Załącznik Nr 5 do Zarządzenia Nr 150/18

Prezydenta Miasta Szczecin

z dnia 6 kwietnia 2018 r.

Zasady korzystania z Internetu oraz z poczty elektronicznej Urzędu Miasta Szczecin

§ 1. 1. Dostęp do Internetu oraz do poczty elektronicznej Urzędu określa się, jako narzędzia pracy pracowników Urzędu.

2. Użytkownicy będący pracownikami Urzędu, uzyskują dostęp do Internetu i poczty elektronicznej za pomocą sieci teleinformatycznej LAN Urzędu i w sposób określony w niniejszym Załączniku.

3. Użytkownicy, nie będący pracownikami Urzędu, określeni także, jako podmiot zewnętrzny, mogą uzyskać dostęp do sieci teleinformatycznej LAN Urzędu jedynie na podstawie:

1) polecenia służbowego AD lub Sekretarza Miasta;

2) polecenia służbowego Dyrektora WInf;

3) umowy zawartej pomiędzy Urzędem, a podmiotem zewnętrznym, w której określono warunki takiego dostępu.

1. Użytkownicy podmiotu zewnętrznego, w przypadku stwierdzenia naruszeń zapisów Polityki Bezpieczeństwa Informacji podlegają natychmiastowemu odłączeniu od sieci LAN Urzędu. Powyższą decyzję podejmuje Dyrektor WInf lub ASI.

2. Użytkownicy są zobowiązani do wykorzystywania poczty elektronicznej Urzędu i serwisów internetowych zgodnie z zakresem swoich obowiązków, tj. w celu realizacji zadań służbowych oraz zadań związanych z podnoszeniem kwalifikacji zawodowych.

3. Dostęp do Internetu dostarczanego za pomocą sieci teleinformatycznej LAN Urzędu może być realizowany wyłącznie po prawidłowo przeprowadzonej procedurze logowania do tej sieci;

4. Procedury logowania są administrowane przez WInf i zapewniają odpowiedni poziom bezpieczeństwa sieci teleinformatycznej LAN Urzędu;

5. Użytkownicy, jeżeli wykonują pracę poza siecią teleinformatyczną LAN Urzędu mogą uzyskiwać dostęp do Internetu przy pomocy urządzeń i technologii mobilnych -komputerowych.

6. Użytkownicy zobowiązani są do korzystania wyłącznie ze sprzętu komputerowego będącego własnością Urzędu i wyłącznie przy użyciu legalnego oprogramowania, do którego Urząd posiada odpowiednie licencje lub inne uprawnienia.

7. Użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie pobrane z Internetu i przez niego zainstalowane w tym za utratę danych;

8. Procedury przywrócenia właściwego stanu komputera, na którym stwierdzono oprogramowanie niezgodne z zasadami określonym w Zarządzeniu wykonywane są przez WInf.

§ 2. Uprawnienia dostępu do sieci LAN Urzędu.

1. Zabrania się podłączania do sieci LAN Urzędu jakichkolwiek komputerów, w tym komputerów przenośnych czy jakichkolwiek urządzeń pracujących z zastosowaniem technologii komputerowych. Powyższy zakaz nie dotyczy pracowników WInf, którzy realizują zadania służbowe.

2. Zabranie się instalowania i uruchomienia oprogramowania niedopuszczonego do użycia przez Urząd (w tym np. oprogramowania skopiowanego własnoręcznie z Internetu), w szczególności, gdy jego uruchomienie wywołuje działania niedozwolone. Działania powyższe, po ich potwierdzeniu, traktowane będą, jako celowe i świadome, zmierzające do zwiększenia zagrożeń zasobów teleinformatycznych, a w szczególności łamiące postanowienia PBI Urzędu.

§ 3. Ogólne zasady obowiązujące na komputerowym stanowisku pracy w Urzędzie.

1. Wprowadza się następujące postanowienia związane z realizacją dostępu do Internetu oraz korzystania z poczty elektronicznej Urzędu:

1) podczas łączenia się ze skrzynką pocztową należy zachować szczególne warunki bezpieczeństwa i poufności w zakresie korespondencji służbowej i ochrony danych osobowych;

2) korzystanie z poczty elektronicznej Urzędu odbywa się:

a) jedynie przy pomocy konta pocztowego przydzielonego Użytkownikowi przez WInf lub przekierowanego na podstawie decyzji kierownika,

b) za pośrednictwem programu przeglądarki internetowej lub klienta programu pocztowego.

2. W przypadku zainstalowania i uruchomienia oprogramowania niedopuszczonego do użycia przez Urząd - WInf:

1) zastosuje blokadę konta poczty elektronicznej pracownika w sieci LAN Urzędu oraz redukcję typu dostępu do Internetu lub zastosuje całkowite odłączenie komputera pracownika od sieci LAN Urzędu;

2) sporządzi raport potwierdzający stan komputera oraz aktywność sieciową Użytkownika i przekaże ten raport jego kierownikowi,

3. Postanowienia ust. 2 mają zastosowanie dla Użytkowników będących pracownikami Urzędu.

4. W celu zapewnienia bezpieczeństwa zasobom sieci LAN Urzędu oraz jej Użytkownikom zabrania się dokonywania na niej, działań o charakterze nielegalnym, a w szczególności:

1) umieszczania lub uruchamiania programów i innych obiektów niebezpiecznych, w tym „koni trojańskich" czy innych programów realizujących działania określone, jako niepożądane lub wrogie;

2) skanowania sieci teleinformatycznej LAN Urzędu;

3) łączenia urządzeń mobilnych (komputery przenośne), podłączonych już do sieci LAN Urzędu do kolejnych sieci komputerowych w tym bezprzewodowych (Wi-Fi)

4) prowadzenia ataków, włamań itp., innych czynności związanych z ingerencją w działanie lub zasoby komputerów lub urządzeń w sieci LAN Urzędu, a także w stosunku do osób trzecich, ich komputerów i urządzeń w Internecie;

5) naruszania w jakikolwiek sposób bezpieczeństwa serwerów Urzędu i ich bezawaryjnej pracy, a zwłaszcza logowania się do serwerów, jeżeli zakres obowiązków tego nie wymaga;

6) anonimowego wysyłania przesyłek poczty elektronicznej z systemu pocztowego Urzędu lub sieci LAN Urzędu;

7) gromadzenia (w dowolnej, cyfrowej formie) na stanowisku pracy, tj. stacji roboczej lub na zasobie dyskowym dostępnym w sieci LAN, materiałów lub treści niezgodnych z obowiązującym prawem lub naruszających dobre obyczaje;

8) uruchamiania programów z komputerowych nośników zewnętrznych, tj. z płyt CD lub nośników typu pendrive, kart SD, itp.;

9) rozpowszechniania plików do Internetu tj. przesyłania zdjęć, filmów, tekstów czy innych formatów plików.

5. Postanowienia ust. 4. pkt: 2, 8 i 9 nie dotyczą:

1) podmiotów zewnętrznych, które realizują zadania na rzecz Urzędu, na podstawie umów, a użyte technologie powinny zostać ustalone z Administratorem sieci LAN Urzędu i zaakceptowane przez ASI;

2) pracowników Urzędu, których zadania polegają na komunikowaniu się i udostępnianiu danych i materiałów poprzez Internet;

3) pracowników WInf, upoważnionych przez Dyrektora WInf, których zadania wymagają zwiększonych uprawnień.

6. Zakazuje się umożliwiania osobom nieupoważnionym dostępu do sieci LAN Urzędu przy wykorzystaniu infrastruktury technicznej Urzędu, w szczególności umożliwienia pracy na stacjach roboczych Urzędu przy pomocy identyfikatora i hasła pracownika Urzędu.

§ 4. Szczególne postanowienia regulujące pracę w sieci LAN Urzędu.

1. Zabrania się pracownikom Urzędu wykonywania następujących czynności:

1) używania służbowej poczty elektronicznej Urzędu do celów innych niż służbowe;

2) używania prywatnej poczty elektronicznej w celach służbowych;

3) wysyłania wiadomości pocztowych (e-mail), zawierających reklamy, „łańcuszki szczęścia", materiały pornograficzne, czy inne materiały uważane powszechnie za niedozwolone;

4) logowania się w celach prywatnych lub komercyjnych na stronach www czy uczestniczenia w portalach o charakterze społecznościowym, zwłaszcza towarzyskim, rozrywkowym, komercyjnym, itp.;

5) używania w celach prywatnych lub komercyjnych komunikatorów internetowych w rodzaju Skype, Gadu-Gadu, Tlen, i podobnych, gdzie ograniczenie to nie dotyczy wykorzystania komunikatora Skype do celów służbowych;

6) korzystania z serwisów internetowych niezwiązanych z obowiązkami pracownika, np. oferujących gry internetowe i losowe, hazard, prywatne aukcje, rozrywkę, prywatne listy dyskusyjne, usługi IRC (Internet Relay Chat), itp.;

7) przetwarzania na komputerach, kopiowania i wysyłania plików, do których Urząd nie posiada praw autorskich z określonymi polami eksploatacji, w tym filmów (np. mpeg, mpg, avi, mov, QuickTime Movie, Xvid, itp.), plików muzycznych (np. CD-audio, mp3, wav, RealAudio, itp.), wygaszaczy (np. ser), skryptów (np. vbs);

8) korzystania z serwisów internetowych zawierających treści o charakterze przestępczym, hakerskim, pornograficznym, erotycznym, niecenzuralnym, rasistowskim lub w jakikolwiek sposób łamiące prawo obowiązujące na terenie Rzeczypospolitej Polskiej.

§ 5. Eksploatacja mechanizmów centralnych poczty elektronicznej Urzędu.

1. Wszystkie mechanizmy serwera poczty elektronicznej Urzędu przetwarzane są na sprzęcie komputerowym stanowiącym własność Urzędu lub udostępnionym do tego celu na podstawie umowy zawartej przez WInf.

2. Pocztą elektroniczną Urzędu administruje WInf, funkcję tę realizuje wyznaczony ASI.

3. Procedury zabezpieczenia danych i odtworzeniowe serwera poczty elektronicznej Urzędu realizowane są automatycznie i podlegają im wszystkie przesyłki pocztowe, które przeszły przez serwer poczty elektronicznej Urzędu:

1) czas przechowywania kopii zapasowej, ustala się na minimalny okres 12 miesięcy;

2) wszystkie posiadane kopie zapasowe WInf przechowuje w sposób bezpieczny, w odrębnej lokalizacji niż budynek Urzędu.

§ 6. 1. Służbowa poczta elektroniczna Urzędu stanowi pomocnicze narzędzie pracy dla pracowników Urzędu.

2. Przesyłanie informacji poza Urząd może odbywać się tylko przez osoby do tego upoważnione, wynikające z zakresu obowiązków lun prowadzonych postępowań.

3. W przypadku przesyłania informacji wrażliwych wewnątrz Urzędu bądź wszelkich danych osobowych poza Urząd należy wykorzystywać mechanizmy kryptograficzne (pakowanie i wykorzystanie silnych haseł podczas wysyłania plików, podpis elektroniczny).

4. Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu.

5. Nie należy otwierać załączników (plików) w korespondencji elektronicznej nadesłanej przez nieznanego nadawcę lub podejrzanych załączników nadanych przez znanego nadawcę.

6. Pojemność standardowego zasobu dyskowego, przydzielanego użytkownikowi poczty elektronicznej jest limitowana. Limit ten może zwiększyć dyrektor WInf na pisemny, umotywowany wniosek.

7. Obowiązują uregulowania szczegółowe dotyczące wielkości przesyłanych plików:

1) nie należy przesyłać plików o dużych rozmiarach, gdzie 20 MB stanowi maksymalną wielkość dla jednej przesyłki,

2) przesyłki o rozmiarach większych od 20 MB można przesyłać przy pomocy mechanizmu FTP, który udostępnia WInf, po zgłoszeniu potrzeb poprzez Pocztę elektroniczną.

8. Korzystanie z poczty elektronicznej winno odbywać się na bieżąco, w sposób racjonalny, zwłaszcza poprzez regularne przeglądanie zawartości skrzynki pocztowej z uwzględnieniem, że użytkownik:

1) powinien zwrócić szczególną uwagę na wiadomości z nieznanych źródeł (adresów), zawierających jakiekolwiek anonse czy załączniki, w szczególności takie, które wymagają od Użytkownika poczty wpisania danych jego konta lub jego danych osobowych - tych danych nie wolno podawać,

2) powinien reagować w przypadku otrzymywania wiadomości mających charakter przesyłek niechcianych, tj. „spam-u" tzn. powinien takie przesyłki oznaczać i przekierowywać do specjalnego folderu o nazwie SPAM,

3) powinien w przypadku stwierdzenia, że przesyłka wcześniej zakwalifikowana, jako spam jest uprawniona, przenieść ją do folderu „Skrzynka odbiorcza",

4) powinien zgłosić pracownikom WInf blokowanie przesyłek od uprawnionego nadawcy przez zewnętrzne mechanizmy antyspamowe,

5) może kopiować w dowolnym zakresie na swoim komputerze otrzymywane i wysyłane wiadomości pocztowe.

6) może okresowo kasować niepotrzebne wiadomości pocztowe.

9. Użytkownik obsługuje konto pocztowe przy użyciu przeglądarki internetowej lub programu klienta pocztowego. W przypadku planowanej nieobecności w pracy, użytkownik powinien uaktywnić funkcję informującą o nieobecności oraz przekierować pocztę ze swojego adresu na adres innego użytkownika poczty, w jednostce poprzez uzgodnienie wewnątrz jednostki. w przypadku, gdy nieobecność została zaplanowana,

10. W przypadku gdy nieobecność pracownika nie była zaplanowana decyzję o przekierowaniu poczty przychodzącej, podejmuje kierownik. Przekierowanie wiadomości pocztowych na adres innego użytkownika poczty realizowane jest poprzez zgłoszenie przez kierownika ASI poprzez pocztę elektroniczną.

11. Użytkownik po powrocie do pracy podejmuje obsługę poczty elektronicznej i przywraca ustawienia osobiste programu pocztowego.

12. Kierowanie wiadomości pocztowych do dużych grup użytkowników winno odbywać się z zastosowaniem polecenia UDW (ukryty do wiadomości), które powoduje, że użytkownicy wzajemnie nie mogą widzieć swych adresów pocztowych.

13. Hasło użytkownika poczty elektronicznej do konta pocztowego musi spełniać cechy określone dla haseł dostępu wymaganych przy obsłudze danych osobowych, w szczególności nie może być udostępniane innym osobom, a w przypadku ujawnienia winno być niezwłocznie zmienione. Są to hasła tożsame z hasłami dostępu do komputera w domenie AD, w sieci LAN Urzędu.

14. Przyjmuje się procedury resetu hasła po jego utraceniu, tj. ujawnieniu lub zapomnieniu:

1) hasła dostępu do domeny sieciowej Urzędu są resetowane po zgłoszeniu użytkownika, a następnie jego autoryzacji, tj. osobistym zgłoszeniu do ASI i okazaniu identyfikatora. Autoryzacji może także udzielić kierownik pracownika osobiście lub w formie pisemnej.

2) autoryzacja użytkownika może zostać przeprowadzona zdalnie (drogą telefoniczną), przez ASI poprzez pytania związane z 3-ma danymi osobowymi użytkownika, które potwierdzą jego tożsamość. Dane osobowe dla weryfikacji są udostępnione pracownikowi WInf na podstawie upoważnienia udzielonego przez AD.

3) awaryjna procedura resetu hasła – upoważniony ASI generuje sukcesywnie komplety bezpiecznych haseł, gdzie hasło będzie przechowywane w dwóch, zapieczętowanych kopertach. Para kopert będzie opatrzona identycznym, unikalnym numerem opartym o algorytm daty i czasu w postaci rrrrmmddggmm, przykładowo 201412140933. Procedura zabezpiecza poufną metodę przekazania hasła, którą na podstawie występujących potrzeb, inicjuje kierownik, w porozumieniu z ASI.

§ 7. Zasady tworzenia konta poczty elektronicznej Urzędu.

1. Wszystkie konta (adresy) poczty elektronicznej Urzędu, które przydzielono Użytkownikom, stanowią własność Urzędu.

2. Dla sprawnej i nieprzerwanej obsługi poczty elektronicznej Urzędu ustanawia się skrzynki pocztowe (adresy poczty elektronicznej) podstawowe oraz pomocnicze z zastrzeżeniem, że wszystkie zostały ustanowione i przeznaczone wyłącznie do obsługi korespondencji służbowej Urzędu:

1) konto podstawowe (adres) poczty elektronicznej dla komórki organizacyjnej Urzędu tworzone jest po ustaleniu zapisu, np.: winf@um.szczecin.pl co jest tożsame z nazwą komórki organizacyjnej lub rolą jaką pełni, w tym przypadku serwisu WInf,

2) konto pomocnicze (adres) poczty elektronicznej użytkownika tworzone jest na ogólnych zasadach, np.: imienazwisko@um.szczecin.pl,

3) konta podstawowe dla jednostek organizacyjnych Gminy Miasta Szczecin mogą być tworzone w oparciu o zapis - pkt a) lub ustalone zgodnie z dziedziną działania jednostki lub jako pochodna od nazwy jednostki organizacyjnej (np.: nazwa.xx@um.szczecin.pl, gdzie przykładowy adres komórki jednostki przyjmie format: sekretariatboi@um.szczecin.pl,

4) w przypadku wystąpienia konfliktu nazwy konta (powielenie nazwy) ASI wspólnie z pracownikiem ustalą nowy zapis nazwy konta,

5) przesyłki poczty elektronicznej wychodzącej z Urzędu, winny być opatrywane stopką zgodną z:

a) standardami identyfikacji wizualnej Miasta Szczecin,

b) zadaniami informacyjnymi lub promocyjnymi ustalanymi z Dyrektorem WInf.

3. Obowiązują procedury dotyczące podłączenia stanowiska pracy do sieci teleinformatycznej (LAN Urzędu) i utworzenia konta poczty elektronicznej:

1) komputer - stanowisko pracy podłącza do sieci LAN Urzędu tylko pracownik WInf, niezwłocznie po wydaniu i ustawieniu we wskazanej lokalizacji,

2) konto domenowe dla nowego pracownika Urzędu (umowa o pracę) tworzone jest tylko i wyłącznie na podstawie zgłoszenia nowozatrudnionego pracownika przez kierownika. Dla czasowo zatrudnionego pracownika lub stażysty wymagana jest data zakończenia umowy.

3) użytkownicy, nie będący pracownikami Urzędu, mogą otrzymać konto poczty elektronicznej Urzędu na podstawie zapisów umowy pomiędzy Urzędem i podmiotem zewnętrznym lub polecenia służbowe wydane przez Dyrektora WInf, gdzie wykonanie nastąpi za pośrednictwem procedur realizowanych poprzez WInf.

4. Ustala się, jako obowiązujące, dotychczas używane adresy poczty elektronicznej.

5. Zmiana formatu adresów, w tym nazwy domeny może nastąpić na podstawie polecenia służbowego wydanego przez Dyrektora WInf, po uzyskaniu nowego adresu domeny w zasobach Internetu.

§ 8. Określa się następujące zasady likwidacji konta/adresu poczty elektronicznej:

1. Uprawnienia do konta pomocniczego poczty elektronicznej Użytkownika są blokowane i likwidowane po ustaniu zatrudnienia pracownika.

2. W związku z ustaniem stosunku pracy pracownika, WInf wykonuje następujące procedury:

1) w przypadku, gdy były pracownik obsługiwał konto komórki organizacyjnej, tj. konto podstawowe, kierownik pracownika, zawiadamia WInf o zmianie pracownika obsługującego ten adres poprzez pocztę elektroniczną. Procedurę inicjuje kierownik pracownika lub zastępczo ASI, a wykonuje ASI.

2) dla konta pomocniczego (imiennego) ASI blokuje konta pracownika po podpisaniu jego karty obiegowej lub po otrzymaniu informacji o ustaniu zatrudnienia lub zmianie stanowiska.

3) ASI natychmiast blokuje dostęp do imiennego konta pracownika i usuwa to konto po upływie 3 miesięcy od zablokowania.

4) zawartość zablokowanego konta pomocniczego (imiennego) jest przechowywana przez WInf, przez okres roku od jego zablokowania.

3. W związku z likwidacją konta poczty elektronicznej (przykładowo: z powodu ustania zatrudnienia pracownika), ASI może podjąć procedurę zabezpieczenia dostępu do zawartości skrzynki pocztowej, którą inicjuje kierownik, podlegającą na:

1) przepisaniu zawartości skrzynki pocztowej na nośnik zewnętrzny i usunięciu z komputera, gdzie nośnik podlega przekazaniu przełożonemu pracownika;

2) przypisaniu zawartości skrzynki pocztowej na inny komputer, obsługiwany przez innego Użytkownika w Urzędzie;

3) przypisaniu zawartości konta pocztowego do innego, wskazanego konta pocztowego.

§ 9. Dla zapewnienia bezpieczeństwa poczty elektronicznej w sieci LAN Urzędu stosuje się obowiązkowo mechanizmy ochronne i procedury:

1) Ochrona przed spamem (niepożądane przesyłki w poczcie elektronicznej) realizowana jest przez dwa stopnie zabezpieczeń technicznych:

a) serwer wstępnie filtrujący przesyłki pocztowe,

b) mechanizm filtrujący na serwerze poczty elektronicznej Urzędu.

2) Ochrona antywirusowa realizowana jest na wszystkich komputerach przez mechanizmy programu antywirusowego z serwerami realizujących dystrybucję wzorców i raportowanie.

3) Ochrona brzegową sieci LAN Urzędu realizowana jest automatycznie przez urządzenia o funkcjach filtrujących, blokujących, szyfrujących i raportujących. Urządzenia te zapewniają funkcje administracyjne siecią LAN i zapewniają wysoką dostępność wszystkich funkcji.

4) Pracownicy Urzędu, zobowiązani są do reagowania na wszelkie nieprawidłowości, jakie zaobserwują w otrzymywanych przesyłkach pocztowych i zgłaszania do WInf.

§ 10. Procedury kontrolne dotyczące komputerowego stanowiska pracy w Urzędzie.

1. AD wprowadza obowiązek kontrolny zawartości komputerów, gdzie okresowemu sprawdzaniu podlegają wszystkie komputery stanowiące własność Urzędu. Kontrola sprawowana jest poprzez automatyczne procedury oraz aplikacje skanujące komputery Urzędu. Wyniki skanowania komputerów zapisywane są w bazie danych prowadzonej komputerowo. Procedury kontrolne nadzorują administratorzy systemów komputerowych z WInf. Obowiązek ten wprowadza się dla zapewnienia:

1) ochrony zasobów teleinformatycznych i danych Urzędu;

2) zgodności wykorzystywanych zasobów z posiadanymi uprawnieniami i licencjami.

2. Procedury sprawdzające realizowane są przy pomocy specjalistycznego oprogramowania, którego raporty stanowią podstawę dla działań naprawczych podejmowanych przez ASI oraz działań organizacyjnych podejmowanych przez Dyrektora WInf.

3. Przepływ informacji w sieci LAN Urzędu, generowany przez pracownika, podlega monitoringowi z automatycznym zapisem dostępów do stron WWW. Informacje statystyczne potwierdzające; adresy sieciowe, czas dostępu do najczęściej odwiedzanych przez pracowników Urzędu serwisów internetowych, gromadzonych plików oraz uruchamianych aplikacji podlegają automatycznej analizie w celu:

1) przekazywania przez Dyrektora WInf do kierowników;

2) zbierania materiału dowodowego dla dalszych kroków podejmowanych na drodze służbowej;

3) generowania statystyk i ostrzeżeń dla użytkowników próbujących dostępów do stron WWW podlegających filtrowaniu i blokowaniu, gdzie ostrzeżenia dla użytkowników realizowane są w formie komunikatu ostrzegawczego, którego formę zatwierdza Dyrektor WInf.

4. Określa się procedurę wyłączenia niektórych, komputerowych stanowisk pracy od ww. postanowień.

1) użytkownik w celu uzyskania wyłączenia z powyższych procedur kontrolnych, występuje z indywidualnym wnioskiem do Dyrektora WInf.

2) Dyrektor WInf, w przypadku akceptacji kieruje wniosek do realizacji przez ASI.

3) ASI prowadzi rejestr wniosków i udzielonych wyłączeń.

5. Żadne wyłączenia z obowiązków czy uregulowań określone w zarządzeniu i niniejszym załączniku nie zdejmują z pracowników Urzędu obowiązków czy ograniczeń ustawowych związanych w szczególności z ochroną danych osobowych.

§ 11. Niektóre działania, które zostały określone w § 3 ust. 4 pkt 2, 8 i 9 załącznika, jako zabronione - są dozwolone w przypadkach:

1) realizacji działań zgodnych z dyspozycją kierownika lub przepisami szczególnymi, które obowiązują pracowników Urzędu;

2) prowadzenia interakcji z internetowymi portalami instytucji, urzędów, organizacji, w celu realizacji zadań czy wykonywania obowiązków;

3) uzyskania pisemnej zgody AD lub Dyrektora WInf;

4) realizacji na rzecz Urzędu, poprzez podmioty zewnętrzne wynikające z zapisów umów, zwłaszcza, gdy niezbędne jest ustanowienie interoperacyjności pomiędzy systemami teleinformatycznymi Urzędu i systemami zewnętrznymi.