Załącznik Nr 2 do Zarządzenia nr 134/2023
Wojewody Łódzkiego z 5 lipca 2023 r.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM DLA ŁÓDZKIEGO URZĘDU WOJEWÓDZKIEGO W ŁODZI

§ 1. Cel opracowania dokumentu i zawartość dokumentu:

1) Instrukcja Zarządzania Systemem Informatycznym określa podstawowe zasady, których realizacja ma na celu ochronę systemu informatycznego Łódzkiego Urzędu Wojewódzkiego w Łodzi, przetwarzanych w nim danych oraz określenie obowiązków pracowników Urzędu korzystających z tych zasobów. Jako system informatyczny Urzędu należy rozumieć sumę wszystkich elementów składających się na informatyczne środowisko pracy Urzędu. W pojęciu systemu informatycznego Urzędu zawierają się wszystkie elementy infrastruktury fizycznej i logicznej niezbędne do jego działania, w tym również informatyczne systemy dziedzinowe niezbędne do realizacji zadań merytorycznych;
2) zasady zawarte w tym dokumencie dotyczą również urządzeń przenośnych takich jak telefony, tablety, komputery przenośne, o ile możliwe jest ich zastosowanie.

§ 2. Postanowienia ogólne:

1) za zorganizowanie komputerowego stanowiska pracy, ustawienie urządzenia, zapewnienie bezpieczeństwa danych wykorzystywanych na stanowisku pracy oraz prawidłową eksploatację sprzętu komputerowego przydzielonego do poszczególnych komórek organizacyjnych i zespołów odpowiedzialni są Dyrektorzy wydziałów/równorzędnych komórek organizacyjnych lub osoby przez nich wyznaczone;
2) bezpośrednio odpowiedzialnym za bezpieczeństwo i dostęp do komputerowego stanowiska pracy oraz prawidłową eksploatację systemu jest użytkownik stanowiska;
3) dopuszcza się utworzenie dedykowanych polityk bezpieczeństwa i instrukcji zarządzania systemem informatycznym rozszerzających zasady bezpieczeństwa dla wybranych systemów;
4) sprzęt informatyczny będący własnością Urzędu powinien być wykorzystywany tylko i wyłączne do realizacji zadań służbowych;
5) pracownicy Urzędu, wykonawcy i użytkownicy reprezentujący stronę trzecią, powinni zwrócić przydzielony im sprzęt: pracownicy Urzędu w momencie zakończenia stosunku pracy, pozostali po zakończeniu kontraktu, umowy lub innych czynności wykonywanych na rzecz Urzędu;
6) rozliczenie przydzielonego sprzętu następuje:
   a) w odniesieniu do pracowników - w formie karty obiegowej,
   b) dla stron trzecich, na podstawie odpowiednich zabezpieczeń zawartych w treści umowy.

§ 3. Monitorowanie bezpieczeństwa systemu informatycznego:

1) podstawowy system monitorowania bezpieczeństwa opiera się na mechanizmach wbudowanych w kontroler domeny Active Directory. O ile to możliwe systemy informatyczne używają

mechanizmów autoryzacji zintegrowanych z Active Directory (LDAP);

2) dzienniki zdarzeń domeny Active Directory gromadzą dane dotyczące rozpoczynania pracy (logowanie się użytkowników do systemu) w tym udanych i nieudanych logowań wraz z datą i czasem wystąpienia zdarzenia;
3) komputery używane w Urzędzie wykorzystują systemy operacyjne Windows zapewniające tworzenie dzienników zdarzeń. W dziennikach zdarzeń rejestrowane są zdarzenia dotyczące: aplikacji (informacje o ostrzeżeniach systemowych i błędach), zabezpieczeń, instalacji aktualizacji oprogramowania systemowego, działania systemu operacyjnego;
4) dzienniki zdarzeń są prowadzone bezpośrednio na serwerach i komputerach, których dotyczą rejestrowane zdarzenia. Dzienniki zdarzeń powinny zawierać informacje obejmujące ostatnie dwa lata pracy systemu, a dla systemów nowych od chwili ich uruchomienia;
5) dzienniki zdarzeń serwerów są analizowane przez wyznaczonego pracownika właściwego oddziału ds. informatyzacji nie rzadziej niż raz w miesiącu. Raport z analizy dzienników zdarzeń serwerów przedstawiany jest kierownikowi właściwego oddziału ds. informatyzacji oraz udostępniany do wiadomości ASI. Za zabezpieczenie i przechowywanie dzienników zdarzeń serwerów odpowiada właściwy oddział ds. informatyzacji;
6) fizyczny dostęp do węzłów sieci i serwerowni jest dokumentowany odrębnie dla każdego punktu poprzez elektroniczny system kontroli dostępu bądź Dziennik wejść. Dziennik wejść zawiera informacje takie jak: numer porządkowy, data wejścia, godzina wejścia, godzina wyjścia, imię i nazwisko osoby wchodzącej, oznaczenie instytucji, cel wejścia, podpis osoby wchodzącej. Dostęp do węzłów sieci oraz serwerowni posiadają pracownicy właściwego oddziału ds. informatyzacji lub inne osoby upoważnione;
7) monitorowanie obszarów aktywności i działań użytkowników systemu komputerowego jest realizowane przez właściwy oddział ds. informatyzacji.

§ 4. Zabezpieczenia systemów informatycznych:

1) system informatyczny urzędu opiera się na środowisku serwerowym zapewniającym redundancję na poziomie n+1. Awaria pojedynczego elementu, zapewniającego moc obliczeniową, lub pamięci masowej nie może zatrzymać pracy systemu. Przełączenie na elementy zapasowe ma być realizowane w sposób nieodczuwalny dla użytkowników;
2) elementy systemu, dla których w przypadku awarii nie ma możliwości zastosowania mechanizmów automatycznie przełączających pracę systemu na urządzenia sprawne, zaleca się posiadanie urządzeń zapasowych, tak by czas zatrzymania usług był możliwie najkrótszy;
3) zabezpieczenia systemów informatycznych opierają się na kontach użytkowników przypisanych

do pracowników Urzędu oraz poziomach uprawnień dostępu. Nowe konta są tworzone na podstawie *Wniosku o założenie konta użytkownika systemu teleinformatycznego Łódzkiego Urzędu Wojewódzkiego w Łodzi* w systemie EZD, przez właściwy oddział ds. informatyzacji.

4) działanie serwerów jest zabezpieczone poprzez podłączenie do awaryjnej sieci energetycznej oraz do generatora prądu. Ponadto serwery są podpięte do zasilacza UPS.

§ 5. Przeglądy i konserwacja systemów oraz nośników informacji służących do przetwarzania danych:

1) konserwacje i naprawy sprzętu komputerowego prowadzone są przez podmioty zewnętrzne na podstawie odrębnych umów. Umowy określają terminy i zasady przekazywania i odbierania naprawianego sprzętu. W przypadkach nie przewidzianych w umowach naprawy realizowane są na podstawie odrębnych zleceń;
2) podmiot zewnętrzny, mający dostęp do systemu informatycznego i danych ŁUW powinien posiadać w umowie klauzulę o poufności i nieujawnianiu informacji;
3) podmiot zewnętrzny jest zobowiązany do zapewnienia ochrony danych pozyskanych lub udostępnionych mu w związku z wykonywaniem umowy, na zasadach obowiązujących przepisów praw oraz polityk, instrukcji lub innych regulacji, obowiązujących w ŁUW;
4) urządzenia i systemy informatyczne podmiotu zewnętrznego, na których będą przetwarzane dane, pozyskane lub udostępnione w związku z wykonywaniem umowy, winny spełniać wymagania odpowiednie techniczne;
5) w podmiocie zewnętrznym w związku z wykonywaniem umowy może być przeprowadzany audyt, w celu sprawdzenia np. polityki bezpieczeństwa, dystrybucji haseł, punktów styku dostawca-użytkownik;
6) uszkodzone dyski twarde i inne równoważne nośniki danych naprawiane na podstawie umów gwarancyjnych są pozostawiane w właściwym oddziale ds. informatyzacji;
7) z nieprzydatnego sprzętu (likwidowanego) właściwy oddział ds. informatyzacji wymontowuje nośniki danych;
8) uszkodzone lub wymontowane z likwidowanego sprzętu dyski twarde i inne równoważne nośniki danych przechowywane są min. 30 dni i maksimum 180 dni. Następnie są niszczone mechanicznie w właściwym oddziale ds. informatyzacji. Z czynności niszczenia powstaje protokół w postaci elektronicznej lub papierowej zawierający m.in. informację o niszczonym nośniku oraz imię i nazwisko pracownika odpowiedzialnego za zniszczenie;
9) przeglądy i konserwacje sprzętu komputerowego oraz nośników informacji, przeprowadzane są w pomieszczeniach obszaru, o którym mowa w Polityce Bezpieczeństwa Informacji, przy udziale

pracownika właściwego oddziału ds. informatyzacji;

10) w przypadku przekazywania do naprawy sprzętu komputerowego nośniki zawierające dane są demontowane przed przekazaniem do naprawy lub są naprawiane pod nadzorem pracownika właściwego oddziału ds. informatyzacji.

§ 6. Usuwanie danych lub informacji z nośników:

1) dane zapisane na nośnikach muszą zastać usunięte poprzez nadpisanie obszarów nośnika zawierających usuwane dane. Nadpisanie może być wykonane bezpośrednio przez użytkownika lub po przekazaniu nośnika, przez pracownika właściwego oddziału ds. informatyzacji. Informacje o prawidłowym sposobie usuwania danych można uzyskać w właściwym oddziale ds. informatyzacji;
2) w przypadku nośników nie pozwalających na nadpisanie, nośnik należy przekazać do zniszczenia mechanicznego w właściwym oddziale ds. informatyzacji.

§ 7. Nośniki wymienne i zasady ich użytkowania:

1) przed rozpoczęciem przetwarzania danych dostarczonych z zewnątrz w postaci elektronicznej, na nośniku danych elektronicznych, należy zgłosić w systemie EZD chęć sprawdzenia danego nośnika. Pracownik właściwego oddziału ds. informatyzacji podejmuje stosowne działania celem sprawdzenia nośnika pod względem bezpieczeństwa. Po uzyskaniu zgody od pracownika właściwego oddziału ds. informatyzacji możliwe jest używanie nośnika na komputerze;
2) ze względów bezpieczeństwa wprowadza się zakaz samodzielnego podłączania do komputerów Urzędu wszelkiego typu nośników danych pochodzących spoza Urzędu, używających do komunikacji portu USB lub protokołów komunikacyjnych właściwych dla magistrali USB (pendrive, dysk przenośny, telefon, karty pamięci, itp.). W przypadku otrzymania danych na takim nośniku, należy postępować zgodnie z punktem 1;
3) w przypadku przekazania/przyjmowania danych na nośnikach jednorazowych (tj. płyty CD/DVD i inne) należy po użyciu nośniki zniszczyć, jeżeli wymagają tego przepisy. Niszczenie tych nośników odbywa się we właściwym oddziale ds. informatyzacji;
4) w przypadku użycia nośników wielokrotnego zapisu obowiązkiem użytkownika po wykorzystaniu jest skasowanie uzyskanej informacji albo zamazanie nośnika przy użyciu programów nadpisujących lub poprzez zapisanie na nim informacji wypełniających całą przestrzeń dostępną do zapisu. Informacje o prawidłowym sposobie nadpisywania nośników można uzyskać w właściwym oddziale ds. informatyzacji;
5) w przypadku transportu danych na przenośnych nośnikach danych (np. pendrive, CD/DVD,

laptop) należy stosować zabezpieczenia (np. szyfrowanie lub zabezpieczenie hasłem) uzgodnione wcześniej z Administratorem Systemu Informatycznego.

§ 8. Bezpieczeństwo sprzętu mobilnego poza siedzibą Urzędu:

1) zasady korzystania ze sprzętu mobilnego określa stosowne Zarządzenie Dyrektora Generalnego Łódzkiego Urzędu Wojewódzkiego w Łodzi;
2) w zależności od możliwości sprzętu mobilnego należy stosować zabezpieczenia przed uruchomieniem urządzenia oraz odczytem danych przez osoby nieuprawnione. Za takie zabezpieczenia należy rozumieć wymóg podania hasła, kodu, wzoru, itp. przed uruchomieniem lub rozpoczęciem pracy z urządzeniem, szyfrowanie nośników danych uniemożliwiających odczyt informacji po wyjęciu z zabezpieczonego urządzenia. Zabezpieczenia będą aktywowane przez właściwy oddział ds. informatyzacji przy przekazywaniu sprzętu do użytkowania. Na urządzeniach wprowadzonych do eksploatacji przed wejściem w życie niniejszej Instrukcji, zabezpieczenia będą aktywowane przy obsłudze zgłoszeń serwisowych.

§ 9. Aktywacja kont w systemie informatycznym:

1) konta użytkowników systemu informatycznego Urzędu są aktywne od chwili założenia konta do dnia zakończenia pracy wskazanego we *Wniosku o założenie konta użytkownika systemu teleinformatycznego Łódzkiego Urzędu Wojewódzkiego w Łodzi* w systemie EZD;
2) wszyscy pracownicy Urzędu muszą złożyć oświadczenie o odpowiedzialności za naruszenie praw autorskich twórców (właścicieli) oprogramowania (załącznik nr 1 do niniejszej Instrukcji). Oświadczenia przechowywane są w właściwym oddziale ds. kadr w teczkach osobowych. Oświadczenia składane są przez pracowników przyjętych do pracy przy podpisywaniu umowy o pracę. W przypadku pracowników już zatrudnionych, którzy nie złożyli stosownych oświadczeń, właściwy oddział ds. kadr zbierze oświadczenia w ciągu miesiąca od dnia wejścia w życie niniejszej Instrukcji.

§ 10. Stosowane metody i środki uwierzytelniania oraz procedury związane z zarządzaniem i użytkowaniem systemu informatycznego Urzędu:

1) użytkownik systemu informatycznego dysponuje unikalną nazwą użytkownika i znanym wyłącznie sobie hasłem;
2) zalogowanie się użytkownika do systemu jest możliwe po podaniu loginu i prawidłowego hasła. Wszystkie stanowiska komputerowe w domenie Active Directory posiadają odrębne konta. W przypadku nieużywania stanowiska przez ponad 90 dni konto urządzenia zostaje automatycznie

wyłączone;

3) zabrania się udostępniania osobistego hasła innym pracownikom oraz pozostawiania w miejscu, w którym mogłoby zostać ujawnione;
4) bez względu na okoliczności użytkownik nie może ujawniać swojego hasła do systemu, jakimkolwiek osobom;
5) w przypadku długotrwałej nieobecności pracownika przełożony może wnioskować o umożliwienie dostępu do konta tegoż pracownika, poprzez zmianę hasła;
6) jeśli istnieje podejrzenie, że hasło zostało ujawnione, należy je natychmiast zmienić;
7) hasło używane w Urzędzie musi mieć minimum 8 znaków wybranych ze zbiorów: A-Z, a-z, 0-9, znaki specjalne. Do utworzenia prawidłowego hasła należy wykorzystać znaki z trzech powyżej przedstawionych zbiorów. Hasło nie może zawierać imienia, nazwiska lub loginu użytkownika. Przykładowe hasła spełniające wymogi ma następującą postać: T@k-wygl@da- haslo-26;
8) czas ważności hasła wynosi 90 dni. Po upływie tego terminu system wymusza zmianę hasła.

§ 11. Zabezpieczenie oprogramowania:

1) na serwerach i komputerach stacjonarnych oprogramowanie jest instalowane przez właściwy oddział ds. informatyzacji. W przypadku korzystania z komputera przenośnego, użytkownik otrzymuje komputer z zainstalowanym oprogramowaniem. Za dodatkowo zainstalowane lub uruchamiane oprogramowanie odpowiada użytkownik;
2) domyślnie Użytkownicy nie posiadają uprawnień umożliwiających modyfikację uprawnień i oprogramowania. Dla systemów posiadających odrębne mechanizmy autoryzacji możliwe jest nadawanie uprawnień nie dziedziczonych z Active Directory. Możliwe jest przypisanie uprawnień administracyjnych dla osób merytorycznie obsługujących system;
3) w przypadku gdy do uruchomienia aplikacji wymagany jest wyższy poziom uprawnień niż standardowy możliwe jest przypisanie dodatkowego konta lub uprawnień w celu umożliwienia pracy do czasu uzgodnienia z dostawcą aplikacji sposobu pracy w ramach standardowych uprawnień;
4) kierownik właściwego oddziału ds. informatyzacji przygotuje instrukcję wyłączenia i włączenia systemu informatycznego oraz techniczne konto administracyjne. Instrukcja zawiera wszystkie dane administracyjne umożliwiające pełne zarządzanie wszystkimi składowymi systemu informatycznego. Instrukcja będzie przechowywana w zamkniętym sejfie w wydziale właściwym ds. informatyzacji w pomieszczeniu serwerowni.

§ 12. Systemy wspomagające:

1) systemy wspomagające zarządzanie systemem stosuje się z uwagi na rozmiar i dużą ilość użytkowników oraz urządzeń pracujących w systemie informatycznym Urzędu. System może wspomagać zarządzanie oprogramowaniem, aktualizacjami, licencjami, uprawnieniami i kontami użytkowników itp. Oprogramowanie może pełnić również funkcje monitorujące stan urządzeń, ich konfigurację oraz czynności wykonywane przez użytkowników. Za użycie systemów wspomagających zgodnie z przeznaczeniem odpowiada właściwy oddział ds. informatyzacji.

§ 13. Procedura nadawania uprawnień oraz rejestrowania tych uprawnień w systemie informatycznym:

1) do pracy w systemie informatycznym Urzędu wymagane jest konto użytkownika domeny Active Directory. Użytkownicy otrzymują najniższy możliwy poziom uprawnień wystarczający do pracy;
2) za prawidłowość nadawania uprawnień w domenie Active Directory odpowiada kierownik właściwego oddziału ds. informatyzacji;
3) konta użytkowników są zorganizowane w grupach, dla których mogą być nakładane uprawnienia dedykowane dla całej grupy;
4) dla systemów merytorycznych niezintegrowanych z domeną Active Directory stosowana jest dwustopniowa autoryzacja. Wymagane jest zalogowanie się do komputera kontem domeny Active Directory, następnie po uruchomieniu systemu merytorycznego zalogowanie się kontem systemowym. Za nadawanie uprawnień do systemu merytorycznego odpowiada administrator tego systemu. Administratorzy systemu są wyznaczani na etapie wdrożenia spośród przeszkolonych do realizacji tego zadania pracowników Urzędu;
5) uprawnienia do systemów informatycznych nadawane są przez osoby posiadające uprawnienia administratora systemu na podstawie *Wniosku o założenie konta użytkownika systemu teleinformatycznego Łódzkiego Urzędu Wojewódzkiego w Łodzi* podpisanego przez kierownika komórki organizacyjnej. Dla systemów udostępnianych Urzędowi przez inne jednostki sposób nadawania uprawnień i wzory wniosków są określone przez administratorów tych systemów;
6) informacje o uprawnieniach użytkowników przechowywane są odpowiednio dla systemu informatycznego Urzędu w domenie Active Directory, dla systemu merytorycznego w bazach danych danego systemu.

§ 14. Rozpoczęcie, przerwy i zakończenie pracy w systemach informatycznych:

1) rozpoczęcie pracy w systemie informatycznym wymaga podania nazwy użytkownika i hasła;
2) odchodząc od stanowiska pracy pracownik ma obowiązek zablokowania swojego stanowiska pracy. W systemach Windows komputerowe stanowisko pracy blokuje się kombinacją klawiszy

Start+L („logo Windows”+L). Powracając do pracy stanowisko zostanie odblokowane poprzez podanie hasła użytkownika, który stanowisko zablokował;

3) zakończenie pracy w systemie informatycznym polega na wylogowaniu się z systemu lub wyłączeniu komputera;
4) wyłączenie komputera wymaga użycia funkcji systemu operacyjnego rozpoczynającej proces wyłączenia;
5) komputerowe stanowiska pracy blokują się automatycznie maksymalnie po 10 minutach bezczynności;
6) zabrania się spożywania posiłków i picia napojów w pobliżu komputerów.

§ 15. Zabezpieczenie antywirusowe:

1) komputerowe stanowiska pracy w Łódzkim Urzędzie Wojewódzkim w Łodzi objęte są ochroną antywirusową;
2) komputery pracujące w sieci lokalnej korzystają z oprogramowania antywirusowego aktualizowanego z lokalnego serwera aktualizacji.

§ 16. Kopie bezpieczeństwa:

1) kopiami bezpieczeństwa objęte są wszystkie bazy danych przetwarzanych przez serwery Urzędu, wszystkie pliki użytkowników na serwerach plików, pliki dysków twardych serwerów wirtualnych;
2) system realizujący kopie bezpieczeństwa musi być umieszczony w pomieszczeniu zabezpieczonym przed dostępem osób nieupoważnionych. Kopie wykonywane są poza godzinami pracy Urzędu;
3) kopie bezpieczeństwa na stanowiskach komputerowych nie są wykonywane. Jeżeli zachodzi potrzeba zabezpieczenia danych na stanowisku komputerowym podłączonym do sieci komputerowej, należy skopiować dane na serwer plików. W przypadku braku takiej możliwości należy wykonać kopię na nośniku danych;
4) dodatkowa kopia danych przechowywana jest w innej strefie pożarowej oddalonej od strefy pożarowej, w której pracuje system realizujący kopie zapasowe;
5) kopie wykonywane są automatycznie poza godzinami pracy Urzędu, tj. między godziną 17:00 a 7:00 oraz całodobowo w soboty i niedziele. W czasie wykonywania kopii bezpieczeństwa dostęp do systemu informatycznego lub jego składowych może być spowolniony lub niemożliwy;
6) za prawidłowość wykonania kopii bezpieczeństwa odpowiada właściwy oddział ds. informatyzacji. Weryfikacja wykonanej kopii zapasowej odbywa się automatycznie

po zakończeniu procesu zapisu danych. Poprawność procesu wykonywania kopii zapasowych jest sprawdzana co najmniej raz na dwa tygodnie przez wyznaczonego pracownika właściwego oddziału ds. informatyzacji. Raporty informujące o stanie systemu wykonywania kopii zapasowych przesyłane są kierownikowi właściwego oddziału ds. informatyzacji oraz ASI.

§ 17. Wydruki:

1) w Urzędzie używa się urządzeń wielofunkcyjnych w systemie druku centralnego. Drukarki, kserokopiarki lub urządzenia wielofunkcyjne dla pojedynczych użytkowników są instalowane tylko w przypadkach szczególnie uzasadnionych ze względów organizacyjnych i technicznych;
2) Skorzystanie z urządzeń w systemie druku centralnego możliwe jest wyłącznie po zalogowaniu się na indywidulane konto zsynchronizowane z domeną Active Directory poprzez kartę RCP.
3) W systemie druku centralnego prowadzone jest monitorowanie wydruków . Monitorowaniu podlega treść i ilość stron wydruku. W przypadku wykrycia nadużyć podjęte zostaną czynności wyjaśniające;
4) pracownik Urzędu uruchamiający proces wydruku odpowiedzialny jest za ustawienia parametrów wydruku oraz za wydrukowane materiały. Po wydrukowaniu należy niezwłocznie odebrać wydruk;
5) niepotrzebne wydruki zawierające dane chronione należy niszczyć przy pomocy niszczarek dokumentów. Zabrania się niszczyć wydruki w inny sposób.
6) Po zakończeniu korzystania z urządzeń w druku centralnym należy się z nich niezwłocznie wylogować.

§ 18. Komunikacja w sieciach komputerowych:

1) współcześnie używane systemy informatyczne opierają się na wymianie danych między elementami systemu poprzez sieć komputerową. Sieć Urzędu korzysta z protokołu komunikacyjnego IPv4 oraz IPv6. Do zarządzania użytkownikami i urządzeniami używana jest usługa katalogowa Active Directory;
2) na komputerowych stanowiskach pracy zainstalowane jest oprogramowanie umożliwiające zdalną pomoc. Użycie modułu zdalnego dostępu może nastąpić po zgłoszeniu usterki do właściwego oddziału ds. informatyzacji i ustaleniu adresu IP (adres identyfikujący komputer w sieci) lub nazwy komputera;
3) do zabezpieczenia punktu styku lokalnej sieci komputerowej z siecią Internet używany jest firewall sprzętowy. Dopuszczona jest wymiana informacji na portach i adresach IP wykorzystywanych do pracy w Urzędzie. Usługi i porty nieużywane w Urzędzie są zablokowane;

4) dozwolone jest korzystanie ze służbowych skrzynek poczty elektronicznej. Użytkownik powinien regularnie sprawdzać zawartość poczty elektronicznej. Konta poczty elektronicznej nie używane przez okres dłuższy niż 6 miesięcy będą usuwane;
5) adresy e-mail są zakładane dla wszystkich pracowników Urzędu. Adresy e-mail mają postać imię.nazwisko@lodz.uw.gov.pl . W przypadku zatrudnienia osoby o tym samym imieniu i nazwisku w adresie e-mail po nazwisku dodana zostaje liczba, np. anna.nowak7@lodz.uw.gov.pl;
6) przy korzystaniu z poczty elektronicznej należy zachować szczególną ostrożność w związku z możliwością przechwycenia korespondencji przez osoby nieuprawnione;
7) pocztę elektroniczną należy traktować, jako uzupełniający kanał wymiany informacji o niskiej wiarygodności;
8) za treści wysyłane pocztą elektroniczną odpowiada osoba, z której konta wiadomość jest wysyłana;
9) w przypadku otrzymania wiadomości e-mail nakłaniającej do uruchomienia lub otworzenia załącznika należy zachować szczególną ostrożność. Zaleca się przekazanie ww. wiadomości w celu ich sprawdzenia na adres zbti@lodz.uw.gov.pl. Właściwy oddział ds. informatyzacji analizuje niechciane wiadomości (tzw. spam) i ustawia filtry, aby ograniczyć ilość przychodzącej niechcianej poczty;
10) z uwagi na możliwość użycia tożsamości znanego nadawcy, wiadomości o treści niewiarygodnej lub budzącej wątpliwości, należy potwierdzić innym kanałem (np. telefonicznie);
11) hasło do służbowej poczty elektronicznej musi być unikalne, inne niż hasło do systemu informatycznego Urzędu oraz inne niż hasła używane w celach prywatnych. Zabrania się przekazywania hasła innym osobom. Za bezpieczeństwo konta e-mail odpowiada bezpośrednio użytkownik, do którego konto jest przypisane;
12) Internet jest traktowany jako źródło informacji, w związku z tym możliwe jest korzystanie z jego zasobów w sposób ograniczający się do celów służbowych;
13) komunikacja elektroniczna prowadzona przy użyciu sieci komputerowej Urzędu może być monitorowana i zapisywana. Zapisane mogą zostać wszystkie elementy wymieniane drogą elektroniczną, w tym np. adresy poczty elektronicznej, e-maile, hasła, adresy internetowe, pliki wysyłane i odbierane, dane wprowadzane w formularze. Dane zgromadzone w ten sposób mogą być analizowane przez właściwy oddział ds. informatyzacji;
14) na urządzeniach pracujących w systemie informatycznym Urzędu zabrania się korzystania z punktów dostępu do sieci Internet lub komutowanych. Zakaz obejmuje hotspoty WiFi, modemy, udostępniane połączenia, access pointy, routery, itp. Nieautoryzowana transmisja

w pomieszczeniach Urzędu może zostać wykryta, zlokalizowana oraz jej treść zapisana. Dane zgromadzone w ten sposób mogą być analizowane i udostępniane organom ścigania.

§ 19. Komunikacja inna:

1) w przypadku nawiązania komunikacji głosowej, faksowej, wizyjnej lub innej należy zachować ostrożność;
2) nie należy udostępniać danych osobom nieuprawnionym.

§ 20. Zmiany w systemach informatycznych:

1) aktualizacja systemów operacyjnych komputerowych stanowisk pracy, objętych domeną Active Directory, odbywa się automatycznie. Po uzyskaniu informacji o dostępności pakietów aktualizacyjnych użytkownicy urządzeń mobilnych powinni aktualizować oprogramowanie systemowe samodzielnie lub przekazać urządzenie do właściwego oddziału ds. informatyzacji w celu aktualizacji;
2) aktualizacje oprogramowania autorskiego realizowane są na wniosek użytkowników przez dostawców oprogramowania lub w wyniku zmian wprowadzanych w celu usunięcia zgłoszonych błędów lub dostosowania do zmian przepisów prawa.

§ 21. Przekazywanie sprzętu poza Urząd:

1) likwidowany sprzęt komputerowy może zostać przekazany podmiotom zewnętrznym po wymontowaniu nośników informacji;
2) w przypadku przekazywania podmiotom zewnętrznym telefonów komórkowych posiadających system operacyjny (smartfony) przed przekazaniem należy przywrócić ustawienia fabryczne z wymazaniem pamięci, następnie całą dostępną pamięć urządzenia wypełnić losowymi danymi i ponownie przywrócić ustawienia fabryczne. Dla telefonów bez systemu operacyjnego nie dopuszcza się przekazania podmiotom zewnętrznym.

§ 22. Postanowienia końcowe:

1) nieprzestrzeganie powyższych zapisów może skutkować dla użytkowników systemu informatycznego Urzędu oraz dla użytkowników urządzeń będących własnością Urzędu odpowiedzialnością dyscyplinarną określoną przepisami Kodeksu Pracy, odpowiedzialnością karną lub odpowiedzialnością określoną przepisami Kodeksu Cywilnego;
2) za aktualizację i nadzór nad realizacją postanowień Instrukcji odpowiada Administrator Systemu Informatycznego.