Załącznik nr 2
do zarządzenia nr 100/02/2019
z dnia 19 lutego 2019 r.

Załącznik Nr 4 do Regulaminu Pracy Urzędu Miasta Starogard Gdański
stanowiącego załącznik do Zarządzenia Nr 194/06/2014
Prezydenta Miasta Starogard Gdański z dnia 24 czerwca 2014 r.
w sprawie Regulaminu Pracy Urzędu Miasta Starogard Gdański

Załącznik nr 4
do Regulaminu Pracy Urzędu Miasta Starogard Gdański

Regulamin
określający procedury korzystania z legalnego oprogramowania, sprzętu komputerowego i sieci teleinformatycznej w Urzędzie oraz procedury monitoringu wykorzystania komputerów służbowych, a także monitoringu służbowej poczty elektronicznej

I. Postanowienia ogólne

§ 1. Niniejszy Regulamin jest zgodny z zasadami zachowania prawa do prywatności pracownika uregulowanego w:

1) Konstytucji Rzeczypospolitej Polskiej, przepisy art. 30, art. 31 ust. 1 i 2, art. 47 oraz art. 51, (prawo do prywatności);
2) Kodeksie cywilnym, ochrony dobra osobistego, jakim jest prywatność, w zakresie przepisów art. 23 i 24;
3) Kodeksie Pracy – zachowany zostaje obowiązek poszanowania godności i innych dóbr osobistych pracownika wynikających z art. 111;
4) warunkach ochrony danych osobowych określonych w rozporządzeniu 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 i ochronie danych)(Dz. U. UE. L. z 2016 r. Nr 119, str. 1 z późn. zm.) - dalej RODO.

§ 2. Regulamin ustala zasady:

1) korzystania z komputerów służbowych i służbowej poczty elektronicznej;
2) monitorowania komputerów służbowych i służbowej poczty elektronicznej;
3) nadzoru nad bezpieczeństwem Systemu Teleinformatycznego w Urzędzie Miasta Starogard Gdański zwanego dalej Urzędem;
4) nadzoru nad ochroną danych osobowych w Urzędzie.

§ 3. 1. Celem wdrożenia Regulaminu jest zachowanie równowagi pomiędzy uzasadnionym interesem pracownika do ochrony jego prywatności, a prawem do ochrony bezpieczeństwa Urzędu, tajemnicy służbowej i mienia pracodawcy, a w szczególności:

1) poprawa jakości i zgodności z procedurami obowiązującymi w Urzędzie wykonywania pracy przez pracowników;
2) zabezpieczenie uzasadnionych interesów pracodawcy;

3) ochrona bezpieczeństwa Urzędu;
4) zabezpieczenie danych oraz mienia pracodawcy;

II. Zasady korzystania z oprogramowania.

§ 4. 1. Zobowiązuje się pracowników do korzystania z legalnego oprogramowania wymienionego w ewidencji, stanowiącej załącznik do Instrukcji Zarządzania Systemem Informatycznym - dostępnej na serverze-10.

2. Instalacje oprogramowania na stanowiskach komputerowych mogą być dokonywane z nośników znajdujących się w zasobach Urzędu. Ich instalacja może być dokonywana wyłącznie przez ASI.

3. Pracownik może dokonać tylko autoryzowanej instalacji. Autoryzowanie instalacji następuje po wydaniu zgody przez ASI, zinwentaryzowaniu oprogramowania i dopisaniu go do ewidencji oprogramowania, o której mowa w ust. 1.

4. Oprogramowanie w wersjach testowych lub w jakikolwiek inny sposób ograniczone umowami licencyjnymi może być użytkowane wyłącznie zgodnie z jego przeznaczeniem i w czasie określonym w umowie licencyjnej.

5. Zabrania się pobierania i kopiowania z Internetu wszelkich utworów (programów komputerowych, utworów muzycznych, filmów, gier komputerowych, itp.), będących przedmiotem ochrony praw autorskich.

6. Naruszenia wyżej wymienionych ustaleń, ze względu na obowiązujące przepisy prawne, stanowią poważne naruszenie dyscypliny pracy.

§ 5. 1. W Urzędzie obowiązuje centralizacja zakupów oprogramowania komputerowego – procedury Systemu Zarządzania Jakością.

2. W Urzędzie obowiązuje wyłącznie pisemna forma zleceń dotyczących zakupu oprogramowania.

3. Decyzję o zakupie nowego oprogramowania w Urzędzie podejmuje wyłącznie Prezydent Miasta na wniosek Sekretarza.

4. Pracownicy nie mogą samodzielnie dokonywać zakupu oprogramowania.

5. Za prowadzenie dokumentacji licencyjnej zakupionego oprogramowania odpowiedzialny jest ASI.

6. Nośniki instalacyjne oprogramowania znajdują się w zamkniętej szafie lub na serwerze zasobów, do których dostęp ma ASI. Nośniki oprogramowania nie mogą być przechowywane w żadnym innym miejscu, a szczególnie nie mogą być kopiowane, wypożyczane lub w żaden inny sposób przekazywane osobom trzecim. Dotyczy to również kodów aktywacyjnych produktów.

7. Przypadki instalowania i uruchamiania oprogramowania niedopuszczonego do użycia przez Urząd (w tym np. oprogramowania skopiowanego własnoręcznie z Internetu), w szczególności, gdy jego uruchomienie wywołuje działania niedozwolone, po ich potwierdzeniu, będą podlegały szczegółowej analizie i mogą być traktowane jako celowe i świadome działanie zmierzające do zwiększenia ryzyka nieprawidłowego działania zasobów i sieci teleinformatycznej Urzędu.

III. Zasady korzystania ze sprzętu komputerowego

§ 6. 1. Sprzęt komputerowy powierza się pracownikom wyłącznie w celu wykonywania obowiązków służbowych.

2. W Urzędzie Pracownikowi zabrania się korzystania ze sprzętu komputerowego, do którego Pracodawca nie jest uprawniony.
3. Zabrania się dokonywania bez autoryzacji ASI zmian w ustawieniach systemowych komputerów, w szczególności: ustawień BIOS-u, ustawień systemu operacyjnego (w tym instalowania urządzeń), ustawień sieci teleinformatycznej.
4. Zabrania się samodzielnego otwierania obudowy komputera oraz innych części komputerowych (np. monitorów, drukarek, myszy).
5. Uprawnionymi do dokonywania czynności, o których mowa w ust. 4 i 5 na warunkach określonych warunkami gwarancji sprzętu, jest ASI.
6. Pracownik, w którego dyspozycji pozostaje sprzęt komputerowy ma obowiązek wyłączyć go po zakończeniu pracy.
7. Korzystanie z nośników danych dopuszczalne jest po wcześniejszym sprawdzeniu ich programem antywirusowym.
8. Pracownik może bez wiedzy i zgody ASI:

1) wymienić toner, tusz, taśmę i inne materiały eksploatacyjne,

2) usunąć zakleszczony papier.

9. Zezwala się Pracownikom na korzystanie z przenośnego komputera służbowego poza miejscem pracy, na zasadach wymienionych w odrębnych przepisach wewnętrznych.

IV. Zasady korzystania z sieci komputerowej (teleinformatycznej) i poczty elektronicznej

§ 7. 1. Do sieci teleinformatycznej może być podłączony tylko sprzęt będący własnością Pracodawcy, z zastrzeżeniem ust. 2.
2. Inny sprzęt komputerowy podłączany jest wyłącznie za zgodą ASI.
3. Zabrania się samowolnego podłączania do sieci komputerów lub innych urządzeń.
4. O rozdziale adresów IP decyduje ASI.
5. Zabrania się wykorzystywania gniazd elektrycznych sieci teleinformatycznej do zasilania innych urządzeń niż komputery i peryferia komputerowe.
6. W celu zapewnienia bezpieczeństwa mechanizmom sieci teleinformatycznej Urzędu oraz dla jej użytkowników Pracownikowi 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 niepożądane lub wrogie działania,

2) skanowania sieci teleinformatycznej Urzędu,

3) prowadzenia ataków, włamań, itp., innych czynności związanych z ingerencją w działanie lub zasoby sieci teleinformatycznej Urzędu, lub Internetu,

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

5*)* anonimowego wysyłania poczty elektronicznej z sieci teleinformatycznej Urzędu,

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

7) uruchamiania programów z komputerowych nośników zewnętrznych, tj. z płyt CD/DVD lub nośników typu pendrive, itp.,

8) rozpowszechnia nielegalnych plików do Internetu, tj. przesyłania zdjęć, filmów, tekstów czy innych formatów plików.

7. Pracownikowi zakazuje się umożliwiania osobom postronnym dostępu do sieci teleinformatycznej Urzędu, np. umożliwienia pracy na identyfikatorach i hasłach Pracownika.
8. Zabrania się Pracownikom Urzędu wykonywania następujących czynności przy użyciu sprzętu i oprogramowania należącego do Pracodawcy :

   1) korzystania z komputera służbowego do celów prywatnych.

   2) używania poczty elektronicznej Urzędu do celów innych niż służbowe,

   3) wykorzystywania połączenia z siecią internet do celów innych niż służbowe,

   4) wysyłania wiadomości pocztowych (e-mail), typu reklamy, „łańcuszki szczęścia", pornograficznych, itp.,

   5)logowania się w celach prywatnych lub komercyjnych na stronach WWW czy uczestniczenia w portalach o charakterze społecznościowym, zwłaszcza towarzyskim, komercyjnych, itp.**,**

   5) używania w celach prywatnych lub komercyjnych komunikatorów internetowych w rodzaju Skype, Gadu-Gadu, Tlen, itp.,

   6) korzystania z serwisów internetowych niezwiązanych z obowiązkami Pracownika, np. oferujących gry internetowe i losowe, hazard, prywatne aukcje, rozrywkę, prywatne listy dyskusyjne., itp.,

   7) przetwarzania na komputerach materiałów, do których Pracodawca nie posiada praw autorskich,

   8) korzystania z serwisów internetowych zawierających treści niecenzuralne lub jakiekolwiek łamiące prawo obowiązujące na terenie Rzeczpospolitej Polskiej,

   9) instalowania i wykorzystywania jakiegokolwiek oprogramowania bez wiedzy i udziału osób odpowiedzialnych za tego rodzaju czynności w Urzędzie.

   10) zapisywania, przechowywania na dyskach lokalnych lub zasobach sieciowych wszelkich plików multimedialnych niezwiązanych z wykonywaniem czynności służbowych,

   11) używania sprzętu komputerowego poza siedzibami Urzędu bez wcześniejszego powiadomienia Sekretarza Miasta,

   12) samodzielnej zmiany konfiguracji sprzętowej zestawu i jego ustawień systemowych bez zgody ASI,

   13) udostępniania innym użytkownikom haseł dostępowych i ich przechowywanie w łatwo dostępnych lub widocznych miejscach,

14) używania nośników danych nieznanego pochodzenia oraz nośników wymiany pamięci wcześniej nie zgłoszonych do ASI.

9. O każdej usterce sprzętu należy powiadomić ASI. Za dane i wykonywanie kopii danych przechowywanych na dyskach lokalnych odpowiada użytkownik zestawu komputerowego.

V. Procedury kontrolne dotyczące komputerowego stanowiska pracy w Urzędzie

§ 8. Wszelkie czynności pracownika w zakresie działań pracodawcy zmierzających do poprawy jakości pracy z komputerem polegające, w szczególności na eliminowaniu możliwości pobierania określonych danych z Internetu, odciążeniu sieci informatycznej, poprzez ograniczenie możliwości transferu danych z lub do komputera pracownika, usuwaniu nielegalnego oprogramowania, blokowania dostępu do nielegalnych treści oraz kontroli antywirusowej związane są bezpośrednio z bezpieczeństwem Urzędu i ochroną danych osobowych, będą monitorowane.

§ 9. Monitorowanie pracy pracowników przy wykorzystaniu komputerów służbowych będzie przeprowadzone na bazie dedykowanego oprogramowania, będącego własnością pracodawcy, który posiada do niego stosowaną licencję.

§ 10. Zakresem monitoringu w Urzędzie objęte są:

1) kontrola zdarzeń na komputerze użytkownika;
2) przesyłanie alertów na komputer pracownika przez administratora sieci informatycznej;
3) monitoring używanych przez pracownika aplikacji;
4) możliwość blokowania zbędnych aplikacji, lub stron internetowych;
5) monitoring wykonywanych przez pracowników wydruków;
6) monitoring odwiedzanych przez pracowników stron internetowych;
7) możliwość podglądu on-line ekranu każdego komputera w Urzędzie;
8) monitoring ruchu w sieci informatycznej (LAN, WAN) Urzędu;
9) monitoring legalności oprogramowania;
10) powiadamianie o monitorowaniu każdego użytkownika po uruchomieniu komputera;
11) monitoring służbowych kont poczty e-mail. Pracodawca zastrzega sobie prawo do kontroli treści wysłanych i otrzymanych e-maili z konta służbowego;
12) monitoring używania przenośnych nośników danych (pendrive, karty pamięci, CD-ROM, HDD, itp.) z możliwością blokowana, jak i odczytania ich treści;
13) monitoring podłączonego sprzętu w Urzędzie.

§ 11. 1. Ruch w sieci teleinformatycznej Urzędu, generowany przez Pracownika, podlega monitoringowi z automatycznym zapisem dostępu do stron WWW.

2. Informacje statystyczne potwierdzające: adresy sieciowe, czas dostępu do najczyściej odwiedzanych przez Pracowników serwisów internetowych, gromadzonych plików oraz uruchamianych aplikacji mogą:

1) podlegać analizie i przekazaniu do kierowników komórek organizacyjnych,
2) stanowić podstawę do dalszych kroków podejmowanych na drodze służbowej.

3. Dane z ruchu w sieci informatycznej będą przechowywane przez okres 2 lat.

4. Monitoring poczty elektronicznej pracownika nie może naruszać tajemnicy korespondencji oraz innych dóbr osobistych pracownika.

§ 12. Prezydent Miasta Starogard Gdański lub Sekretarz Miasta Starogard Gdański może w indywidualnych przypadkach wydać polecenie zaniechania czynności opisanych w Regulaminie tj. monitoringu służbowej poczty elektronicznej i monitoringu wykorzystania komputerów służbowych - w stosunku do niektórych osób, na czas określony lub nieokreślony.

§ 13. Wszelkie dane uzyskane w wyniku monitoringu przechowywane będą zgodnie z RODO.

§ 14. Informacje dotyczące celów, zakresu oraz sposobu monitoringu przekazuje się pracownikowi przed dopuszczeniem pracownika do pracy. Treść informacji stanowi załącznik nr 4b do Regulaminu.