjnych Urzędu Miasta Łodzi do postanowień Polityki SZBI.

§ 4. Wykonanie zarządzenia powierzam wiceprezydentom Miasta Łodzi, Sekretarzowi Miasta Łodzi, Skarbnikowi Miasta Łodzi oraz kierownikom komórek organizacyjnych Urzędu Miasta Łodzi.

§ 5. Tracą moc następujące zarządzenia Prezydenta Miasta Łodzi:

1) Nr 8183//VII/18 z dnia 10 kwietnia 2018 r. w sprawie wdrożenia polityki ochrony danych osobowych w Urzędzie Miasta Łodzi;
2) Nr 8706/VII/18 z dnia 21 czerwca 2018 r. zmieniające zarządzenie w sprawie wdrożenia polityki ochrony danych osobowych w Urzędzie Miasta Łodzi;
3) Nr 8972/VII/18 z dnia 18 lipca 2018 r. zmieniające zarządzenie w sprawie wdrożenia polityki ochrony danych osobowych w Urzędzie Miasta Łodzi;
4) Nr 9199/VII/18 z dnia 21 sierpnia 2018 r. zmieniające zarządzenie w sprawie wdrożenia polityki ochrony danych osobowych w Urzędzie Miasta Łodzi;
5) Nr 2992/VIII/20 z dnia 3 stycznia 2020 r. zmieniające zarządzenie w sprawie wdrożenia polityki ochrony danych osobowych w Urzędzie Miasta Łodzi;
6) Nr 2993/VIII/20 z dnia 3 stycznia 2020 r. w sprawie określenia sposobu realizacji oceny skutków operacji przetwarzania dla ochrony danych osobowych w Urzędzie Miasta Łodzi;
7) Nr 2994/VIII/20 z dnia 3 stycznia 2020 r. w sprawie określenia sposobu realizacji oceny ryzyka przetwarzania informacji i danych osobowych w Urzędzie Miasta Łodzi;
8) Nr 6537/VIII/21 z dnia 18 lutego 2021 r. w sprawie ustalenia regulaminów korzystania przez pracowników Urzędu Miasta Łodzi ze służbowych: telefonów stacjonarnych, telefonów komórkowych, kart SIM, modemów internetowych oraz tabletów/iPadów.

§ 6. Zarządzenie wchodzi w życie z dniem 1 października 2021 r.

PREZYDENT MIASTA ŁODZI

PREZYDENT MIASTA

Hanna ZDANOWSKA

Załącznik
do zarządzenia Nr 7639 /VIII/21
Prezydenta Miasta Łodzi
z dnia 2 lipca 2021 r.

Polityka Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi

DEKLARACJA NAJWYŻSZEGO KIEROWNICTWA

Mając na względzie postanowienia ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2021 r. poz. 670 i 952 i 1005) oraz ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2020 r. poz. 1369), a także rozporządzenia 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) i rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych ustanawia się, wdraża, eksploatuje, monitoruje i przegląda, a także utrzymuje i doskonali System Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi. System Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi to system zapewniający poufność, dostępność i integralność informacji, a także rozliczalność, autentyczność, niezaprzeczalność, niezawodność oraz ciągłość działania organizacji – wykonywania zadań publicznych.
Głównym celem wielopoziomowego systemu zarządzania bezpieczeństwem informacji jest ochrona aktywów informacyjnych, w tym danych osobowych, na każdym etapie ich przetwarzania. Szczegółowe cele zostały określone w niniejszym dokumencie, tj. w Polityce Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi, która stanowi główny dokument przyjętego rozwiązania. System został opracowany na podstawie obowiązujących przepisów prawa, ze szczególnym uwzględnieniem postanowień Polskich Norm PN-ISO/IEC 27001, PN-ISO/IEC 27002 i PN-ISO/IEC 27005, a także przyjętych strategii i programów działania urzędu.

Najwyższe kierownictwo deklaruje, w szczególności:

1) zapewnienie dostępności zasobów potrzebnych do utrzymania, rozwoju i ciągłego doskonalenia Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi (zasoby finansowe, osobowe, rzeczowe);
2) zaangażowanie w odniesieniu do Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi, w tym kompleksową ochronę informacji oraz aktywów wspierających ich przetwarzanie, a w szczególności osiąganie zamierzonych wyników;
3) kierowanie i aktywne wspieranie osób przyczyniających się do osiągnięcia skuteczności Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi, ze szczególnym uwzględnieniem osób odpowiedzialnych za realizację zadań związanych z bezpieczeństwem informacji, a także zaangażowanie wszystkich pracowników w ochronę aktywów poprzez stałe podnoszenie świadomości pracowników urzędu w zakresie bezpieczeństwa informacji.

Rozdział 1
Zagadnienia ogólne

§ 1. 1. Niniejszy dokument, zwany dalej Polityką SZBI, jest głównym elementem ustanowionego Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi, zwanego dalej SZBI.

2. W celu zapewnienia właściwego poziomu bezpieczeństwa informacji, Polityka SZBI zawiera ogólne ramy, wymagania, zasady, procedury i instrukcje w zakresie ochrony informacji przetwarzanych w urzędzie oraz stanowi dokument podstawowy, w stosunku do pozostałych wewnętrznych aktów prawnych dotyczących bezpieczeństwa, tworząc wspólnie z nimi kompleksową dokumentację.

3. Postanowienia Polityki SZBI mogą być stosowane przez administratorów danych, z którymi urząd z mocy przepisów prawa albo na mocy odrębnych porozumień współadministruje danymi osobowymi, pod warunkiem, że administrator wyrazi wolę stosowania tych regulacji poprzez złożenie deklaracji stosowania.

4. Polityka SZBI podlega okresowym przeglądom pod kątem aktualności, przydatności i adekwatności, zgodnie z Procedurą monitorowania i nadzoru nad dokumentacją związaną z bezpieczeństwem informacji w Systemie Zarządzania Bezpieczeństwem Informacji Urzędu Miasta Łodzi, stanowiącą załącznik Nr 2 do Polityki SZBI.

§ 2. Ilekroć w Polityce SZBI jest mowa o:

1) urzędzie, należy przez to rozumieć Urząd Miasta Łodzi;
2) prezydencie, należy przez to rozumieć Prezydenta Miasta Łodzi, pełniącego także funkcję starosty;
3) najwyższym kierownictwie, należy przez to rozumieć osobę lub grupę osób, która określa kierunek i steruje organizacją na najwyższym poziomie, tj. prezydenta, wiceprezydentów Miasta Łodzi, Sekretarza Miasta Łodzi, Skarbnika Miasta Łodzi oraz dyrektorów departamentów urzędu;
4) komórce organizacyjnej, należy przez to rozumieć: departament, wydział (równorzędną komórkę organizacyjną o innej nazwie), samodzielną komórkę organizacyjną urzędu, Geodetę Miejskiego;
5) kierowniku komórki organizacyjnej, należy przez to rozumieć dyrektora departamentu, dyrektora wydziału (równorzędnej komórki organizacyjnej o innej nazwie) oraz kierownika samodzielnej komórki organizacyjnej urzędu;
6) ogólnym rozporządzeniu, należy przez to rozumieć 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);
7) inspektorze, należy przez to rozumieć inspektora ochrony danych – pracownika urzędu, wyznaczonego przez administratora danych zgodnie z art. 37 ogólnego rozporządzenia;
8) interesariuszu, należy przez to rozumieć klientów urzędu, w tym osoby fizyczne oraz instytucje;
9) aktywach, należy przez to rozumieć aktywna główne oraz aktywa wspierające;
10) aktywach głównych, należy przez to rozumieć wszelkie informacje, w tym dane osobowe oraz procesy ich przetwarzania;
11) aktywach wspierających, należy przez to rozumieć wszelkie elementy wspomagające obsługę procesów w postaci infrastruktury, budynków i pomieszczeń, pracowników, sprzętu i oprogramowania.

Rozdział 2
Cele bezpieczeństwa informacji

§ 3. 1. W urzędzie ustanawia się wymagania w zakresie bezpieczeństwa informacji.

2. Ustanowione cele Polityki SZBI wspierają obowiązującą strategię, przyczyniają się do osiągnięcia celów ustawowych, oraz realizacji usług świadczonych na rzecz klientów i stron zainteresowanych.

§ 4. 1. Do głównych celów bezpieczeństwa informacji w urzędzie należy:

1) ochrona informacji, w szczególności danych osobowych, przetwarzanych w urzędzie;
2) zapewnienie bezpieczeństwa aktywów informacyjnych urzędu (w tym ochrona wizerunku i relacji z podmiotami zewnętrznymi), zgodnie z wymogami obowiązującego prawa oraz adekwatnie do wyników szacowania ryzyka w bezpieczeństwie informacji;
3) usprawnienie funkcjonowania urzędu poprzez uporządkowanie zasad przetwarzania informacji oraz zarządzanie aktywami informacyjnymi w zorganizowany sposób, tak aby ułatwić ciągłe doskonalenie i dostosowanie do bieżących celów i potrzeb urzędu;
4) minimalizowanie ryzyka i ograniczanie skutków utraty bezpieczeństwa informacji;
5) stałe podnoszenie świadomości w zakresie bezpieczeństwa informacji.

2. W ramach realizacji ww. celów, adekwatnie do poziomu zidentyfikowanych zagrożeń, podejmowane są działania w kierunku osiągnięcia poziomu organizacyjnego i technicznego urzędu, który w szczególności zapewni:

1) ciągłość realizacji celów publicznych;
2) poufność przetwarzanych informacji;
3) integralność informacji oraz ich dostępność;
4) uwzględnienie dodatkowych atrybutów bezpieczeństwa, zgodnie z wymaganiami i decyzjami oraz zapewnienie bezpiecznego przetwarzania informacji, w tym zdolności do podejmowania działań w sytuacjach kryzysowych;
5) udokumentowanie informacji dotyczących celów bezpieczeństwa informacji i stopnia ich realizacji.

§ 5. W urzędzie prowadzona jest okresowa ocena stopnia realizacji wyznaczonych celów bezpieczeństwa informacji poprzez kontrole/audyty wewnętrzne oraz przeglądy dokumentacji. Szczegółowe zasady i tryb prowadzenia przedmiotowej oceny określają opracowane dokumenty II i III poziomu bezpieczeństwa informacji zawarte w Deklaracji stosowania, stanowiącej załącznik Nr 1 do Polityki SZBI.

Rozdział 3
Kontekst funkcjonowania urzędu

§ 6. 1. Urząd funkcjonuje w otoczeniu zewnętrznym i wewnętrznym, które mają wpływ, na jakość realizacji usług świadczonych na rzecz klientów i stron zainteresowanych.

2. Urząd jest jednostką budżetową, za pomocą której prezydent jako organ wykonawczy realizuje:

1) gminne i powiatowe zadania publiczne (zadania własne);
2) zadania publiczne z zakresu administracji rządowej (zadania zlecone);
3) zadania publiczne na podstawie porozumień zawartych z organami administracji rządowej.

3. Realizacja zadań, o których mowa w ust. 2, następuje z uwzględnieniem następujących przepisów prawa:

1) ogólnego rozporządzenia;
2) ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781);
3) ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa;
4) ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2020 r. poz. 2176);

5) ustawy z dnia 25 lutego 2016 r. o ponownym wykorzystywaniu informacji sektora publicznego (Dz. U. z 2019 r. poz. 1446);
6) ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2020 r. poz. 1913);
7) rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.

4. Postanowienia niniejszego rozdziału podlegają analizie, ocenie i aktualizowaniu w ramach monitorowania i doskonalenia SZBI.

§ 7. 1. Strukturę organizacyjną urzędu, zasady jego funkcjonowania, a także zakres zadań realizowanych przez komórki organizacyjne określa Regulamin organizacyjny Urzędu Miasta Łodzi oraz szczegółowe wykazy zadań, przyjęte zarządzeniami prezydenta.

2. Sposób realizacji zadań publicznych jest regulowany zarządzeniami prezydenta, albo wewnętrznymi procedurami, lub instrukcjami określonymi przez kierowników komórek organizacyjnych.

§ 8. 1. Urząd funkcjonuje oraz realizuje zadania z uwzględnieniem określonych uwarunkowań zewnętrznych i wewnętrznych, które mają wpływ na bezpieczeństwo posiadanych aktywów.

2. Realizując Politykę SZBI uwzględnia się w szczególności:
1) uwarunkowania zewnętrzne:
   a) technologiczne,
   b) ekonomiczne,
   c) naturalne, kulturowe, społeczne i polityczne,
   d) konieczność zapewnienia zgodności z obowiązującymi przepisami prawa, a także z orzecznictwem sądów,
   e) wymagania i oczekiwania interesariuszy,
   f) czynniki wpływające na osiąganie celów strategicznych urzędu,
   g) wizerunek i reputację urzędu;
2) uwarunkowania wewnętrzne:
   a) strukturę organizacyjną urzędu, podział kompetencji, ról i odpowiedzialności,
   b) budżet miasta Łodzi,
   c) strategie, cele oraz kierunki działania i rozwoju, a także postanowienia wewnętrznych aktów prawnych,
   d) charakter wykonywanych zadań i ich wpływ na sposoby przetwarzania informacji,
   e) zasoby wykorzystywane do realizacji powierzonych zadań, w tym: pracowników, zasoby finansowe, wiedzę, nieruchomości oraz systemy informatyczne,
   f) przyjęte i realizowane wytyczne i standardy podnoszące kulturę organizacji.

§ 9. W urzędzie zidentyfikowano następujące grupy interesariuszy:
1) odbiorcy usług realizowanych przez komórki organizacyjne urzędu, w tym mieszkańcy miasta Łodzi;
2) posłowie, senatorowie;
3) radni Rady Miejskiej w Łodzi i jednostek pomocniczych;
4) pracownicy urzędu, w tym najwyższe kierownictwo urzędu, kierownicy komórek organizacyjnych;
5) przedsiębiorcy (inwestorzy);
6) organy administracji publicznej, w tym organy kontrolne;
7) miejskie jednostki organizacyjne, spółki prawa handlowego, w których miasto Łódź jest akcjonariuszem lub udziałowcem i ich klienci;

8) organizacje pozarządowe, związki wyznaniowe, partie polityczne;
9) dostawcy, kontrahenci i inne osoby oraz podmioty, które realizują zadania w imieniu i na rzecz urzędu;
10) media.

Rozdział 4
Zakres i zasady SZBI

§ 10. 1. Zakres ustanowionego SZBI obejmuje:
1) procesy oraz realizowane w urzędzie działania i zadania;
2) wszelkie informacje przetwarzane w ramach ww. procesów i zadań będące własnością urzędu lub stron zainteresowanych, o ile zostały przekazane na podstawie obowiązujących przepisów prawnych lub umów, w tym:
   a) przetwarzane w formie tradycyjnej (m.in. informacje wydrukowane lub zapisane na papierze),
   b) przetwarzane w formie elektronicznej (np. w systemach informatycznych urzędu, przesyłane za pośrednictwem poczty elektronicznej lub urządzeń elektronicznych, elektronicznych nośników informacji);
3) aktywa wspierające przetwarzanie informacji w ramach ww. procesów oraz realizowanych w urzędzie działań i zadań, w tym:
   a) personel (wszyscy pracownicy urzędu bez względu na podstawę zatrudnienia oraz inne osoby i podmioty zewnętrzne wykonujące czynności w imieniu i na rzecz urzędu i/lub mające dostęp do aktywów informacyjnych urzędu),
   b) budynki i pomieszczenia urzędu, w których są lub będą przetwarzane informacje,
   c) sprzęt, w tym sprzęt komputerowy, urządzenia mobilne oraz inne nośniki danych, na których znajdują się informacje podlegające ochronie, oprogramowanie, infrastruktura sieciowa,
   d) technologie służące pozyskiwaniu, selekcjonowaniu, analizowaniu, przetwarzaniu, zarządzaniu i udostępnianiu informacji, do których zalicza się zarówno systemy papierowe jak i elektroniczne wspomagające realizację zadań publicznych.

2. Z uwagi na szczególny charakter informacji niejawnych wynikający z obowiązujących przepisów prawa, ochrona informacji niejawnych i aktywów wspierających ich przetwarzanie podlega wyłączeniu z ustanowionego SZBI. Zasady i tryb ochrony informacji niejawnych w urzędzie określone zostały w treści odrębnych uregulowań wewnętrznych.

§ 11. W urzędzie obowiązują określone zasady bezpieczeństwa informacji, na podstawie których kształtują się mechanizmy techniczne i organizacyjne bezpieczeństwa informacji, w szczególności:
1) zasada adekwatności zabezpieczeń – stosowane zabezpieczenia muszą być adekwatne do zidentyfikowanych zagrożeń oraz rodzajów przetwarzanych danych;
2) zasada bezpiecznego przetwarzania – przetwarzanie informacji szczególnie chronionych powinno odbywać się wyłącznie w bezpiecznych środowiskach, tj. w separowanych systemach informatycznych, zabezpieczonych pomieszczeniach itp.;
3) zasada bezpiecznej współpracy z podmiotami zewnętrznymi – dokumenty regulujące współpracę z podmiotami zewnętrznymi, winny zawierać regulacje odnośnie bezpieczeństwa informacji, w tym klauzule o zachowaniu poufności;
4) zasada ochrony danych w fazie projektowania – ocenę przetwarzania danych należy przeprowadzić w czasie planowania sposobów przetwarzania danych przy np. ustalaniu procedur, architektury systemów, uprawnień użytkownika itd.;

5) zasada domyślnej ochrony danych – zagwarantowanie, że w procesie przetwarzania danych osobowych „domyślnie" przetwarzane są dane jedynie w takim zakresie w jakim jest to niezbędne do zrealizowania celu przetwarzania (ilość zbieranych danych, ich zakres, czas retencji oraz dostępność do danych);
6) zasada cykliczności oceny – przeprowadzenie regularne oceny przetwarzania w czasie istnienia procesu przetwarzania;
7) zasada „czystego biurka i ekranu" – opuszczając stanowisko pracy należy usunąć dokumenty zawierające informacje inne niż jawne i zabezpieczyć je w meblach biurowych lub sejfach; dostęp do komputera, podczas nieobecności, należy skutecznie zablokować, a po zakończeniu pracy komputer wyłączyć, chyba, że charakter realizowanych zadań wymaga jego pracy w sposób ciągły;
8) zasada doskonalenia SZBI – system podlega przeglądowi i dostosowaniu do zmieniających się warunków w oparciu o prowadzony monitoring i nadzór;
9) zasada najsłabszego ogniwa – poziom bezpieczeństwa informacji wyznacza jego najsłabiej zabezpieczony element;
10) zasada uprawnionego dostępu – korzystanie z aktywów informacyjnych urzędu może następować tylko w oparciu o formalne uprawnienia do korzystania z danego zasobu;
11) zasada wiedzy uzasadnionej – pracownicy mają dostęp do informacji w ograniczonym zakresie, jaki jest im niezbędny do realizacji powierzonych zadań;
12) zasada segregacji obowiązków i zadań – obowiązki i uprawnienia powinny być tak rozdzielone, aby pojedyncza osoba nie dysponowała pełnią uprawnień do wykonywania zadań w całości.

Rozdział 5
Funkcje i odpowiedzialność w zakresie bezpieczeństwa informacji

§ 12. 1. W ramach wprowadzonego SZBI określa się funkcje i odpowiedzialność poszczególnych uczestników procesu przetwarzania informacji, na wszystkich poziomach organizacji.

2. Generalną zasadą jest ponoszenie odpowiedzialności za bezpieczeństwo informacji przez wszystkich pracowników urzędu, niezależnie od formy nawiązania stosunku pracy, a także przez inne osoby i podmioty objęte zakresem SZBI.

3. Odpowiedzialność polega na przestrzeganiu powszechnie obowiązujących przepisów prawa, prawa miejscowego, a także wewnętrznych regulacji określonych zarządzeniami prezydenta, a w szczególności stosowania się do zasad określonych Polityką SZBI.

4. Szczegółowe określenie pełnionych funkcji i odpowiedzialności zostało opisane w dziedzinowych dokumentach, składających się łącznie na SZBI w urzędzie.

§ 13. 1. Prezydent pełni rolę administratora danych i wyznacza:
1) inspektora oraz jego zastępcę – pracowników urzędu, zgodnie z art. 37 ogólnego rozporządzenia;
2) administratora bezpieczeństwa systemu.

2. Wiceprezydenci Miasta Łodzi, Sekretarz Miasta Łodzi oraz Skarbnik Miasta Łodzi w zakresie powierzonych im spraw miasta Łodzi i kierownicy komórek organizacyjnych w zakresie właściwości rzeczowej kierowanej komórki organizacyjnej pełnią funkcję lokalnych administratorów danych.

3. Kierownicy komórek organizacyjnych, w zakresie właściwości rzeczowej kierowanej komórki organizacyjnej, wyznaczają lokalnych inspektorów ochrony danych, którzy w szczególności będą wspierać ich działania w zakresie przestrzegania prawa i stosowania dobrych praktyk ochrony danych osobowych, z zastrzeżeniem ust. 4.

4. Wyznaczenia lokalnych inspektorów ochrony danych dokonuje się na następujących zasadach:

1) w przypadku komórki organizacyjnej urzędu o liczbie do 35 etatów – 1 lokalny inspektor;
2) w przypadku komórki organizacyjnej urzędu o liczbie od 36 do 70 etatów – 2 lokalnych inspektorów;
3) w przypadku komórki organizacyjnej urzędu o liczbie powyżej 70 etatów – 3 lokalnych inspektorów.

5. Kierownik komórki organizacyjnej właściwej w sprawach ochrony danych osobowych wspiera działania administratora danych w zakresie nadzorowania prawidłowego przetwarzania informacji w urzędzie, w szczególności w zakresie materialno-technicznych warunków ich przetwarzania, a także pełni rolę inspektora.

§ 14. 1. Najwyższe kierownictwo ponosi odpowiedzialność za:
1) zapewnienie zasobów niezbędnych do bieżącego funkcjonowania, utrzymania i ciągłego monitorowania oraz doskonalenia SZBI;
2) stosowanie, odpowiednich do zagrożeń, środków technicznych i organizacyjnych zapewniających przetwarzanie informacji, w tym danych osobowych z uwzględnieniem charakteru, zakresu, kontekstu i celów przetwarzania danych, a także kategorii danych objętych ochroną, a w szczególności zabezpieczenia danych przed dostępem do nich osób nieupoważnionych w tym przed ich udostępnieniem osobom nieupoważnionym, przed ich zabraniem przez nieuprawnioną osobę, przetwarzaniem z naruszeniem przepisów prawa oraz zmianą, utratą uszkodzeniem lub zniszczeniem, ze szczególnym uwzględnieniem informacji przetwarzanych w systemach informatycznych;
3) określenie zasobów podlegających ochronie;
4) decyzję o akceptacji ryzyka wraz z planem postępowania z ryzykiem, ze szczególnym uwzględnieniem ryzyka naruszenia praw i wolności osób fizycznych.

2. Nadzór i kontrolę w zakresie przetwarzania informacji, z upoważnienia prezydenta jako administratora danych, sprawują wiceprezydenci Miasta Łodzi, Skarbnik Miasta Łodzi i Sekretarz Miasta Łodzi oraz kierownicy komórek organizacyjnych urzędu, przy wsparciu lokalnych inspektorów ochrony danych, w zakresie swojej właściwości rzeczowej, wynikającej z odrębnych zarządzeń prezydenta.

§ 15. 1. Kierownik komórki organizacyjnej właściwej w sprawach bezpieczeństwa informacji, odpowiedzialny jest za:
1) nadzór nad realizacją SZBI;
2) nadzór nad dokumentacją SZBI na etapie jej tworzenia, weryfikacji, aktualizacji, udostępniania i przechowywania;
3) zarządzanie analizą ryzyka jako kluczowym narzędziem SZBI;
4) zarządzanie zabezpieczeniami aktywów informacyjnych w sposób adekwatny do celów stosowania zabezpieczeń;
5) zapewnienie, okresowych przeglądów oraz nadzór nad realizacją ustaleń z nich wynikających oraz inicjowanie oraz nadzorowanie działań wdrożeniowych, korygujących i zapobiegawczych;
6) przedstawianie sprawozdań najwyższemu kierownictwu, dotyczących funkcjonowania SZBI oraz realizacji celów, jak również informowanie o skuteczności systemu, a także bieżące informowanie o działalności niezgodnej z przyjętymi założeniami;
7) zarządzanie kontrolami wewnętrznymi w obszarze bezpieczeństwa informacji w tym w zakresie planowania kontroli, nadzoru nad ich realizacją oraz realizacją zaleceń pokontrolnych;
8) organizowanie szkoleń z zakresu monitorowania i nadzoru nad dokumentacją związaną z bezpieczeństwem informacji oraz ochrony danych osobowych, a także koordynacja szkoleń w pozostałym zakresie;
9) koordynację działań związanych z ochroną informacji;

10) analizę raportów z wszelkich zdarzeń związanych z bezpieczeństwem wszystkich zasobów informacyjnych i nadzorowanie działań korygujących i zapobiegawczych;
11) monitorowanie zachowania właściwego poziomu bezpieczeństwa informacji.

2. Kierownik komórki organizacyjnej właściwej w sprawach bezpieczeństwa informacji, uprawniony jest do:
1) wydawania poleceń pracownikom urzędu w zakresie związanym z utrzymaniem i doskonaleniem SZBI;
2) rozstrzygania sporów dotyczących stosowania wymagań zawartych w dokumentacji SZBI oraz wydawania wiążących decyzji w tym zakresie;
3) dostępu do wszystkich dokumentów, których treść może być istotna z punktu widzenia funkcjonowania SZBI i uzyskania wyjaśnień od pracowników w zakresie realizowanych działań w ramach SZBI;
4) podejmowania decyzji w kwestiach bezpieczeństwa informacji, w zakresie nierodzącym zobowiązań finansowych, a w szczególności w zakresie współpracy z innymi podmiotami.

3. Do zadań kierownika komórki organizacyjnej właściwej w sprawach ochrony danych osobowych należy:
1) sprawowanie nadzoru nad przestrzeganiem obowiązujących zasad wynikających z funkcjonowania SZBI w zakresie bezpieczeństwa informacji, a w szczególności przepisów prawa dotyczących ochrony danych osobowych;
2) przeprowadzanie kontroli zgodności przetwarzania danych osobowych z przepisami oraz opracowywanie sprawozdań i zaleceń dla kierownictwa;
3) prowadzenie dokumentacji wynikającej z postanowień SZBI;
4) opiniowanie procesów związanych z zarządzaniem systemem informatycznym przetwarzającym informacje (w tym dane osobowe) w aspekcie ich bezpieczeństwa w tym doradzaniem w kwestiach związanych z powierzeniem danych, monitorowaniem udostępniania danych osobowych, w tym wydawaniem opinii w zakresie realizacji wniosku o udostępnienie;
5) organizowanie i przeprowadzanie szkoleń z zakresu ochrony danych osobowych;
6) realizowanie działań wynikających z dokumentacji bezpieczeństwa informacji i utrzymywanie zapisów świadczących o funkcjonowaniu SZBI;
7) informowanie najwyższego kierownictwa o stanie bezpieczeństwa informacji w zakresie stosowanych zabezpieczeń i ocenie ich skuteczności oraz doradzanie jakie działania powinny być podejmowane;
8) pełnienie funkcji punktu kontaktowego dla Prezesa Urzędu Ochrony Danych;
9) pełnienie funkcji punktu kontaktowego dla osób, których dane dotyczą, w tym koordynacja nad przygotowywaniem odpowiedzi na ich żądanie;
10) koordynowanie działań wynikających z realizacji żądań osób, których dane dotyczą;
11) wspieranie komórek organizacyjnych w przypadku konieczności przeprowadzania oceny skutków oddziaływania na dane osobowe;
12) wspieranie komórek organizacyjnych, w przypadku stwierdzenia incydentu lub naruszenia.

4. Zakres zadań inspektora określa ogólne rozporządzenie, a zakres posiadanych upoważnień został nadany odrębnym zarządzeniem.

§ 16. 1. Kierownik komórki organizacyjnej właściwej w sprawach zapewnienia ochrony i bezpieczeństwa danych w systemach informatycznych w urzędzie, pełniący funkcję administratora bezpieczeństwa systemu, odpowiada za bezpieczeństwo i utrzymanie ciągłości działania sieci teleinformatycznych oraz systemów i oprogramowania, a w szczególności:
1) zarządza systemami informatycznymi;

2) prowadzi dokumentację wynikającą z postanowień SZBI, w tym przygotowuje i wprowadza politykę bezpieczeństwa systemów informatycznych w Urzędzie Miasta Łodzi;
3) opracowuje dokumentację związaną z incydentami cyberbezpieczeństwa;
4) nadzoruje proces doboru zabezpieczeń dla wszystkich aktywów informacyjnych urzędu;
5) przygotowuje dokumenty planów ciągłości działania i planów awaryjnych dla systemów informatycznych, wprowadza i sprawdza plany;
6) ocenia pracę systemów informatycznych w celu wykrycia potencjalnych zagrożeń, w szczególności identyfikacji wszelkich nieprawidłowości związanych z bezpieczeństwem systemów informatycznych;
7) przeprowadza analizy ryzyka dla systemów informatycznych i analizy podatności systemów informatycznych;
8) analizuje raporty z wszelkich zdarzeń związanych z bezpieczeństwem systemów informatycznych;
9) szkoli pracowników z zakresu bezpieczeństwa informacji w systemach informatycznych;
10) podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia bezpieczeństwa informacji w systemie informatycznym;
11) określa zakres uprawnień do systemów informatycznych w porozumieniu z kierownikami komórek organizacyjnych;
12) prowadzi, uaktualniania na bieżąco oraz przesyła do kierownika komórki organizacyjnej właściwej w sprawach ochrony danych osobowych informacje o zdarzeniach wpływających na bezpieczeństwo systemów informatycznych, w tym m.in. wykrytego oprogramowania złośliwego lub szpiegującego oprogramowania nielegalnego lub zainstalowanego bez upoważnienia, awarii systemu informatycznego lub jego nieprawidłowego działania, stwierdzenia faktu korzystania z systemu informatycznego przez osobę niepowołaną, awarii zasilania; w przypadku gdy zdarzenie ma wpływ na ochronę danych osobowych przesyła również informację do inspektora.

2. Kierownik komórki organizacyjnej właściwej w sprawach zapewnienia ochrony i bezpieczeństwa danych w systemach informatycznych w urzędzie prowadzi dokumentację wynikającą z postanowień SZBI.

3. Szczegółowe obowiązki kierownika komórki organizacyjnej właściwej w sprawach zapewnienia ochrony i bezpieczeństwa danych w systemach informatycznych w urzędzie zostały uregulowane w opracowanych dokumentach II i III poziomu bezpieczeństwa informacji.

§ 17. 1. Kierownicy komórek organizacyjnych, pełniący rolę lokalnych administratorów danych, odpowiadają za wykonywanie powierzonych zadań publicznych z zachowaniem zasad bezpieczeństwa informacji, a w szczególności:
1) czuwają nad właściwym wykonywaniem obowiązków przez pracowników komórek w zakresie bezpieczeństwa informacji;
2) stwarzają właściwe warunki organizacyjne i techniczne, gwarantujące bezpieczeństwo systemów informatycznych, w tym nadzorują właściwą lokalizację sprzętu komputerowego, tj. ustawiania monitorów i drukarek w sposób uniemożliwiający wgląd w dane osobowe osobom nieuprawnionym lub kradzież wymiennych nośników danych, a także właściwego wyposażenia stanowisk pracy w sprzęt biurowy;
3) określają zasoby podlegające ochronie i aktualizują ich wykazy;
4) podejmują odpowiednie działania w przypadku wykrycia naruszeń bezpieczeństwa;
5) przeprowadzają okresową analizę ryzyka wraz z określeniem planu postępowania z ryzykiem, w tym identyfikowanie i dokumentowanie zagrożeń dla bezpieczeństwa informacji oraz definiowanie oraz realizację działań zapobiegających zagrożeniom;

6) przestrzegają zasad ochrony informacji przez nich samych, jak i przez podległych im pracowników, w tym nadzorują postępowanie zgodne z opisanymi i przyjętymi zasadami bezpiecznego przetwarzania danych osobowych i innych informacji;
7) nadzorują zapoznanie pracowników z obowiązkami z zakresu ochrony informacji na stanowiskach pracy, w tym stanowiskowego przeszkolenia pracowników w zakresie przepisów prawa oraz wewnętrznych zasad ochrony informacji;
8) nadzorują poprawność merytoryczną danych gromadzonych w systemach informatycznych oraz w tradycyjnej formie.

2. Szczegółowe obowiązki kierowników komórek organizacyjnych zostały uregulowane w opracowanych dokumentach II i III poziomu bezpieczeństwa informacji.

§ 18. 1. Kierownik komórki organizacyjnej właściwej w sprawach administrowania budynkami urzędu odpowiada za działania zmierzające do zapobiegania nieuprawnionemu dostępowi do aktywów urzędu, a także usuwaniu szkód i zakłóceń, jakie mogłyby być skutkiem nieuprawnionego dostępu do budynków i pomieszczeń.

2. Prowadzi dokumentację wynikającą z postanowień SZBI.

3. Szczegółowe obowiązki kierownika komórki organizacyjnej właściwej w sprawach administrowania budynkami urzędu zostały uregulowane w opracowanych dokumentach II i III poziomu bezpieczeństwa informacji.

§ 19. 1. Kierownik komórki organizacyjnej właściwej w sprawach zarządzania kadrami odpowiada za działania w zakresie zapewnienia bezpieczeństwa zasobów ludzkich w odniesieniu do osób zatrudnionych w ramach stosunku pracy.

2. Za zapewnienie bezpieczeństwa zasobów ludzkich w przypadku innych osób i podmiotów wykonujących czynności w imieniu i na rzecz urzędu odpowiada kierownik komórki organizacyjnej odpowiedzialny za nawiązanie współpracy.

3. Szczegółowy sposób postępowania przed nawiązaniem zatrudnienia oraz w jego trakcie regulują odrębne zarządzenia prezydenta, z zastrzeżeniem postanowień wynikających z Polityki SZBI.

4. Prowadzi dokumentację wynikającą z postanowień Polityki SZBI.

5. Szczegółowe obowiązki kierownika komórki organizacyjnej właściwej w sprawach zarządzania kadrami zostały uregulowane w opracowanych dokumentach II i III poziomu bezpieczeństwa informacji.

§ 20. 1. Odpowiedzialność za bezpieczeństwo informacji ponoszą wszyscy pracownicy zgodnie z posiadanymi zakresami obowiązków. Każdy pracownik obowiązany jest dbać o bezpieczeństwo powierzonych mu do przetwarzania danych, zgodnie z obowiązującymi przepisami prawa, a także wewnętrznymi procedurami czy instrukcjami, a w szczególności do:
1) przetwarzania danych osobowych z poszanowaniem praw osób, których dane dotyczą;
2) przetwarzania danych na podstawie przepisów prawa, z zachowaniem zasad rzetelności, przejrzystości;
3) przetwarzania danych osobowych w minimalnym zakresie, niezbędnym do osiągnięcia celu przetwarzania i jedynie przez okres niezbędny do jego osiągnięcia, a także prawidłowości, integralności i poufności;
4) zabezpieczanie danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osoby nieuprawnione, modyfikacją, utratą, uszkodzeniem lub zniszczeniem;
5) stosowania zasad opisanych w dokumentacji SZBI oraz innych dokumentach wewnętrznych;
6) ochrony sprzętu, wydruków komputerowych i innych nośników danych zawierających dane chronione;
7) utrzymywania w tajemnicy powierzonych informacji także po ustaniu zatrudnienia;

8) stosowania się do szczegółowych zaleceń w zakresie bezpiecznej obsługi systemów informatycznych;
9) natychmiastowego zgłaszania zauważonych incydentów oraz innych potencjalnych zdarzeń bezpośrednio przełożonemu.

2. W celu zgłoszenia informacji o naruszeniu, bądź też podejrzeniu naruszenia bezpieczeństwa informacji w urzędzie, osoby bądź podmioty niezwiązane z urzędem mogą zgłaszać przypadki bądź podejrzenie naruszenia bezpieczeństwa aktywów informacyjnych urzędu na adres iod@uml.lodz.pl.

3. Szczegółowe obowiązki pracowników zostały uregulowane w opracowanych dokumentach II i III poziomu bezpieczeństwa informacji.

Rozdział 6
Klasyfikacja przetwarzanych informacji

§ 21. 1. Informacjami podlegającymi ochronie, zgodnie z zasadami opisanymi w Polityce, są:
1) dane osobowe;
2) dane gromadzone w systemach zamkniętych użytkowanych na podstawie odrębnych przepisów prawa;
3) dane systemowe, w skład których wchodzą m.in. opisy procesów realizowanych w aplikacjach, struktur danych, procesów autoryzacji, ustawienia/konfiguracje systemu, logi, historie zmian, uprawnienia, kody źródłowe;
4) dane, będące przedmiotem praw autorskich lub prawa własności przemysłowej – dane, w skład których wchodzą m.in. rozwiązania techniczne, dokumentacje techniczne, różnego typu opracowania doradcze, pomocnicze itp. (tajemnice prawnie chronione);
5) inne informacje, co do których wymagane jest zachowanie poufności, dostępności oraz integralności.

2. Klasyfikacja informacji jest dokonywana na podstawie ustalonej wartości aktywów informacyjnych w urzędzie na zasadach określonych w opracowanych dokumentach II poziomu bezpieczeństwa informacji.

3. Szczegółowe zasady bezpieczeństwa przetwarzania i ochrony zidentyfikowanych grup informacji, w tym ich zakres, tryb udostępniania, dystrybucji, archiwizacji zostały określone w opracowanych dokumentach II i III poziomu bezpieczeństwa informacji zawartych w Deklaracji stosowania stanowiącej załącznik Nr 1 do Polityki SZBI.

Rozdział 7
Struktura dokumentacji bezpieczeństwa informacji

§ 22. 1. Ustanowiona Polityka SZBI wprowadza trójpoziomową dokumentację bezpieczeństwa informacji określającą zasady i tryb zarządzania bezpieczeństwem informacji, aktywami informacyjnymi, a w szczególności danymi osobowymi oraz aktywami wspierającymi, z zachowaniem fundamentalnych zasad przetwarzania, o których mowa w § 11.

2. I poziom dokumentacji bezpieczeństwa informacji stanowi Polityka SZBI będąca dokumentem o charakterze publicznym, podstawowym w stosunku do pozostałych wewnętrznych aktów tworzących wspólnie dokumentację bezpieczeństwa informacji.

3. II poziom dokumentacji bezpieczeństwa informacji obejmuje następujące dokumenty:
1) Politykę Ochrony Danych w Urzędzie Miasta Łodzi, stanowiącą załącznik Nr 3 do Polityki SZBI;
2) Politykę Bezpieczeństwa Systemów Informatycznych w Urzędzie Miasta Łodzi, stanowiącą załącznik Nr 4 do Polityki SZBI;

3) Politykę Bezpieczeństwa Fizycznego i Środowiskowego w Urzędzie Miasta Łodzi, stanowiącą załącznik Nr 5 do Polityki SZBI;
4) odrębne zarządzenia prezydenta opisujące szczegółowy sposób postępowania przed nawiązaniem zatrudnienia, w jego trakcie oraz po zakończeniu a także zarządzenia prezydenta opisujące zagadnienia bezpieczeństwa informacji, a w szczególności organizacji wewnętrznej oraz zarządzania aktywami.

4. III poziom dokumentacji bezpieczeństwa informacji stanowią dokumenty dedykowane i udostępnianie, na zasadzie wiedzy koniecznej, ze względu na szczególnych charakter przetwarzanych informacji.

5. Dokumenty, o których mowa w ust. 3, są dedykowane i udostępniane:
1) pracownikom urzędu w zależności od zakresu powierzonych zadań;
2) wybranym osobom i podmiotom zewnętrznym wykonującym czynności w imieniu i na rzecz urzędu i/lub mającym dostęp do aktywów informacyjnych urzędu, w uzasadnionych przypadkach.

§ 23. 1. Dokumenty opracowywane na poszczególnych poziomach uzupełniają się wzajemnie i tworzą kompleksową dokumentację bezpieczeństwa informacji.

2. W przyjętym w urzędzie modelu bezpieczeństwa informacji dopuszcza się opracowywanie dodatkowych dokumentów, w ramach właściwości rzeczowej komórek organizacyjnych, takich jak np. instrukcje, procedury, rekomendacje, zasady, wytyczne.

3. W celu zapewnienia właściwości, adekwatności i skuteczności obowiązujących przepisów wewnętrznych w zakresie bezpieczeństwa, prowadzone są okresowe przeglądy i aktualizacja ww. dokumentacji. Zasady monitorowania i nadzoru nad dokumentacją związaną z bezpieczeństwem informacji określa załącznik Nr 2 do Polityki SZBI.

Rozdział 8
Kontrola dostępu do informacji

§ 24. 1. W ramach zapewnienia ograniczonego dostępu do aktywów informacyjnych urzędu, w tym do budynków i pomieszczeń, sprzętu i urządzeń oraz systemów informatycznym tylko dla osób i podmiotów uprawnionych, prowadzona jest kontrola dostępu fizycznego i logicznego.

2. Szczegółowe zasady zarządzania dostępem do aktywów informacyjnych urzędu zostały uregulowane w opracowanych dokumentach II i III poziomu bezpieczeństwa informacji.

Rozdział 9
Zarządzanie aktywami informacyjnymi

§ 25. 1. W celu zapewnienia adekwatnego poziomu bezpieczeństwa aktywów informacyjnych, przedmiotowe aktywa są inwentaryzowane, klasyfikowane i zarządzane zgodnie z obowiązującymi wymaganiami w zakresie ich ochrony.

2. Szczegółowe zasady dotyczące identyfikowania, klasyfikowania, postępowania z aktywami oraz odpowiedzialności za aktywa informacyjne zostały uregulowane w opracowanych dokumentach II i III poziomu bezpieczeństwa informacji.

Rozdział 10
Zarządzanie ryzykiem w bezpieczeństwie informacji

§ 26. 1. Skuteczne zarządzanie bezpieczeństwem informacji wymaga podejmowania okresowych działań w obszarze zarządzania ryzykiem, w szczególności w zakresie szacowania tj. identyfikowania, analizy i oceny ryzyka w bezpieczeństwie informacji, zmierzających do ograniczenia oraz eliminacji przedmiotowego ryzyka.

2. Działania związane z zarządzaniem ryzykiem mającym wpływ na bezpieczeństwo informacji obejmują w szczególności:

1) przygotowanie oraz okresową aktualizację dokumentów dotyczących zarządzania ryzykiem;
2) prowadzenie okresowego szacowania ryzyka;
3) postępowanie z ryzykiem;
4) podejmowanie działań korygujących lub naprawczych.

3. Szczegółowe zasady zarządzania ryzykiem w bezpieczeństwie informacji zostały uregulowane w opracowanych dokumentach II i III poziomu bezpieczeństwa informacji.

Rozdział 11
Bezpieczeństwo teleinformatyczne

§ 27. 1. W ramach zarządzania bezpieczeństwem teleinformatycznym są podejmowane działania w zakresie rozwoju, monitorowania i doskonalenia infrastruktury teleinformatycznej, aplikacji i usług informatycznych, a także szacowania i kontroli ryzyka utraty poufności, integralności, dostępności informacji w związku z przetwarzaniem danych w systemie informatycznym urzędu.

2. Szczegółowe zasady i wymogi w zakresie bezpieczeństwa teleinformatycznego zostały uregulowane w opracowanych dokumentach II i III poziomu bezpieczeństwa informacji.

Rozdział 12
Bezpieczeństwo fizyczne i środowiskowe

§ 28. 1. W celu zapobieżenia nieuprawnionemu fizycznemu dostępowi, szkodom i zakłóceniom w przetwarzaniu informacji, a w szczególności utracie, zniszczeniu, uszkodzeniu, kradzieży aktywów informacyjnych urzędu stosowane są mechanizmy ochrony w obszarze bezpieczeństwa fizycznego i środowiskowego.

2. Szczegółowe zasady dotyczące zarządzania bezpieczeństwem fizycznym i środowiskowym zostały uregulowane w opracowanych dokumentach II i III poziomu bezpieczeństwa informacji.

Rozdział 13
Bezpieczeństwo zasobów ludzkich

§ 29. 1. Kierownik komórki organizacyjnej właściwej w sprawach zarządzania kadrami oraz właściwi kierownicy komórek organizacyjnych odpowiedzialni za nawiązanie współpracy z innymi podmiotami zewnętrznymi w celu ograniczenia ryzyka błędu ludzkiego, kradzieży lub nadużycia, zapewnienia, że pracownicy urzędu, oraz inne osoby i podmioty wykonujące czynności w imieniu i na rzecz urzędu i/lub mające dostęp do aktywów informacyjnych urzędu są świadomi odpowiedzialności i swoich obowiązków dotyczących bezpieczeństwa informacji oraz wypełniają je w odpowiedni sposób i z uwzględnieniem interesów urzędu, podejmują określone działania w obszarze bezpieczeństwa zasobów ludzkich, a w szczególności:

1) zapewniają wykwalifikowanych pracowników i/lub inne osoby albo podmioty zewnętrzne do realizacji zadań;
2) uwzględniają przepisy o odpowiedzialności w zakresie bezpieczeństwa informacji w umowach cywilnoprawnych zawieranych z ww. osobami i podmiotami;
3) realizują szkolenia ww. osób i podmiotów w zakresie bezpieczeństwa informacji oraz regularnego informowania o aktualizacji polityk i procedur związanych z ich stanowiskiem pracy.

2. Szczegółowe zasady dotyczące zarządzania bezpieczeństwem zasobów ludzkich w odniesieniu do osób zatrudnionych w ramach stosunku pracy zostały uregulowane w opracowanych dokumentach II i III poziomu bezpieczeństwa informacji.

Rozdział 14
Zapewnienie ciągłości działania

§ 30. 1. W urzędzie podejmowane są działania w zakresie planowania, weryfikowania, zapewnienia, przeglądu i oceny ciągłości działania i postępowania w przypadku wystąpienia sytuacji kryzysowych.

2. Szczegółowe zasady dotyczące zarządzania ciągłością działania zostały uregulowane w opracowanych dokumentach II i III poziomu bezpieczeństwa informacji.

Rozdział 15
Relacje z podmiotami zewnętrznymi

§ 31. 1. W celu zapewnienia ochrony aktywów informacyjnych udostępnianych usługodawcom, dostawcom i innym osobom oraz podmiotom zewnętrznym wykonującym czynności w imieniu i na rzecz urzędu i/lub mającym dostęp do aktywów urzędu, wprowadza się zasady postępowania w przypadku współpracy związanej z dostępem do aktywów informacyjnych urzędu i korzystania z usług ww. osób i podmiotów.

2. W przypadku wykonywania zadań delegowanych i/lub korzystania z aktywów, w tym przetwarzania informacji powierzonych przez podmioty zewnętrzne w drodze stosownej umowy i/lub porozumienia, poza wymogami określonymi w obowiązującej w urzędzie dokumentacji bezpieczeństwa dopuszcza się stosowanie wymogów i zaleceń bezpieczeństwa określonych przez ww. podmioty zewnętrzne, o ile wskazane wymogi i zalecenia „zewnętrzne" nie obniżają poziomu bezpieczeństwa pozostałych informacji przetwarzanych w urzędzie.

3. Przedmiotowe zasady i wymogi współpracy zostały uregulowane w opracowanych dokumentach II i III poziomu bezpieczeństwa informacji.

Rozdział 16
Zgodność z przepisami prawa i postanowieniami umownymi

§ 32. 1. W celu uniknięcia naruszenia obowiązujących przepisów prawa, zobowiązań ustawowych, postanowień zawartych umów i porozumień, jest prowadzona kontrola zgodności regulacji wewnętrznych oraz zasad bezpieczeństwa z ww. przepisami, w tym identyfikowanie, dokumentowanie i aktualizowanie wszystkich istotnych wymagań prawnych, regulacyjnych, umownych oraz podejścia organizacji do ich przestrzegania.

2. Przedmiotowa kontrola dotyczy również zgodności z wymaganiami prawnymi, regulacyjnymi i umownymi, związanymi z prawami własności intelektualnej i użytkowaniem prawnie zastrzeżonego oprogramowania.

3. Kierownicy komórek organizacyjnych, w zakresie zadań realizowanych zgodnie z Regulaminem organizacyjnym Urzędu Miasta Łodzi prowadzą bieżący nadzór w zakresie zgodności z przepisami prawa i postanowieniami umownymi.

4. Inspektor odpowiedzialny jest za zapewnienie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych.

5. Kierownik komórki organizacyjnej właściwej w sprawach ochrony danych osobowych, we współpracy z kierownikami poszczególnych komórek organizacyjnych dokonuje okresowych przeglądów regulacji wewnętrznych dotyczących bezpieczeństwa informacji w zakresie ich zgodności z przepisami prawa i postanowieniami umownymi, na zasadach i w trybie określonym w opracowanych dokumentach II i III poziomu bezpieczeństwa informacji.

6. Komórka organizacyjna właściwa ds. przeprowadzania audytów wewnętrznych i kontroli zapewnia okresowy audyt w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.

Rozdział 17
Odpowiedzialność za naruszenie bezpieczeństwa informacji

§ 33. 1. Nieprzestrzeganie zasad zawartych w dokumentacji bezpieczeństwa stanowi naruszenie obowiązków pracowniczych i może skutkować sankcjami natury dyscyplinarnej.

2. Naruszenie postanowień Polityki SZBI przez kontrahenta urzędu, w części go dotyczącej, może stanowić podstawę do odstąpienia od umowy i żądania pokrycia powstałej szkody lub zapłaty kary umownej, jeżeli taki obowiązek wynika z zawartej umowy.

3. Szczegółowe zasady dotyczące odpowiedzialności za naruszenie postanowień Polityki SZBI zostały uregulowane w opracowanych dokumentach II i III poziomu bezpieczeństwa informacji.

Rozdział 18
Dobór zabezpieczeń

§ 34. 1. Cele i dobór zabezpieczeń jest prowadzony w oparciu o aktualne wymogi prawa powszechnie obowiązującego, zalecenia polskich norm z rodziny ISO 27000 oraz wyniki monitorowania SZBI, w szczególności wyniki szacowania ryzyka w bezpieczeństwie informacji.

2. Stosowane zabezpieczenia fizyczne, techniczne i organizacyjne powinny uzupełniać się wzajemnie, zapewniając wymagany poziom bezpieczeństwa informacji.

3. Wykaz stosowanych zabezpieczeń opisany został w Deklaracji stosowania, stanowiącej załącznik Nr 1 do Polityki SZBI.

Rozdział 19
Utrzymywanie, monitorowanie i doskonalenie SZBI

§ 35. 1. Działania w zakresie utrzymania, monitorowania i doskonalenia SZBI mają charakter działań bieżących i okresowych i zostały opisane w załączniku Nr 2 do Polityki SZBI, a także w opracowanych dokumentach II i III poziomu bezpieczeństwa informacji.

2. W oparciu o wyniki prowadzonego monitorowania i nadzoru nad bezpieczeństwem informacji, podejmowane są adekwatne działania korekcyjne lub zapobiegawcze, mające na celu wyeliminowanie przyczyn niezgodności.

Załącznik Nr 1
do Polityki SZBI

Deklaracja stosowania

Wymagania PN-ISO/IEC 27001:2014-12 Załącznik A	Stosowana kontrola			Wybrane zabezpieczenia i powody stosowania zabezpieczeń				Uwagi (dokumenty, procedury, instrukcje)
	Wdrożone	Planowane wdrożenie	Wykluczone	Wymagania dot. funkcjonowania UML	Wymagania prawne	Dobre praktyki	Wyniki analizy ryzyka	
5 Polityki bezpieczeństwa informacji								
5.1 Kierunki bezpieczeństwa informacji określone przez kierownictwo								
5.1.1 Polityki bezpieczeństwa informacji	X			X	X			Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi.
5.1.2 Przegląd polityk bezpieczeństwa informacji	X			X	X			Załącznik Nr 2 do Polityki SZBI - Procedura monitorowania i nadzoru nad dokumentacją związaną z bezpieczeństwem informacji w Systemie Zarządzania Bezpieczeństwem Informacji Urzędu Miasta Łodzi.
6 Organizacja bezpieczeństwa informacji								
6.1 Organizacja wewnętrzna								
6.1.1 Role i odpowiedzialność za bezpieczeństwo informacji	X			X	X			Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi. Regulamin organizacyjny Urzędu Miasta Łodzi. Wszyscy pracownicy urzędu oraz podmioty współpracujące.
6.1.2 Rozdzielanie obowiązków	X			X	X	X		Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi. Kodeks Etyki pracowników Urzędu Miasta Łodzi. Zarządzenie Nr 7520/VII/17 Prezydenta Miasta Łodzi z dnia 21 grudnia 2017 r. w sprawie zasad składania i analizowania oświadczeń majątkowych, oświadczeń o prowadzeniu działalności gospodarczej, dodatkowym zatrudnieniu lub innej działalności zarobkowej.
6.1.3 Kontakty z organami władzy	X			X	X	X		Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi. Instrukcje bezpieczeństwa pożarowego i plany ewakuacji UML, telefony alarmowe, organy kontroli, organy nadzorcze, wymiar sprawiedliwości.
6.1.4 Kontakty z grupami zainteresowanych specjalistów	X				X	X		Urząd utrzymuje stosowne kontakty z grupami zainteresowanych specjalistów oraz innymi specjalistycznymi forami oraz stowarzyszeniami zawodowymi z obszaru bezpieczeństwa informacji: Unia Metropolii Polskich, Związek Miast Polskich, udział w

Wymagania PN-ISO/IEC 27001:2014-12 Załącznik A	Stosowana kontrola			Wybrane zabezpieczenia i powody stosowania zabezpieczeń				Uwagi (dokumenty, procedury, instrukcje)
	Wdrożone	Planowane wdrożenie	Wykluczone	Wymagania dot. funkcjonowania UML	Wymagania prawne	Dobre praktyki	Wyniki analizy ryzyka	
								konferencjach i szkoleniach
6.1.5 Bezpieczeństwo informacji w zarządzaniu projektami	X							Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi. Zarządzenie Nr 7052/VIII/21 Prezydenta Miasta Łodzi z dnia 22 kwietnia 2021 r. w sprawie określenia procedury wprowadzania zmian organizacyjnych i przeprowadzania czynności sprawdzających w Urzędzie Miasta Łodzi
6.2 Urządzenia mobilne i telepraca								
6.2.1 Polityka stosowania urządzeń mobilnych	X			X		X		Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi, konfiguracja, instrukcje wewnętrzne.
6.2.2 Telepraca	X			X	X	X	X	Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi, konfiguracja, instrukcje wewnętrzne. Zarządzenie Nr 4476/VIII/20 Prezydenta Miasta Łodzi z dnia 1 lipca 2020 r. w sprawie określenia zasad wykonywania pracy zdalnej w Urzędzie Miasta Łodzi
7 Bezpieczeństwo zasobów ludzkich								
7.1 Przed zatrudnieniem								
7.1.1 Postępowanie sprawdzające	X			X	X	X		Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi. Procedura naboru na wolne stanowiska urzędnicze w Urzędzie Miasta Łodzi
7.1.2 Warunki zatrudnienia	X			X		X		Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi, umowy z pracownikami, umowy z kontrahentami, Regulamin pracy w Urzędzie Miasta Łodzi Zasady podnoszenia wiedzy i kwalifikacji zawodowych przez pracowników Urzędu Miasta Łodzi
7.2 Podczas zatrudnienia								
7.2.1 Odpowiedzialność kierownictwa	X			X	X	X	X	Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi
7.2.2 Uświadomienie, kształcenie i szkolenie z zakresu bezpieczeństwa informacji	X			X	X	X		Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi - szkolenia na wszystkich szczeblach, podpisane oświadczenia o zapoznaniu się z dokumentacją Regulamin pracy w Urzędzie Miasta Łodzi. Zasady podnoszenia wiedzy i kwalifikacji zawodowych

Wymagania PN-ISO/IEC 27001:2014-12 Załącznik A	Stosowana kontrola			Wybrane zabezpieczenia i powody stosowania zabezpieczeń				Uwagi (dokumenty, procedury, instrukcje)
	Wdrożone	Planowane wdrożenie	Wykluczone	Wymagania dot. funkcjonowania UML	Wymagania prawne	Dobre praktyki	Wyniki analizy ryzyka	
								przez pracowników Urzędu Miasta Łodzi
7.2.3 Postępowanie dyscyplinarne	X			X	X	X	X	Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi Regulamin pracy w Urzędzie Miasta Łodzi.
7.3 Zakończenie i zmiana zatrudnienia								
7.3.1 Zakończenie zatrudnienia lub zmiana zakresu obowiązków	X			X	X	X		Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi. Regulamin pracy w Urzędzie Miasta Łodzi. Regulamin wynagradzania w Urzędzie Miasta Łodzi, karta obiegowa.
8. Zarządzanie aktywami								
8.1 Odpowiedzialność za aktywa								
8.1.1 Inwentaryzacja aktywów	X			X	X	X	X	Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi. Instrukcja obiegu dokumentów w zakresie rachunkowości dla Urzędu Miasta Łodzi. Instrukcja przeprowadzania i rozliczania inwentaryzacji składników majątkowych stanowiących własność Miasta Łodzi, będących w używaniu lub pod nadzorem komórek organizacyjnych Urzędu Miasta Łodzi.
8.1.2 Własność aktywów	X			X		X	X	Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi. Instrukcja obiegu dokumentów w zakresie rachunkowości dla Urzędu Miasta Łodzi. Instrukcja przeprowadzania i rozliczania inwentaryzacji składników majątkowych stanowiących własność Miasta Łodzi, będących w używaniu lub pod nadzorem komórek organizacyjnych Urzędu Miasta Łodzi.
8.1.3 Akceptowalne użycie aktywów	X			X		X		Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi.
8.1.4 Zwrot aktywów	X			X	X	X		Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi. Regulamin pracy w Urzędzie Miasta Łodzi, karta obiegowa.
8.2 Klasyfikacja informacji								
8.2.1 Klasyfikowanie informacji	X			X	X	X	X	Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi. Instrukcja kancelaryjna. Instrukcja archiwalna

Wymagania PN-ISO/IEC 27001:2014-12 Załącznik A	Stosowana kontrola			Wybrane zabezpieczenia i powody stosowania zabezpieczeń				Uwagi (dokumenty, procedury, instrukcje)
	Wdrożone	Planowane wdrożenie	Wykluczone	Wymagania dot. funkcjonowania UML	Wymagania prawne	Dobre praktyki	Wyniki analizy ryzyka	
8.2.2 Oznaczanie informacji			X					-
8.2.3 Postępowanie z aktywami	X			X	X	X	X	Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi. Instrukcja kancelaryjna. Instrukcja archiwalna. Upoważnienia do przetwarzania danych wraz z zakresem zadań związanych z przetwarzaniem danych osobowych.
8.3 Postępowanie z nośnikami								
8.3.1 Zarządzanie nośnikami wymiennymi	X			X		X	X	Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi. Instrukcja obiegu dokumentów w zakresie rachunkowości dla Urzędu Miasta Łodzi. Instrukcja przeprowadzania i rozliczania inwentaryzacji składników majątkowych stanowiących własność Miasta Łodzi, będących w używaniu lub pod nadzorem komórek organizacyjnych Urzędu Miasta Łodzi.
8.3.2 Wycofywanie nośników	X				X	X	X	Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi Instrukcja obiegu dokumentów w zakresie rachunkowości dla Urzędu Miasta Łodzi. Instrukcja przeprowadzania i rozliczania inwentaryzacji składników majątkowych stanowiących własność Miasta Łodzi, będących w używaniu lub pod nadzorem komórek organizacyjnych Urzędu Miasta Łodzi.
8.3.3 Przekazywanie nośników	X			X	X	X		Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi
9 Kontrola dostępu								
9.1 Wymagania biznesowe wobec kontroli dostępu								
9.1.1 Polityka kontroli dostępu	X			X	X	X	X	Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi Regulamin pracy w Urzędzie Miasta Łodzi.
9.1.2 Dostęp do sieci i usług sieciowych	X			X	X	X		Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi
9.2 Zarządzanie dostępem użytkowników								
9.2.1 Rejestrowanie użytkowników	X			X	X	X	X	Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi, upoważnienie do przetwarzania danych, podpis użytkownika,
9.2.2 Przydzielanie dostępu użytkownikom	X			X	X	X	X	Dokumentacja Systemu Zarządzania Bezpieczeństwem

Wymagania PN-ISO/IEC 27001:2014-12 Załącznik A	Stosowana kontrola			Wybrane zabezpieczenia i powody stosowania zabezpieczeń				Uwagi (dokumenty, procedury, instrukcje)
	Wdrożone	Planowane wdrożenie	Wykluczone	Wymagania dot. funkcjonowania UML	Wymagania prawne	Dobre praktyki	Wyniki analizy ryzyka	
								Informacji w Urzędzie Miasta Łodzi, upoważnienie do przetwarzania danych, podpis użytkownika
9.2.3 Zarządzanie prawami uprzywilejowanego dostępu	X			X	X	X	X	Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi, upoważnienie do przetwarzania danych.
9.2.4 Zarządzanie poufnymi informacjami uwierzytelniającymi użytkowników	X			X	X	X	X	Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi.
9.2.5 Przegląd praw dostępu	X			X	X	X	X	Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi.
9.2.6 Odbieranie lub dostosowywanie praw dostępu	X			X	X	X	X	Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi.
9.3 Odpowiedzialność użytkowników								
9.3.1 Stosowanie poufnych informacji uwierzytelniających	X			X	X	X	X	Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi.
9.4 Kontrola dostępu do systemów i aplikacji								
9.4.1 Ograniczanie dostępu do informacji	X			X	X	X		Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi, upoważnienia do przetwarzania danych.
9.4.2 Procedury bezpiecznego logowania	X			X	X	X		Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi, konfiguracja systemów.
9.4.3 System zarządzania hasłami	X			X	X	X		Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi.
9.4.4 Użycie uprzywilejowanych programów narzędziowych	X					X		Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi.
9.4.5 Kontrola dostępu do kodów źródłowych programów	X					X		Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi.
10. Kryptografia								
10.1 Zabezpieczenia kryptograficzne								
10.1 Polityka korzystania z zabezpieczeń kryptograficznych	X			X	X	X		Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi.
10.1.2 Zarządzanie kluczami	X			X	X	X		Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi.
11 Bezpieczeństwo fizyczne i środowiskowe								
11.1 Obszary bezpieczne								
11.1.1. Fizyczna granica obszaru bezpiecznego	X			X		X		Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi.

Wymagania PN-ISO/IEC 27001:2014-12 Załącznik A	Stosowana kontrola			Wybrane zabezpieczenia i powody stosowania zabezpieczeń				Uwagi (dokumenty, procedury, instrukcje)
	Wdrożone	Planowane wdrożenie	Wykluczone	Wymagania dot. funkcjonowania UML	Wymagania prawne	Dobre praktyki	Wyniki analizy ryzyka	
								Regulamin pracy w Urzędzie Miasta Łodzi.
11.1.2 Fizyczne zabezpieczenie wejść	X			X		X		Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi. Regulamin pracy w Urzędzie Miasta Łodzi, kontrola dostępu przez Straż Miejską w Łodzi oraz firmy zewnętrzne, monitoring wizyjny w wybranych obiektach.
11.1.3 Zabezpieczenie biur, pomieszczeń i urządzeń	X			X		X		Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi. Regulamin pracy w Urzędzie Miasta Łodzi, kontrola dostępu przez Straż Miejską w Łodzi oraz firmy zewnętrzne, monitoring wizyjny w wybranych obiektach.
11.1.4 Ochrona przed zagrożeniami zewnętrznymi i środowiskowymi	X			X		X		Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi. Regulamin pracy w Urzędzie Miasta Łodzi, kontrola dostępu przez Straż Miejską w Łodzi oraz firmy zewnętrzne, monitoring wizyjny w wybranych obiektach. Instrukcje bezpieczeństwa pożarowego i plany ewakuacji.
11.1.5 Praca w obszarach bezpiecznych	X			X		X		Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi.
11.1.6 Obszary dostaw i załadunku	X					X		Kontrola dostępu przez Straż Miejską w Łodzi.
11.2 Sprzęt								
11.2.1 Lokalizacja i ochrona sprzętu	X			X	X	X		Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi. Regulamin pracy w Urzędzie Miasta Łodzi, kontrola dostępu przez Straż Miejską w Łodzi oraz firmy zewnętrzne, monitoring wizyjny w wybranych obiektach.
11.2.2 Systemy wspomagające	X			X		X		Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi.
11.2.3 Bezpieczeństwo okablowania	X			X		X		Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi.
11.2.4 Konserwacja sprzętu	X			X		X		Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi.
11.2.5 Wynoszenie aktywów	X			X		X		Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi. Regulamin pracy w Urzędzie Miasta Łodzi.
11.2.6 Bezpieczeństwo sprzętu i aktywów poza siedzibą	X			X		X	X	Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi.
11.2.7 Bezpieczne zbywanie lub przekazywanie do	X			X		X	X	Dokumentacja Systemu Zarządzania Bezpieczeństwem

Wymagania PN-ISO/IEC 27001:2014-12 Załącznik A	Stosowana kontrola			Wybrane zabezpieczenia i powody stosowania zabezpieczeń				Uwagi (dokumenty, procedury, instrukcje)
	Wdrożone	Planowane wdrożenie	Wykluczone	Wymagania dot. funkcjonowania UML	Wymagania prawne	Dobre praktyki	Wyniki analizy ryzyka	
ponownego użycia								Informacji w Urzędzie Miasta Łodzi.
11.2.8 Pozostawienie sprzętu użytkownika bez opieki	X			X		X		Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi.
11.2.9 Polityka czystego biurka i czystego ekranu	X			X		X		Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi.
12 Bezpieczna eksploatacja								
12.1 Procedury eksploatacyjne i odpowiedzialność								
12.1.1 Dokumentowanie procedur eksploatacyjnych	X			X	X	X		Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi.
12.1.2 Zarządzanie zmianami	X			X		X	X	Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi. Zarządzenie Nr 7052/VIII/21 Prezydenta Miasta Łodzi z dnia 22 kwietnia 2021 r. w sprawie określenia procedury wprowadzania zmian organizacyjnych i przeprowadzania czynności sprawdzających w Urzędzie Miasta Łodzi.
12.1.3 Zarządzanie pojemnością	X					X		Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi.
12.1.4 Oddzielanie środowisk rozwojowych, testowych i produkcyjnych		X		X		X		Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi.
12.2 Ochrona przed szkodliwym oprogramowaniem								
12.2.1 Zabezpieczenia przed szkodliwym oprogramowaniem	X			X				Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi.
12.3 Kopie zapasowe								
12.3.1 Zapasowe kopie informacji	X			X	X	X	X	Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi.
12.4 Rejestrowanie zdarzeń i monitorowanie								
12.4.1 Rejestrowanie zdarzeń	X			X	X		X	Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi.
12.4.2 Ochrona informacji w dziennikach zdarzeń	X					X		Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi.
12.4.3 Rejestrowanie działań administratorów i operatorów	X				X	X	X	Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi.
12.4.4. Synchronizacja zegarów	X					X		Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi.
12.5 Nadzór nad oprogramowaniem produkcyjnym								
12.5.1 Instalacja oprogramowania w systemach produkcyjnych	X			X		X		Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi.

Wymagania PN-ISO/IEC 27001:2014-12 Załącznik A	Stosowana kontrola			Wybrane zabezpieczenia i powody stosowania zabezpieczeń				Uwagi (dokumenty, procedury, instrukcje)
	Wdrożone	Planowane wdrożenie	Wykluczone	Wymagania dot. funkcjonowania UML	Wymagania prawne	Dobre praktyki	Wyniki analizy ryzyka	
12.6 Zarządzanie podatnościami technicznymi								
12.6.1 Zarządzanie podatnościami technicznymi	X			X	X	X		Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi.
12.6.2 Ograniczenia w instalowaniu oprogramowania	X			X	X	X	X	Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi.
12.7 Rozważania dotyczące audytu systemów informacyjnych								
12.7.1 Zabezpieczenia audytu systemów informacyjnych	X			X	X	X		Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi. Regulamin kontroli.
13 Bezpieczeństwo komunikacji								
13.1 Zarządzanie bezpieczeństwem sieci								
13.1.1 Zabezpieczenia sieci	X			X	X		X	Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi.
13.1.2 Bezpieczeństwo usług sieciowych	X			X			X	Umowy
13.1.3 Rozdzielanie sieci	X			X		X		Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi.
13.2 Przesyłanie informacji								
13.2.1 Polityki i procedury przesyłania informacji	X			X	X	X	X	Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi.
13.2.2 Porozumienia dotyczące przesyłania informacji	X			X		X		Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi.
13.2.3 Wiadomości elektroniczne	X			X	X			Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi.
13.2.4 Umowy o zachowaniu poufności	X			X		X		Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi.
14 Pozyskiwanie, rozwój i utrzymanie systemów								
14.1 Wymagania związane z bezpieczeństwem systemów informacyjnych								
14.1.1 Analiza i specyfikacja wymagań dla bezpieczeństwa informacji	X			X	X	X		Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi. Regulamin udzielania zamówień publicznych w Urzędzie Miasta Łodzi. Regulamin udzielania zamówień publicznych, których wartość szacunkowa nie przekracza kwoty 130 000 PLN. Zasady stosowania klauzul społecznych i środowiskowych w zamówieniach publicznych w Urzędzie Miasta Łodzi.

Wymagania PN-ISO/IEC 27001:2014-12 Załącznik A	Stosowana kontrola			Wybrane zabezpieczenia i powody stosowania zabezpieczeń				Uwagi (dokumenty, procedury, instrukcje)
	Wdrożone	Planowane wdrożenie	Wykluczone	Wymagania dot. funkcjonowania UML	Wymagania prawne	Dobre praktyki	Wyniki analizy ryzyka	
14.1.2 Zabezpieczenie usług aplikacyjnych w sieciach publicznych	X			X	X	X		Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi.
14.1.3 Ochrona transakcji usług aplikacyjnych	X			X	X	X		Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi.
14.2 Bezpieczeństwo w procesach rozwoju i wsparcia								
14.2.1 Polityka bezpieczeństwa prac rozwojowych	X			X		X		Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi.
14.2.2 Procedury kontroli zmian w systemach	X			X		X		Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi.
14.2.3 Przegląd techniczny aplikacji po zmianach w platformie produkcyjnej	X			X		X		Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi.
14.2.4 Ograniczenia dotyczące zmian w pakietach oprogramowania	X			X		X		Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi
14.2.5 Zasady projektowania bezpiecznych systemów	X			X		X		Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi.
14.2.6 Bezpieczne środowisko rozwojowe	X			X		X		Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi.
14.2.7 Prace rozwojowe zlecane podmiotom zewnętrznym	X			X		X		Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi.
14.2.8 Testowanie bezpieczeństwa systemów		X		X		X		-
14.2.9 Testy akceptacyjne systemów		X		X		X		-
14.3 Dane testowe								
14.3.1 Ochrona danych testowych	X					X		Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi.
15 Relacje z dostawcami								
15.1 Bezpieczeństwo informacji w relacjach z dostawcami								
15.1.1. Polityka bezpieczeństwa informacji w relacjach z dostawcami	X			X	X	X		Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi, umowy.
15.1.2 Uwzględnienie bezpieczeństwa w porozumieniach z dostawcami	X			X	X	X		Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi, umowy.
15.1.3 Łańcuch dostaw technologii informacyjnych i telekomunikacyjnych	X			X	X	X		Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi, umowy.
15.2 Zarządzanie usługami dostarczanymi przez dostawców								
15.2.1 Monitorowanie i przegląd usług świadczonych przez dostawców	X			X		X		Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi, protokoły odbioru,

Wymagania PN-ISO/IEC 27001:2014-12 Załącznik A	Stosowana kontrola			Wybrane zabezpieczenia i powody stosowania zabezpieczeń				Uwagi (dokumenty, procedury, instrukcje)
	Wdrożone	Planowane wdrożenie	Wykluczone	Wymagania dot. funkcjonowania UML	Wymagania prawne	Dobre praktyki	Wyniki analizy ryzyka	
								umowy.
15.2.2 Zarządzanie zmianami w usługach świadczonych przez dostawców	X			X		X		Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi, umowy.
16 Zarządzanie incydentami związanymi z bezpieczeństwem informacji								
16.1 Zarządzanie incydentami związanymi z bezpieczeństwem informacji oraz udoskonaleniami								
16.1.1 Odpowiedzialność i procedury	X			X		X		Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi.
16.1.2 Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji	X			X		X		Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi.
16.1.3 Zgłaszanie słabości związanych z bezpieczeństwem informacji	X			X		X		Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi.
16.1.4 Ocena i podejmowanie decyzji w sprawie zdarzeń związanych z bezpieczeństwem informacji	X			X		X		Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi.
16.1.5 Reagowanie na incydenty związane z bezpieczeństwem informacji	X			X		X		Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi.
16.1.6 Wyciąganie wniosków z incydentów związanych z bezpieczeństwem informacji	X			X		X		Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi.
16.1.7 Gromadzenie materiału dowodowego	X			X		X		Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi.
17 Aspekty bezpieczeństwa informacji w zarządzaniu ciągłością działania								
17.1 Ciągłość bezpieczeństwa informacji								
17.1.1 Planowanie ciągłości bezpieczeństwa informacji	X			X		X		Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi.
17.1.2 Wdrożenie ciągłości bezpieczeństwa informacji	X			X		X		Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi.
17.1.3 Weryfikowanie, przegląd i ocena ciągłości bezpieczeństwa informacji	X			X		X		Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi.
17.2 Nadmiarowość								
17.2.1 Dostępność środków przetwarzania informacji	X			X		X		Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi.
18 Zgodność								
18.1 Zgodność z przepisami prawnymi i umownymi								
18.1.1 Określenie stosownych wymagań prawnych i umownych	X			X	X			Ustawy, rozporządzenia, uchwały, zarządzenia, źródła prawa w UE.

Wymagania PN-ISO/IEC 27001:2014-12 Załącznik A	Stosowana kontrola			Wybrane zabezpieczenia i powody stosowania zabezpieczeń				Uwagi (dokumenty, procedury, instrukcje)
	Wdrożone	Planowane wdrożenie	Wykluczone	Wymagania dot. funkcjonowania UML	Wymagania prawne	Dobre praktyki	Wyniki analizy ryzyka	
								Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi
18.1.2 Prawa do własności intelektualnej	X			X	X			Ustawa o prawie autorskim i prawach pokrewnych i in.
18.1.3 Ochrona zapisów organizacji	X				X			Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi.
18.1.4 Prywatność i ochrona danych identyfikujących osobę	X				X			Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi, upoważnienia do przewarzania danych, oświadczenie o zachowaniu poufności.
18.1.5 Regulacje dotyczące zabezpieczeń kryptograficznych	X			X	X	X		Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi.
18.2 Przeglądy bezpieczeństwa informacji								
18.2.1 Niezależny przegląd bezpieczeństwa informacji	X				X			Kontrole zewnętrzne.
18.2.2 Zgodność z politykami bezpieczeństwa i normami	X			X				Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi Audyt wewnętrzny i kontrola.
18.2.3 Sprawdzanie zgodności technicznej	X			X		X		Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Łodzi.