STAROSTA
WARSZAWSKI ZACHODNI
z siedzibą
w Ożarowie Mazowieckim

ZARZĄDZENIE Nr 49/2020
STAROSTY WARSZAWSKIEGO ZACHODNIEGO
z dnia 17 sierpnia 2020 roku

w sprawie wprowadzenia regulaminów korzystania z internetu i komputerów przenośnych, oraz procedury obsługi i korzystania z monitoringu wizyjnego.

Na podstawie art. 34 ust 1 oraz art. 35 ust 2 ustawy z dnia 5 czerwca 1998 roku o samorządzie powiatowym (Dz. U. z 2020 roku, poz. 920) zarządzam co następuje:

§ 1

Wprowadza się :

1. **Regulamin korzystania komputerów przenośnych stanowiący załącznik nr 1 do niniejszego zarządzenia**
2. **Regulamin korzystania z internetu, stanowiący załącznik nr 2 do niniejszego zarządzenia**
3. **Procedurę obsługi i korzystania z monitoringu wizyjnego, stanowiący załącznik nr 3 do niniejszego zarządzenia, składającą się z:**
   - **Wzoru druku dotyczącego wniosku o udostępnienie nagrań z monitoringu wizyjnego,**
   - **Wzoru druku rejestru dotyczącego udostępnionych nagrań z monitoringu wizyjnego,**
   - **Wzoru druku dotyczącego wykazu elementów systemu monitoringu wizyjnego oraz miejsc ich zainstalowania.**

§ 2

1. Wykonanie niniejszego zarządzenia powierzam Administratorowi Systemów Informatycznych, Naczelnikom Wydziałów i pracownikom zatrudnionym na poszczególnych stanowiskach pracy w zakresie wskazanym w ww. dokumentach określających zasady nadzoru nad prawidłowością stosowania procedur ochrony danych osobowych i w zakresie zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowym w Starostwie Warszawskim Zachodnim.
2. Zobowiązuję wszystkich pracowników do zapoznania się z wymienionymi dokumentami.
3. Zobowiązuję pracowników przetwarzających dane osobowe do przestrzegania procedur zawartych w ww. dokumentach.

§ 3

Zarządzenie wchodzi w życie z dniem podpisania.

WICESTAROSTA
Wojciech Białas

Załącznik nr 1 do Zarządzenia nr 49/2020
Starosty Warszawskiego Zachodniego
z dnia 17 sierpnia 2020 r.

REGULAMIN UŻYTKOWANIA KOMPUTERÓW PRZENOŚNYCH

1. Użytkownik otrzymujący komputer przenośny winien podpisać oświadczenie o zobowiązaniu się do przestrzegania zaleceń związanych z ochroną komputera.
2. Osobą uprawnioną do korzystania z komputera jest wyłącznie Użytkownik.
3. Korzystanie z komputerów, Internetu i programów użytkowych ma służyć Użytkownikom wyłącznie do celów służbowych.
4. Komputer powierzony Użytkownikowi stanowi własność Urzędu i jako narzędzie pracy powinien być do niej wykorzystywany.
5. Zarządzanie komputerem powinno być zgodne z Krajowymi Ramami Interoperacyjności określonymi zgodnie z ustawą z dnia 17 lutego 2005 roku o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U.2014.1114 t.j. z dnia 2014.08.22), oraz innymi wewnętrznymi regulacjami Urzędu.
6. Użytkownik jest zobowiązany właściwie eksploatować i dbać o powierzony mu komputer oraz utrzymać go w stanie nie gorszym, niż wynika to ze zwykłego zużycia eksploatacyjnego.
7. Wszystkie dane zapisane w komputerze (dokumenty tworzone i przechowywane w pamięci komputera, pliki oraz inne posiadane informacje i dane) związane z wykonywanymi zadaniami służbowymi są własnością Urzędu.
8. Użytkownikowi nie wolno samodzielnie zmieniać konfiguracji sprzętowej komputera oraz ustawień w systemie operacyjnym, do których nie ma uprawnień.
9. Użytkownik korzystający z komputera nie może przechowywać na nim danych oraz oprogramowania nielegalnego, jak również danych, informacji, materiałów mogących naruszać prawa osobiste lub majątkowe osób trzecich.
10. Urząd udostępnia Użytkownikowi komputer z zainstalowanym oprogramowaniem, w tym elektroniczną skrzynką pocztową, oraz zapoznaje Użytkownika z obowiązującymi zasadami korzystania z takiego sprzętu.
11. Konfiguracją komputerów zajmuje się Zespół ds. Informatycznych. Każdy komputer wyposażony jest w domyślnie zainstalowane oprogramowanie.
12. Komputery podlegają automatycznej ewidencji pod kątem konfiguracji sprzętowej i zainstalowanego oprogramowania oraz ewidencji środków trwałych.
13. Ze względów bezpieczeństwa Użytkownik nie posiada uprawnień administracyjnych pozwalających na instalację oprogramowania.
14. Na komputerach służbowych można używać tylko oprogramowania, które zainstalowane zostało przez Administratora Systemów Informatycznych lub osobę upoważnioną z Zespołu ds. Informatycznych.
15. W przypadku przechowywania na komputerze przenośnym danych osobowych lub stanowiących tajemnicę Urzędu, pracownik zobowiązany jest do ich przechowywania na dysku szyfrowanym, zabezpieczonym hasłem - co najmniej 8 znakowym (duże, małe litery, znaki specjalne lub cyfry).
16. Na komputerach przenośnych przeznaczonych do zewnętrznych prezentacji multimedialnych nie powinny, o ile jest to możliwe, znajdować się dane osobowe lub stanowiące tajemnicę Urzędu.

17. W przypadku kradzieży lub zgubienia komputera przenośnego Pracownik powinien natychmiast powiadomić o tym Zespół ds. informatycznych, zaznaczając jednocześnie, jakiego rodzaju dane były na tym urządzeniu przechowywane.
18. Pracownik zobowiązany jest do zabezpieczenia komputera w czasie transportu, a w szczególności:

a) zaleca się przenoszenie go w zamkniętej i zabezpieczonej torbie.
b) zabrania się pozostawiania komputera przenośnego w samochodzie podczas postoju w miejscu publicznym.
c) podczas jazdy samochodem zaleca się przechowywanie komputera przenośnego pod tylnym siedzeniem kierowcy. Przewożenie go np. na siedzeniach może skutkować kradzieżą na skrzyżowaniach, przejściach dla pieszych lub w korkach.

19. W przypadku pozostawiania komputerów przenośnych w biurze zaleca się umieszczanie ich po zakończeniu pracy w zamykanych szafach.
20. Użytkownik laptopa jest zobowiązany do regularnego tworzenia kopii bezpieczeństwa danych na serwer lub zapasowe nośniki (pendrive, CD, DVD). Nośniki z takimi kopiami powinny być przechowywane w bezpiecznym miejscu, z uwzględnieniem ochrony przed dostępem osób niepowołanych.
21. Pracując na komputerze przenośnym w miejscu publicznym, użytkownik zobowiązany jest zwrócić szczególną uwagę na ochronę wyświetlanych na monitorze informacji przed podejrzeniem ich przez osoby nieuprawnione. Zakazuje się pracy nad informacjami wrażliwymi w miejscach publicznych i środkach transportu (np. pociąg, samolot, autokar).
22. Korzystanie z sieci komputerowej podlega filtrowaniu ruchu sieciowego.
23. Urząd ma prawo wglądu do zapisanych na służbowym komputerze informacji służbowych. Jeżeli Użytkownik zabezpieczył je hasłem, na żądanie przełożonego zobowiązany jest je udostępnić.
24. Urząd zastrzega sobie prawo do instalacji na sprzęcie komputerowym oprogramowania do monitorowania legalności programów zainstalowanych na komputerach.
25. Na polecenie Starosty będzie dokonywana okresowa kontrola przestrzegania postanowień niniejszego Regulaminu.
26. Osobą wykonującą kontrolę będzie Pracownik upoważniony przez Starostę.

Zapoznałem się z treścią Regulaminu użytkowania komputerów przenośnych i zobowiązuję się do przestrzegania zasad w nim zawartych

Czytelny podpis Użytkownika

.....

Załącznik nr 2 do Zarządzenia nr 49/2020
Starosty Warszawskiego Zachodniego
z dnia 17 sierpnia 2020 r.

REGULAMIN KORZYSTANIA Z INTERNETU

1. Użytkownik zobowiązany jest do korzystania z internetu wyłącznie w celach służbowych.
2. Zabrania się zgrywania na dysk twardy komputera oraz uruchamia jakichkolwiek programów nielegalnych oraz plików pobranych z niewiadomego źródła. Pliki takie powinny być ściągane tylko za każdorazową zgodą osoby upoważnionej do administrowania infrastrukturą IT (np. ASI) i tylko w uzasadnionych przypadkach.
3. Użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie instalowane z Internetu.
4. Zabrania się wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, hackerskim, pornograficznym, lub innym zakazanym przez prawo (na większości stron tego typu jest zainstalowane szkodliwe oprogramowanie infekujące w sposób automatyczny system operacyjny komputera szkodliwym oprogramowaniem).
5. Nie należy w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł.
6. W przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, należy zwracać uwagę na pojawienie się odpowiedniej ikonki (kłódka) oraz adresu www rozpoczynającego się frazą "https:". Dla pewności należy „kliknąć" na ikonkę kłódki i sprawdzić, czy właścicielem certyfikatu jest wiarygodny właściciel.
7. Należy zachować szczególną ostrożność w przypadku podejrzanego żądania lub prośby zalogowania się na stronę (np. na stronę banku, portalu społecznościowego, e-sklepu, poczty mailowej) lub podania loginów i haseł, PIN-ów, numerów kart płatniczych przez Internet.

ZASADY KORZYSTANIA Z POCZTY ELEKTRONICZNEJ

1. Przesyłanie danych osobowych z użyciem maila poza Urząd może odbywać się tylko przez osoby, którym nadano upoważnienia do przetwarzania danych osobowych.
2. W przypadku przesyłania danych osobowych poza organizację należy wykorzystywać mechanizmy kryptograficzne (hasłowanie wysyłanych dokumentów lub plików zzipowanych, podpis elektroniczny).
3. W przypadku zabezpieczenia plików hasłem, obowiązuje minimum 8 znaków: duże i małe litery i cyfry lub znaki specjalne, a hasło należy przesłać inną metodą, np. telefonicznie lub SMS-em.
4. Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu.
5. Zaleca się, aby użytkownik podczas przesyłania danych osobowych mailem zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata.

6. Nie należy otwierać załączników (plików) w mailach bez weryfikacji nadawcy. Tego typu maile większości przypadków zawierają załączniki ze szkodliwymi programami, w wyniku działania takiego szkodliwego oprogramowania może dojść do poważnych incydentów, łącznie z pełną utratą danych osobowych lub zaszyfrowanie m przez kryptowirusy
7. Bez weryfikacji wiarygodności nadawcy, nie należy „klikać" na hiperlinki w mailach, gdyż mogą to być hiperlinki do stron zainfekowanych lub niebezpiecznych. W wyniku takiej infekcji może dojść do poważnych incydentów, łącznie z pełną utratą danych osobowych lub zaszyfrowanie przez kryptowirusy
8. Przypadki podejrzanych e-maili, należy zgłaszać Administratorowi Systemów Informatycznych.
9. Podczas wysyłania maili do wielu adresatów jednocześnie, należy użyć metody „Ukryte do wiadomości – UDW". Zabronione jest rozsyłanie maili do wielu adresatów z użyciem opcji „Do wiadomości".
10. Użytkownicy powinni okresowo kasować niepotrzebne maile i archiwizować.
11. E-mail służbowy jest przeznaczony wyłącznie do wykonywania obowiązków służbowych.
12. Zakazuje się wysyłania korespondencji służbowej na prywatne skrzynki pocztowe pracowników lub innych osób.
13. Użytkownicy mają prawo korzystać z poczty mailowej dla celów prywatnych wyłącznie okazjonalnie i powinno być to ograniczone do niezbędnego minimum.
14. Korzystanie z maila dla celów prywatnych nie może wpływać na jakość i ilość świadczonej przez Użytkownika pracy oraz na prawidłowe i rzetelne wykonywanie przez niego obowiązków służbowych.
15. Przy korzystaniu z maila, Użytkownicy mają obowiązek przestrzegać prawa własności przemysłowej i prawa autorskiego.
16. Użytkownicy nie mają prawa korzystać z e-maila w celu rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec powszechnie obowiązujących zasad postępowania.

Zapoznałem się z treścią Regulaminu korzystania z internetu oraz poczty elektronicznej i zobowiązuję się do przestrzegania zasad w nim zawartych.

Czytelny podpis Użytkownika

.....

Załącznik nr 3 do Zarządzenia nr 49/2020
Starosty Warszawskiego Zachodniego
z dnia 17 sierpnia 2020 r.

PROCEDURA OBSŁUGI I KORZYSTANIA Z SYSTEMU MONITORINGU WIZYJNEGO DLA STAROSTWA POWIATU WARSZAWSKIEGO ZACHODNIEGO

Monitoring wizyjny prowadzony jest przez Starostwo Powiatu Warszawskiego Zachodniego w Ożarowie Mazowieckim, a Administratorem Danych w związku z zadaniami bezpośrednio przypisanymi staroście - Starosta Warszawski Zachodni, mający siedzibę w Ożarowie Mazowieckim (05-850), przy ul. Poznańskiej 129/133, na podstawie art. 4b ust.1 ustawy
z dnia 5 czerwca 1998 r. o samorządzie powiatowym (Dz. U. z 2018 poz. 995 z późn. zm.) w celu zapewnienia porządku publicznego i bezpieczeństwa osób przebywających na monitorowanym terenie oraz ochrony mienia, ochrony przeciwpożarowej i przeciwpowodziowej, zwiększenia bezpieczeństwa interesantów i pracowników przebywających w budynkach i na terenie Starostwa Powiatowego w Ożarowie Mazowieckim.

Zgodnie z art. 13 ust. 1 i ust. 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. U. UE. L. z 2016 r. Nr 119, str. 1 z późn. zm.), wcześniej i dalej: RODO, mając na uwadze przepisy ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j. Dz. U. z 2019 r. poz. 1781) oraz ustawy z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (t.j. Dz. U. z 2020 r. poz. 838 z późn. zm.), a także ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (t.j. Dz. U. z 2020 r. poz. 1320
z późn. zm.), Administrator informuje, iż:

1. Na terenie nieruchomości położonej w Ożarowie Mazowieckim, przy ul. Poznańskiej 129/133, Ożarów Mazowiecki (05-850), w tym znajdujących się tam budynków i pomieszczeń zainstalowano system monitoringu wizyjnego (dalej: „Monitoring").
2. Monitoring, o którym mowa powyżej, rejestruje obraz, nie rejestruje dźwięku.
3. Monitoring rejestruje obraz w sposób ciągły, przez 24 godziny na dobę, przez 7 dni w tygodniu, zarówno w czasie rzeczywistym, jak i poprzez zapis obrazu na dysku twardym.
4. Celem zainstalowania monitoringu wizyjnego jest:
   1) ochrona mienia przed kradzieżami,
   2) zapewnienia bezpieczeństwa na terenie monitorowanym,
   3) zapobieganie dostępu do pomieszczeń przez osoby nieuprawnione,
   4) kontrola procedur bezpieczeństwa i higieny pracy.
5. Rejestrator obrazu monitoringu obejmuje swoim zasięgiem łącznie całą przestrzeń ciągów komunikacyjnych na parterze oraz poszczególnych piętrach (korytarze, sala główna dla interesantów, inne) oraz przestrzeń na zewnątrz budynków parkingi i wejścia główne.

6. Podgląd monitoringu w czasie rzeczywistym możliwy jest całodobowo.
7. Obraz przechowywany jest na dysku twardym do 14 dni. Po tym czasie następuje kasowanie zapisów poprzez nadpisywanie.
8. Zapisy monitoringu mogą zostać udostępnione uprawnionym instytucjom i organom państwa, w szczególności na potrzeby prowadzonych postępowań (np. policji, sądom, prokuraturom itp.), o ile organ taki zwróci się do Administratora o udostępnienie w/w nagrań lub obowiązek ich udostępnienia będzie wynikał z przepisów prawa powszechnie obowiązującego.
9. Osoby przebywające na terenie nieruchomości objętej monitoringiem są informowane o funkcjonowaniu monitoringu za pośrednictwem klauzul informacyjnych znajdujących się zarówno na zewnątrz, jak i wewnątrz budynku. W ten sposób Administrator realizuje swój obowiązek informacyjny względem osób, których wizerunek jest przetwarzany za pośrednictwem monitoringu. Klauzula informacyjna,
   o której mowa powyżej, zostanie także umieszczona na stronie internetowej Administratora, pod adresem: www.pwz.pl.
10. We wszystkich sprawach związanych z przetwarzaniem danych w systemie monitoringu wizyjnego można się kontaktować z Inspektorem Ochrony Danych, pod adresem: iod@pwz.pl
11. Dane zarejestrowane na nośnikach nie stanowią informacji publicznej i nie podlegają udostępnieniu w oparciu o przepisy ustawy o dostępie do informacji publicznej.
12. Osoba, której dane dotyczą, lub inny uprawniony podmiot może zwrócić się do Administratora z wnioskiem o udostępnienie nagrania monitoringu w określonym zakresie (np. co do nagrania z danej daty i godziny). Administrator może uzależnić udostępnienie nagrania monitoringu od uprzedniego potwierdzenia przez wnioskodawcę uprawnienia do jego uzyskania, w tym przedłożenia stosownej dokumentacji w tym zakresie. Nagranie udostępnione wnioskodawcy – co do zasady – nie może jednak obejmować wizerunku osób trzecich, chyba, że dotyczy to nagrań, co do których wnioskodawca jest upoważniony na podstawie przepisów prawa powszechnie obowiązującego.
13. Wzór wniosku o udostępnienie nagrania z monitoringu wizyjnego stanowi załącznik nr 1 do niniejszej procedury.
14. Udostępnienie nagrania z systemu monitoringu, zgodnie z treścią ust. 13 powyżej, może nastąpić jedynie w okolicznościach, gdy:
    1) wnioskodawcą jest osoba uprawniona (wymagany jest dokument to poświadczający),
    2) zgrania nagrania lub jego udostępnienia do wglądu dokonuje pracownik upoważniony przed Administratora,
    3) odtworzenie materiału następuje z udziałem osoby lub osób wnioskujących o zapoznanie się z treścią danego nagrania,

4) po zakończeniu odtworzenia, w przypadku stwierdzenia, że dalsze przetwarzanie danego nagrania może być związane z prawnie uzasadnionym interesem Administratora lub z koniecznością wypełnienia obowiązku prawnego ciążącego na Administratorze, czy też jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, nagranie należy zabezpieczyć i przechowywać w miejscu do tego wskazanym przez Administratora. W razie wątpliwości poczytuje się, że za prawidłowe zabezpieczenie nagrania, o którym mowa w zdaniu poprzedzającym, odpowiedzialny jest pracownik upoważniony przez Administratora, który dokonał jego odtworzenia.

5) do odtworzonego i zabezpieczonego nagrania monitoringu, upoważniony przez Administratora pracownik dołącza podpisany zarówno przez Administratora danych, jak i upoważnionego pracownika, wniosek uprawnionej osoby, a także formularz zawierający w szczególności:

   a) cel, dla którego wnioskowano o zabezpieczenie nagrania,

   b) datę, miejsce oraz godzinę zgrania i zabezpieczenia nagrania,

   c) informację o sposobie zabezpieczenia i miejscu przechowywania zabezpieczonego nagrania,

   d) informację o przewidywanym czasie przechowywania zabezpieczonego nagrania

   e) czas przechowywania - do rozstrzygnięcia sporu/ sprawy/ udzielenia odpowiedzi stronie wnioskującej, lecz nie dłużej niż przez okres roku,

15. Nagranie z monitoringu wizyjnego zapisywane jest na nośnikach elektronicznych, po wcześniejszym uzyskaniu zgody Administratora w tym zakresie. Nagranie przekazuje się osobie wnioskującej, za potwierdzeniem odbioru na Wniosku o udostępnienie nagrań z monitoringu wizyjnego.

16. Administrator prowadzi rejestr udostępnionych nagrań z monitoringu wizyjnego. Wzór rejestru stanowi załącznik nr 2 do niniejszej procedury.

17. Elementy monitoringu wizyjnego mogą być w miarę konieczności i możliwości finansowych Administratora rozbudowywane i udoskonalane.

18. Zapisy z monitoringu mogą zostać odtworzone za zgodą Administratora danych w obecności osoby upoważnionej i tylko w uzasadnionych przypadkach.

19. System monitoringu nie obejmuje pomieszczeń udostępnianych pracownikom takich jak kuchnia, pomieszczenia sanitarne, toalety oraz palarnie.

20. Załącznik nr 3 określa wykaz elementów wchodzących w skład całego systemu monitoringu wizyjnego oraz lokalizację instalacji.

21. W sprawach nieuregulowanych niniejszą procedurą ostateczną decyzję podejmuje Administrator.

Załącznik nr 3 do Zarządzenia nr 49/2020
Starosty Warszawskiego Zachodniego
z dnia 17 sierpnia 2020 r.

WNIOSEK O UDOSTĘPNIENIE NAGRAŃ Z MONITORINGU WIZYJNEGO

Dane osoby wnioskującej:

Imię i nazwisko: .....

Nazwa instytucji: .....

Adres: .....

Telefon: .....

Data, godzina i miejsce zdarzenia:

.....

Krótki opis zdarzenia:

.....

.....

Wskazanie celu otrzymania nagrania z monitoringu:

.....

Data i czytelny podpis: .....

WYRAŻAM ZGODĘ / NIE WYRAŻAM ZGODY*

Podpis: .....

Potwierdzam odbiór nagrania i oświadczam, że otrzymane materiały zostaną wykorzystane wyłącznie w celu wskazanym we wniosku. W przypadku niewykorzystania materiałów, zostaną one zniszczone w terminie 30 dni.

Załącznik nr 3 do Zarządzenia nr 49/2020
Starosty Warszawskiego Zachodniego
z dnia 17 sierpnia 2020 r.

Data i czytelny podpis: .....

REJESTR UDOSTĘPNIONYCH NAGRAŃ Z MONITORINGU WIZYJNEGO

ROK .....

L.p.	Data wpływu wniosku	Dane wnioskodawcy	Nr sprawy	Przedmiot/zakres wniosku	Data udostępnienia danych	Forma udostępnienia (np. notatka, nośnik)	Uwagi
1.							
2.							
3.							
4.							
5.							
6.							

Załącznik nr 3 do Zarządzenia nr 49/2020
Starosty Warszawskiego Zachodniego
z dnia 17 sierpnia 2020 r.

WYKAZ ELEMENTÓW SYSTEMU MONITORINGU WIZYJNEGO ORAZ MIEJSC ICH ZAINSTALOWANIA

Lp.	Nazwa elementu systemu monitoringu	Numer inwentarzowy	Lokalizacja
REJESTRATOR			
KAMERY			