Załącznik do Zarządzenia Nr 55 /2020
Burmistrza Miasta Mława
z dnia 7 kwietnia 2020 r .

Szczegółowe warunki i zasady korzystania z technologii informacyjno-komunikacyjnej w czasie realizacji zadań poza siedzibą Urzędu Miasta Mława

1. Każdy pracownik Urzędu Miasta Mława korzystający ze służbowego sprzętu IT zobowiązany jest do jego zabezpieczenia przed zniszczeniem lub uszkodzeniem. Za sprzęt IT przyjmuje się: komputery stacjonarne, monitory, drukarki, skanery, ksera, modemy, laptopy, służbowe tablety i smartfony.
2. Pracownik jest zobowiązany niezwłocznie zgłosić Naczelnikowi Wydziału Organizacyjnego zagubienie, utratę lub zniszczenie powierzonego mu sprzętu IT.
3. Samowolna ingerencja w konfigurację sprzętową służbowego sprzętu informatycznego (otwieranie obudowy, instalowanie lub demontaż jakichkolwiek wewnętrznych komponentów sprzętowych), instalowanie dodatkowych urządzeń (np. twardych dysków, pamięci) lub podłączanie jakichkolwiek niezatwierdzonych urządzeń do systemu informatycznego jest zabronione.
4. Przed czasowym opuszczeniem stanowiska pracy, pracownik Urzędu zobowiązany jest zablokować stację roboczą poprzez wciśnięcie kombinacji klawiszy (WINDOWS + L) lub wylogować się z systemu oraz programów.
5. Po zakończeniu pracy, pracownik Urzędu zobowiązany jest:
    1) wylogować się z systemu informatycznego, wyłączyć sprzęt komputerowy,
    2) zabezpieczyć stanowisko pracy oraz wszelkie nośniki magnetyczne i optyczne, natomiast pliki zawierające dane osobowe, skarbowe muszą znajdować się na szyfrowanym dysku w laptopie.
6. Pracownik jest zobowiązany do usuwania plików z nośników/dysków, do których mają dostęp inne osoby nieupoważnione do dostępu do takich plików (np. podczas współużytkowania komputerów prywatnych).
7. Zabrane przez Pracownika dane służbowe w celu wykonywania pracy zdalnej na pendriwach, dyskach zewnętrznych, płytach muszą być przeniesione na dysk zaszyfrowany na laptopach służbowych.

8. Pracownicy Urzędu, użytkujący służbowe komputery przenośne, na których znajdują się dane osobowe lub z dostępem do danych osobowych przez Internet zobowiązani są do stosowania zasad bezpieczeństwa określonych w polityce ochrony danych osobowych.
9. W trakcie pracy zdalnej, w sytuacji, gdy pracownicy Urzędu korzystają ze swojego prywatnego sprzętu komputerowego, ponoszą odpowiedzialność za bezpieczeństwo danych służbowych, które gromadzą i są zobowiązani do przestrzegania procedur określonych w polityce ochrony danych osobowych, bezpieczeństwa informacji.
10. Urząd Miasta Mława nie ponosi odpowiedzialności za prywatny sprzęt komputerowy.
11. Każdy pracownik – zwany dalej użytkownikiem (np. komputera stacjonarnego, laptopa, dysku sieciowego, programów, w których użytkownik pracuje, poczty elektronicznej, itp.) musi posiadać swój własny indywidualny identyfikator (login) do logowania się.
12. Każdy użytkownik musi posiadać indywidualny identyfikator. Zabronione jest umożliwianie innym osobom pracy na koncie innego użytkownika.
13. Zabrania się pracy wielu użytkowników na wspólnym koncie sieciowym.
14. Użytkownik (np. komputera stacjonarnego, laptopa, dysku sieciowego, programów, w których użytkownik pracuje, poczty elektronicznej) rozpoczyna pracę z użyciem identyfikatora i hasła.
15. Użytkownik jest zobowiązany do niezwłocznego powiadomienia informatyków Urzędu o próbach logowania się do systemu osoby nieupoważnionej.
16. Po zakończeniu pracy, użytkownik zobowiązany jest:
    1) wylogować się z systemu informatycznego, a następnie wyłączyć sprzęt komputerowy,
    2) zabezpieczyć stanowisko pracy, w szczególności wszelką dokumentację oraz nośniki magnetyczne i optyczne, na których znajdują się dane osobowe.
17. Zabrania się zgrywania na dysk twardy komputera służbowego oraz uruchamiania jakichkolwiek programów oraz plików pobranych z niewiadomego źródła. Instalacja jakiegokolwiek oprogramowania na służbowym sprzęcie powinna wynikać z przyjętej polityki bezpieczeństwa lub innych regulacji obowiązujących w Urzędzie Miasta Mława. Odstępstwo od tej reguły może zaakceptować tylko Naczelnik Wydziału Organizacyjnego.
18. 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).

19. Nie należy w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł.
20. 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. Należy wystrzegać się wchodzenia na strony lub pobierać pliki, gdzie adres ma postać liczbową np. http://10.126.15.12/. W 95% przypadków są to zasoby niebezpieczne.
21. Należy zachować szczególną ostrożność w przypadku podejrzanego żądania lub prośby zalogowania się na stronę (np. na stronę banku, portalu społecznościowego, e-sklepu, poczty e-mailowej) lub podania naszych loginów i haseł, PIN-ów, numerów kart płatniczych przez Internet. Szczególnie tyczy się to żądania podania takich informacji przez rzekomy bank.
22. W przypadku przesyłania danych osobowych należy wysyłać pliki zaszyfrowane/spakowane (np. programem 7 zip, winzipem, winrarem) i zahasłowane, gdzie hasło powinno być przesłane do odbiorcy telefonicznie lub SMS-em.
23. W przypadku zabezpieczenia plików hasłem, obowiązuje minimum 8 znaków: duże litery + małe litery + cyfry + znaki specjalne, a hasło należy przesłać odrębnym e-mailem lub inną metodą, np. telefonicznie lub SMS-em.
24. Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu.
25. Zaleca się, aby użytkownik podczas przesyłania danych osobowych e-mailem zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata.
26. Nie wolno otwierać załączników od nieznanych nadawców typu .zip, .xlsm, .exe w e-mailach. Są to zwykle „wirusy”, które infekują komputer oraz często pozostałe komputery w sieci. WYSOKIE RYZYKO BEZPOWROTNEJ UTRATY DANYCH.
27. Nie wolno „klikać” na hiperlinki w e-mailach od nieznanych nadawców, gdyż mogą to być hiperlinki do stron z „wirusami”. Użytkownik „klikając” na taki hiperlink infekuje komputer oraz inne komputery w sieci.
28. Podczas wysyłania e-maili do wielu adresatów spoza Urzędu jednocześnie, należy użyć metody „Ukryte do wiadomości – UDW”.
29. Zabronione jest rozsyłanie e-maili do wielu adresatów z użyciem opcji „Do wiadomości” Nie dotyczy e-maili wysyłanych ramach Urzędu Miasta Mława.
30. Użytkownicy powinni okresowo kasować niepotrzebne e-maile, a e-maile podejrzane powinni usuwać na bieżąco wraz z opróżnieniem „kosza” w aplikacji poczty elektronicznej.

31. Przy korzystaniu z e-maila, użytkownicy mają obowiązek przestrzegać prawa własności przemysłowej i prawa autorskiego.

32. Użytkownicy nie mają prawa korzystać z e-maila w celu rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec powszechnie obowiązujących zasad postępowania. Zabronione jest również rozsyłanie tzw. łańcuszków, w których nadawca prosi o przesłanie wiadomości do jak największej grupy odbiorców powołując się na „szlachetną" inicjatywę.

33. Stosując zasady określone w niniejszym dokumencie jednocześnie należy przestrzegać wdrożony i obowiązujący System Zarządzania Bezpieczeństwem Informacji (SZBI) oraz Politykę Bezpieczeństwa Informacji.