Zarządzenie wewnętrzne Nr 42/2023
Dyrektora Miejskiego Zarządu Budynków Komunalnych w Kędzierzynie-Koźlu
z dnia 11 grudnia 2023 roku

w sprawie wprowadzenia procedur dotyczących bezpieczeństwa informatycznego Miejskiego Zarządu Budynków Komunalnych w Kędzierzynie-Koźlu

Działając na podstawie § 3 ust. 3 w związku z § 3 ust. 1 Statutu Miejskiego Zarządu Budynków Komunalnych w Kędzierzynie-Koźlu wprowadzonego Uchwałą Nr LVIII/682/23 Rady Miasta Kędzierzyn-Koźle z dnia 25 maja 2023r. w sprawie statutu Miejskiego Zarządu Budynków Komunalnych w Kędzierzynie-Koźlu[1)] w związku z Ustawą z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2023r. poz. 57 ze zm.) oraz Rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017r. poz. 2247), zarządzam co następuje:

§ 1. Wprowadzam do stosowania:

1. **Procedurę zarządzania sprzętem informatycznym i oprogramowaniem w Miejskim Zarządzie Budynków Komunalnych w Kędzierzynie-Koźlu**, stanowiącą załącznik Nr 1 do niniejszego Zarządzenia,
2. **Procedurę tworzenia kopii zapasowych**, stanowiącą załącznik Nr2 do niniejszego Zarządzenia.

§ 2. Pana Sylwestra Lecht – Administratora Systemu Informatycznego, dalej ASI zobowiązuję do prowadzenia Ewidencji Oprogramowania i Ewidencji zasobów informatycznych, o których mowa w procedurze określonej w § 1 ust. 1.

§ 3. Zobowiązuję wszystkich pracowników uczestniczących w procesach przetwarzania informacji do zapoznania się z procedurami o których mowa w § 1 i ich przestrzegania.

§ 4. 1. Zarządzenie wchodzi w życie z dniem wydania. Zarządzenie nie podlega ogłoszeniu w BIP.

DYREKTOR
Stanisław Węgrzyn

Otrzymują do wiadomości i realizacji :
1) Pracownicy uczestniczący w procesach przetwarzania informacji,
2) a/a.

[1] Uchwała została zmieniona następującą uchwałą : Uchwałą Nr LIX/693/23 Rady Miasta Kędzierzyn-Koźle z dnia 27 czerwca 2023 roku.

Załącznik Nr. 1 do Zarządzenia wewnętrznego Nr 42/2023 Dyrektora Miejskiego Zarządu Budynków Komunalnych w Kędzierzynie-Koźlu z dnia 11 grudnia 2023 roku.

Procedura zarządzania sprzętem informatycznym i oprogramowaniem w Miejskim Zarządzie Budynków Komunalnych w Kędzierzynie-Koźlu

§ 1
Postanowienia ogólne

Niniejszy Procedura ustala zasady:

a) zakupu komputerów i innego sprzętu informatycznego,
b) korzystania z komputerów służbowych,
c) korzystania z oprogramowania,
d) zarządzania oprogramowaniem,
e) korzystania z zasobów informatycznych sieci komputerowej,
f) korzystania z służbowej poczty elektronicznej,
g) monitorowania pracy pracowników przy wykorzystaniu komputerów służbowych.

§ 2.
Zasady zakupu komputerów służbowych i innego sprzętu informatycznego

1. Podstawą zakupu komputerów (stacjonarnych i przenośnych) i innego sprzętu informatycznego jest wniosek złożony przez Kierownika Komórki Organizacyjnej, wskazujący bezpośredniego użytkownika (użytkowników) lub przyszłego użytkownika (w przypadku tworzenia nowego stanowiska) sprzętu. Wniosek jest opiniowany przez ASI pod kątem zasadności zakupu, z uwagi na posiadane aktywa informatyczne i ich przydatność. Wniosek przekazywany jest następnie do akceptacji przez Dyrektora MZBK.
2. Po akceptacji zakup dokonywany jest zgodnie z procedurami wewnętrznymi dotyczącymi zamówień publicznych z uwzględnieniem zapisów Ustawy z dnia 19 września 2019 roku – Prawo zamówień publicznych (t.j. Dz.U. z 2023 r. poz. 1605, 1720 z późn. zm.).
3. Powierzenie sprzętu użytkownikowi następuje na podstawie Karty przyjęcia środka trwałego OT i wpisaniu sprzętu do ewidencji prowadzonej przez Dział Księgowości oraz Ewidencji Zasobów Informatycznych, za prowadzenie której odpowiedzialny jest ASI.
4. Wzór „Ewidencji zasobów informatycznych" stanowi załącznik nr 1 do Procedury i określa minimalny zakres danych, które powinny być w niej umieszczone.

§ 3.
Zasady korzystania ze sprzętu komputerowego

1. Sprzęt komputerowy powierza się pracownikom wyłącznie w celu wykonywania obowiązków służbowych.
2. 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. 3 i 4 na warunkach określonych warunkami gwarancji sprzętu, jest ASI, inna osoba upoważniona przez

Dyrektora lub zewnętrzy podmiot świadczący usługę serwisową, po uzgodnieniu i akceptacji z ASI lub Dyrektorem, w razie ich nieobecności, z Zastępcą Dyrektora MZBK.

6. Pracownik, w którego dyspozycji pozostaje sprzęt komputerowy ma obowiązek wyłączyć go po zakończeniu pracy.
7. Korzystanie z nośników danych dopuszczalne jest po wcześniejszym zaakceptowaniu ich przez ASI. Nośniki danych przed podłączeniem powinny być sprawdzone programem antywirusowym.
8. Pracownik ma prawo bez wiedzy i zgody ASI:
   1) wymienić toner, tusz, taśmę i inne materiały eksploatacyjne,
   2) usunąć zakleszczony papier.
9. Zezwala się na korzystanie z przenośnego komputera służbowego (urządzenia mobilnego) poza miejscem pracy, pod warunkiem przestrzegania zasad wymienionych poniżej:
   1) wszyscy pracownicy MZBK korzystający z komputerów przenośnych (urządzeń mobilnych np. laptop, tablet, smartfon. telefon komórkowy) mogą korzystać z nich poza miejscem pracy zachowując obowiązujące w MZBK zasady korzystania z oprogramowania;
   2) zabrania się użyczania komputerów (urządzeń mobilnych) osobom postronnym;
   3) komputer przenośny (urządzenie mobilne) wymaga zachowania szczególnej ostrożności podczas jego transportu, przechowywania i użytkowania;
   4) stosowanie komputerów przenośnych (urządzeń mobilnych) poza obszarem przetwarzania MZBK, w szczególności wyniesienie ich poza MZBK, wymaga fizycznego ich zabezpieczenia przed kradzieżą i zgubieniem;
   5) komputery przenośne (urządzenia mobilne) i dane na nich, w miarę możliwości powinny być zamaskowane, a urządzenia zaopatrzone w minimalne dane kontaktowe właściciela;
   6) komputery przenośne (urządzenia mobilne) wynoszone poza obszar przetwarzania lub poza MZBK zabezpiecza się środkami ochrony kryptograficznej, co oznacza szyfrowanie danych narzędziami dostarczonymi przez ASI.

§ 4.
Zasady korzystania z oprogramowania

1. Zobowiązuje się pracowników do korzystania tylko z legalnego oprogramowania wymienionego w ewidencji prowadzonej przez ASI. Wzór „Ewidencji oprogramowania" stanowi załącznik nr 2 do niniejszej procedury i określa minimalny zakres danych, które powinny się w niej umieszczone.
2. Instalacje oprogramowania na stanowiskach komputerowych mogą być dokonywane z nośników znajdujących się w zasobach MZBK. Ich instalacja może być dokonywana wyłącznie przez ASI lub inną osobę upoważnioną przez Dyrektora.
3. Oprogramowanie może być tylko instalowane po autoryzacji. Autoryzowanie instalacji następuje po wydaniu zgody przez ASI, zinwentaryzowaniu oprogramowania i dopisaniu go do ewidencji oprogramowania oraz ewidencji środków trwałych i niematerialnych prowadzonej przez dział DK.
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 plików (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.
Zasady zarządzania oprogramowaniem i zasobami informatycznymi

1. W MZBK obowiązuje centralizacja zakupów oprogramowania komputerowego.
2. Decyzję o zakupie nowego oprogramowania w MZBK podejmuje Dyrektor lub osoba upoważniona, po konsultacji z ASI.
3. Pracownicy nie mogą samodzielnie dokonywać zakupu oprogramowania.
4. Za prowadzenie dokumentacji licencyjnej zakupionego oprogramowania odpowiedzialny jest ASI. Zakupione oprogramowanie wprowadzane jest do ewidencji prowadzonej przez Dział Księgowości oraz Ewidencji oprogramowania, za prowadzenie której odpowiedzialny jest ASI.
5. 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.
6. Zgromadzenie oprogramowania wraz z dowodami potwierdzającymi ich legalność (dokumentacja, certyfikaty, licencje, nośniki, nalepki, itp.) i przechowywanie ich w wyodrębnionym miejscu, należy do obowiązków ASI.
7. Przypadki instalowania i uruchamiania oprogramowania niedopuszczonego do użycia przez MZBK (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 działania zasobów i sieci teleinformatycznej MZBK.
8. Likwidacji podlega oprogramowanie, które:
   1) nie jest i nie będzie mogło być wykorzystywane w realizacji zadań związanych z działalnością MZBK;
   2) nie nadaje się do współpracy ze sprzętem lub/i oprogramowaniem w MZBK, a ich przystosowanie byłoby technicznie i ekonomicznie nieuzasadnione;
   3) podczas przeprowadzania audytu oprogramowania wykryto braki odpowiedniej liczby atrybutów legalności.
9. Likwidacja oprogramowania odbywa się na podstawie opinii ASI określającej niemożliwość dalszego użytkowania (przestarzałość, nieprzydatność, wygaśnięcie licencji, brak kompatybilności z używanymi systemami operacyjnymi). Opinia dołączana jest do wniosku o likwidację.
10. Ewidencja zasobów informatycznych oraz Ewidencja oprogramowania powinna być aktualizowania w przypadku nastąpienia zmian danych w nich zawartych. O zmianach skutkujących zmianą osoby użytkującej i odpowiedzialnej, likwidacją zasobu informatycznego ASI niezwłocznie powiadamia Dział Księgowości celem aktualizacji danych w ewidencjach środków trwałych i niematerialnych.
11. Przegląd aktualności danych zawartych w ewidencjach wymienionych w ust. 10 powinien być dokonywany nie rzadziej niż raz na kwartał. Z przeglądu ASI tworzy informację zatwierdzaną przez Dyrektora MZBK.

§ 6.
Zasady korzystania z zasobów informatycznych sieci komputerowej

1. Do sieci komputerowej (teleinformatycznej) MZBK może być podłączony tylko sprzęt będący własnością MZBK, 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 w celu zasilania innych urządzeń niż komputery i peryferia komputerowe.

6. Zabrania się przerabiania gniazd sieci komputerowej (logicznej i elektrycznej) i podłączania do nich urządzeń bez zgody ASI.
7. Pracownik ma prawo korzystać z zasobów sieci komputerowej (teleinformatycznej) w zakresie wykonywanych czynności służbowych.
8. W celu zapewnienia bezpieczeństwa mechanizmom sieci teleinformatycznej MZBK oraz jej użytkowników 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 MZBK;
   3) prowadzenia ataków, włamań, itp., innych czynności związanych z ingerencją w działanie lub zasoby sieci teleinformatycznej MZBK, 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 MZBK;
   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) rozpowszechniania plików do Internetu, tj. przesyłania zdjęć, filmów, tekstów czy innych formatów plików.
9. Postanowienia ust. 8 punkty 2, 7 nie dotyczą ASI oraz osób trzecich, które realizują zadania na rzecz MZBK, na podstawie umów, gdzie użyte technologie winny być ustalone z ASI.
10. Zakazuje się umożliwiania osobom postronnym dostępu do sieci teleinformatycznej MZBK np. umożliwienia pracy na identyfikatorach i hasłach pracownika.
11. Zabrania się Pracownikom MZBK wykonywania następujących czynności przy użyciu sprzętu i oprogramowania należącego do Pracodawcy:
   1) używania poczty elektronicznej MZBK do celów innych niż służbowe;
   2) wysyłania wiadomości pocztowych (e-mail), typu reklamy, „łańcuszki szczęścia", pornograficznych, itp.;
   3) logowania się w celach prywatnych lub komercyjnych na stronach WWW czy uczestniczenia w portalach o charakterze społecznościowym, zwłaszcza towarzyskim, komercyjnych, itp.;
   4) używania w celach prywatnych lub komercyjnych komunikatorów internetowych w rodzaju Skype, itp.;
   5) korzystania z serwisów internetowych niezwiązanych z obowiązkami Pracownika, np. oferujących gry internetowe i losowe, hazard, prywatne aukcje, rozrywkę, prywatne listy dyskusyjne, itp.;
   6) przetwarzania na komputerach, materiałów do których Pracodawca nie posiada praw autorskich;
   7) korzystania z serwisów internetowych zawierających treści niecenzuralne lub jakiekolwiek łamiące prawo obowiązujące na terenie Rzeczpospolitej Polskiej;
12. Dopuszcza się możliwość stosowania i korzystania w MZBK z sieci i połączeń VPN (połączeń zdalnych).
13. W celu zapewnienia bezpieczeństwa sieci VPN (połączeń zdalnych) należy stosować odpowiednie kategorie zabezpieczeń:
   1) zabezpieczenia programowe (hasła, klucze zaszyfrowane w plikach);
   2) zabezpieczenia sprzętowe (tokeny haseł jednorazowych, tokeny kryptograficzne)
14. W sytuacji, gdy w używanych przez MZBK programach, aplikacjach, internetowych portalach instytucji, urzędów, organizacji, firm, z którymi MZBK prowadzi interakcje, ASI nie może ze względów technicznych zmienić (zresetować) hasła użytkownika, wprowadza

się obowiązek rejestrowania haseł i loginów, w celu zapewnienia bezpieczeństwa i ciągłości pracy na poszczególnych stanowiskach

§ 7.

Zasady korzystania z służbowej poczty elektronicznej

1. Nadzór i opiekę techniczną nad systemem poczty elektronicznej MZBK sprawuje ASI.
2. Poczta elektroniczna może być wykorzystywana tylko do celów służbowych.
3. Korespondencja, którą przechowuje i dostarcza system pocztowy jest własnością MZBK.
4. Pracownik zobowiązany jest do okresowej archiwizacji wiadomości (skrzynki pocztowe posiadają ograniczoną wielkość).
5. Użytkownikom poczty zabrania się:
   1) otwierania linków oraz załączników poczty elektronicznej ze źródeł niewiadomego pochodzenia;
   2) przesyłania i udostępniania danych naruszających prawo, powszechnie uznanych za obsceniczne lub obraźliwe oraz oszczerstw i treści obrażającej uczucia innych;
   3) rozpowszechniania materiałów o treści pornograficznej, propagujących przemoc, nawołujących do nietolerancji i nienawiści itp., lub naruszających obowiązujące prawo;
   4) uprawiania hazardu;
   5) rozpowszechniania niechcianych wiadomości e-mail (spam-u);
   6) prowadzenia działalności komercyjnej nie związanej z działalnością MZBK;
   7) rozsyłania listów, które wykorzystując elementy socjotechniki generują niepożądany ruch na serwerach poczty elektronicznej oraz treści prawem chronionych bez odpowiedniego zabezpieczenia np. szyfrowania;
   8) przesyłania i udostępniania treści niezgodnych z prawem lub będących przedmiotem ochrony własności intelektualnej lub mogących naruszyć czyjekolwiek prawa osobiste;
   9) rozpowszechniania wirusów komputerowych i innych programów mogących uszkodzić komputery innych użytkowników Internetu;
6. Niedopuszczalne są próby włamań na konta innych użytkowników.
7. MZBK w celach dowodowych oraz bezpieczeństwa systemów ma prawo do kontroli służbowych skrzynek pocztowych Pracowników, informując ich o kontroli i jej wynikach.

§ 8.

Procedury kontrolne, audyt wewnętrzny sprzętu i oprogramowania komputerowego

1. Wprowadza się obowiązek kontrolny zawartości komputerów stanowiących własność MZBK wykorzystywanych przez pracowników MZBK, dla zapewnienia ochrony zasobów teleinformatycznych i danych MZBK. Procedury sprawdzające komputerów pracowników MZBK nadzoruje ASI.
2. Procedury sprawdzające mogą być realizowane są przy pomocy specjalistycznego oprogramowania, którego raporty stanowią podstawę dla działań naprawczych podejmowanych przez ASI.
3. Ruch w sieci teleinformatycznej MZBK, generowany przez pracowników, podlega monitoringowi.
4. Informacje statystyczne potwierdzające: adresy sieciowe, czas dostępu do najczęściej odwiedzanych przez pracowników MZBK serwisów internetowych, gromadzonych plików oraz uruchamianych aplikacji mogą:
   1) podlegać analizie i przekazaniu do Dyrektora MZBK;
   2) stanowić podstawę do dalszych kroków podejmowanych na drodze służbowej.
5. Za przeprowadzenie audytu wewnętrznego odpowiada ASI.
6. Audyt obejmuje:
   1) kontrolę legalności zainstalowanego oprogramowania poprzez identyfikację zainstalowanych aplikacji na komputerach pracowników MZBK;
   2) skanowanie zawartości dysków w celu wyeliminowania ukrytych zawartości plików;

3) kontrolę modyfikacji sprzętu komputerowego;
4) prowadzenie statystyk w zakresie:
   - wykorzystywania poszczególnych aplikacji,
   - rzeczywistego czasu pracy poszczególnych stacji roboczych,
   - korzystania z Internetu.

7. Kontrole będą przeprowadzane raz w roku - ogólne oraz doraźnie - na wybranych stanowiskach.
8. Z przeprowadzonych kontroli Administrator Systemu Informatycznego sporządza raporty, które przedkładane będą Dyrektorowi MZBK.

§ 9
Katalog działań specjalnych, dozwolonych dla pracowników oraz ASI

1. Niektóre działania zabronione, określone w § 6 pkt. 8, ust. 2, 7, 8 mogą być wykonywane w przypadku:
   1) realizacji działań zgodnych z zakresem obowiązków, poleceniem przełożonego lub przepisami szczególnymi obowiązującymi pracowników MZBK;
   2) prowadzenia interakcji z internetowymi portalami instytucji, urzędów, organizacji, w celu realizacji zadań czy wykonywania obowiązków;
   3) uzyskaniem pisemnej zgody Dyrektora;
   4) realizacji na rzecz MZBK, poprzez osoby trzecie, zapisów umów, zwłaszcza, gdy niezbędne jest ustanowienie interoperacyjności pomiędzy systemami teleinformatycznymi urzędu i systemami zewnętrznymi.

§ 10.
Postanowienia końcowe

1. Kończąc świadczenie pracy dla MZBK, Pracownik jest zobowiązany przekazać wszystkie dane zapisane w komputerze (dokumenty służbowe tworzone i przechowywane w pamięci komputera, pliki oraz inne posiadane informacje) związane z wykonywanymi zadaniami służbowymi przełożonemu i ASI.
2. Ewidencja zasobów informatycznych oraz Ewidencja oprogramowania mogą być prowadzone w wersji elektronicznej.
3. Zastrzega się możliwość aktualizacji i wprowadzania zmian do treści niniejszej Procedury w zakresie związanym z postępem technicznym lub dotyczącym używania technologii informatycznej.
4. Każdy z pracowników zobowiązany jest podpisać oświadczenie, stanowiące załącznik nr 3 do niniejszej procedury, o przyjęciu do wiadomości i stosowania ustaleń Procedury. Oświadczenie wpinane jest do akt osobowych pracowników.

DYREKTOR
Stanisław Węgrzyn

MIEJSKI ZARZĄD
BUDYNKÓW KOMUNALNYCH
w Kędzierzynie - Koźlu
ul. Grunwaldzka 6
47 - 220 Kędzierzyn - Koźle
Regon: 530859315, tel. 77 483 49 81

Załącznik Nr 1 do Procedury zarządzania sprzętem informatycznym i oprogramowaniem wprowadzonej Zarządzeniem Nr 42/2023 z 11 grudnia 2023 roku

Ewidencja zasobów informatycznych

Lp.	Rodzaj zasobu	Nr inwentarzowy	Cel w jakim zasób jest eksploatowany	Nazwa urządzenia w sieci	Adres (Adresy) IP	Adres (Adresy) MAC	Komórka Organizacyjna użytkująca zasób	Użytkownik korzystający z zasobu	Parametry konfiguracyjne (np. procesor, płyta główna, pamięć operacyjna, dysk twardy)	Zainstalowane oprogramowanie (powiązanie z ewidencją oprogramowania)

Data sporządzenia	Data ostatniej aktualizacji	Podpis osoby odpowiedzialnej za prowadzenie ewidencji

MIEJSKI ZARZĄD
BUDYNKÓW KOMUNALNYCH
w Kędzierzynie - Koźlu
ul. Grunwaldzka 6
47 - 220 Kędzierzyn - Koźle
Regon: 530859315, tel. 77 483 49 81

Załącznik Nr 2 do Procedury zarządzania sprzętem informatycznym i oprogramowaniem wprowadzonej Zarządzeniem Nr 42/2023 z 11 grudnia 2023 roku

Ewidencja oprogramowania

Lp.	Nazwa oprogramowania	Nr inwentarzowy	Miejsce instalacji (powiązanie z ewidencją zasobów informatycznych)	Wersja oprogramowania	Warunki licencjonowania	Dowody licencyjne (Nr faktury)	Komórka Organizacyjna użytkująca oprogramowanie	Użytkownik korzystający z oprogramowania	Wsparcie oprogramowania

Data sporządzenia	Data ostatniej aktualizacji	Podpis osoby odpowiedzialnej za prowadzenie ewidencji

Załącznik Nr 3 do Procedury zarządzania sprzętem informatycznym i oprogramowaniem wprowadzonej Zarządzeniem Nr 42/2023 z 11 grudnia 2023 roku

_____
imię i nazwisko

_____
stanowisko służbowe

OŚWIADCZENIE

Oświadczam, że przyjąłem/przyjęłam do wiadomości i stosowania przepisy **Zarządzenia wewnętrznego Nr 42/2023 Dyrektora Miejskiego Zarządu Budynków Komunalnych w Kędzierzynie-Koźlu z dnia 11 grudnia 2023 roku**, a w szczególności, iż w MZBK istnieje **całkowity zakaz**:

1. samodzielnego podłączania jakichkolwiek urządzeń oraz nośników zewnętrznych do służbowych komputerów;
2. dokonywania nieuprawnionych zmian w systemach informatycznych lub informacji w nich przetwarzanych;
3. dokonywania nieuprawnionych prób testowania zauważonych podatności (luk w zabezpieczeniu systemu);
4. dokonywania nieuprawnionych prób wyjaśniania incydentów;
5. wykorzystywania Internetu i poczty elektronicznej do celów innych niż służbowe, a w szczególności:
    1) uznanych powszechnie za szkodliwe, niewłaściwe, niemoralne lub nielegalne;
    2) ściągania z Internetu i rozsyłania przy pomocy poczty elektronicznej informacji niezwiązanych z realizowanymi zadaniami służbowymi;
    3) nieprzestrzegania praw autorskich w stosunku do materiałów zamieszczonych w sieci.
6. wprowadzania nieuprawnionych zmian w zatwierdzonej konfiguracji bazowej, stosowania nielegalnego oprogramowania, nieupoważnionego logowania się poza nominalnymi godzinami pracy (chyba, że pracownik posiada zgodę na inny czas pracy), prób dostępu do plików i folderów do których użytkownik nie ma dostępu;
7. nieuprawnionego pozyskiwania informacji o zasobach informatycznych i środkach ich ochrony;
8. nieuprawnionego instalowania oprogramowania, zwłaszcza oprogramowania, którego jednostka organizacyjna nie ma prawa używać np. z powodu braku wymaganych licencji.

Sprzęt informatyczny winien być użytkowany wyłącznie w celach służbowych.
Na stanowiskach pracy mogą być wykorzystywane wyłącznie oprogramowania legalne oraz zawierające dane niezbędne do wykonywania zadań służbowych.

Instalacje oprogramowania na stanowiskach pracy w MZBK dokonywane są z nośników znajdujących się w zasobach ww. jednostki przez upoważnione osoby. Wykorzystywanie Internetu i poczty elektronicznej, a także infrastruktury sieciowej resortu jest monitorowane. Wszelkie nieprzestrzeganie przepisów i ustaleń w przedmiotowym zakresie stanowić będzie poważne naruszenie obowiązków służbowych oraz dyscypliny pracy. Podejmowanie nieuprawnionych działań mogących obniżyć poziom bezpieczeństwa infrastruktury teleinformatycznej resortu, wynikających

z niezastosowania się do reguł, o których mowa w niniejszym zarządzeniu, będzie uznane za działanie na szkodę MZBK, jak również stanowić będzie naruszenie obowiązków pracowniczych i może być przyczyną pociągnięcia do odpowiedzialności służbowej lub karnej.

Za zainstalowane oprogramowania na serwerach MZBK odpowiada administrator tych serwerów wg posiadanych uprawnień. Dodatkowe, legalne oprogramowanie może być zainstalowane na pisemny wniosek zaakceptowany przez IOD i Administratora Systemu Informatycznego. Administrator Systemu Informatycznego prowadzi kontrolę legalności oprogramowania, do której mogą być wykorzystywane programy kontrolne. Kontrole przeprowadza się raz w roku – ogólne, oraz doraźnie na wybranych stanowiskach. Z przeprowadzonych kontroli Administrator Systemu Informatycznego sporządza raporty, które przedkładane są Dyrektorowi.
Nadzór nad wykonywaniem przepisów zarządzenia sprawuje Administrator Systemu Informatycznego.

Zapoznanie się z w/w poleceniami potwierdzam własnoręcznym podpisem.

miejscowość	data	podpis składającego

Załącznik Nr. 2 do Zarządzenia wewnętrznego Nr 42/2023
Dyrektora Miejskiego Zarządu Budynków Komunalnych
w Kędzierzynie-Koźlu z dnia 11 grudnia 2023 roku.

Procedura tworzenia kopii zapasowych

§ 1.

Procedura tworzenia kopii zapasowych określa zasady tworzenia, przechowywania i testowania kopii zapasowych oraz odzyskiwania z nich danych i systemów informatycznych, w celu zapewnienia integralności i dostępności informacji oraz środków przetwarzania informacji.

§ 2.

Działania opisane w niniejszej procedurze obowiązują, we wszystkich komórkach organizacyjnych MZBK.

§ 3

Wykonywanie kopii systemów informatycznych.

Na potrzeby zachowania ciągłości działania systemów informatycznych i utrzymania integralności danych wykonuje się kopie zapasowe zbiorów danych. Zadanie to realizowane jest codziennie w dni robocze. Kopie awaryjne są wykonywane automatycznie przez dedykowany proces poza godzinami pracy MZBK według ustalonego harmonogramu. Harmonogram zawiera również określenie jakie zasoby i systemy są kopiowane. Tworzone są kompletne kopie zapasowe wybranych zasobów, tzn. kopiowane są wszystkie pliki. Kopie trafiają do urządzenia magazynującego NAS oraz zapisywane są na macierzy dyskowej stacji roboczej. Wyniki tworzenia kopii zapasowych są rejestrowane. Zakres tworzenia kopii zapasowych obejmuje:

1. Bazy danych zlokalizowane na serwerach;
2. Pliki i katalogi na serwerach;
3. Obrazy maszyn wirtualnych.

Kopie zapasowe sporządza się również w następujących przypadkach:

1. przed dokonaniem istotnej zmiany konfiguracyjnej (np. aktualizacji oprogramowania, ustawień systemowych),
2. po przeprowadzeniu zmiany konfiguracyjnej (np. aktualizacji oprogramowania, ustawień systemowych, zmianie praw dostępu).

Kopie zapasowe, wykonane w danym dniu przechowywane są przez okres 2 miesięcy oraz zabezpieczone są przed nieumyślnym skasowaniem i przechowywane w pomieszczeniach innych niż serwerownia. Kopie przechowywane są w metalowym szafie zamykanej na klucz w zamykanym pomieszczeniu. Po ustaniu użyteczności kopii zapasowej jest ona niezwłocznie usuwana.

Kopie zapasowe konfiguracji systemów operacyjnych serwerów wykonuje administrator systemu po każdej zmianie konfiguracji oprogramowania (np. po utworzeniu, rekonfiguracji lub usunięciu konta użytkownika w systemie, zmianie praw dostępu itp.)

Za prawidłowość tworzenia kopii zapasowych odpowiada administrator systemu Informatycznego (ASI).

§ 4

Wykonywanie kopii zapasowych danych roboczych użytkowników sieci komputerowej MZBK przechowywanych na serwerach.

Administrator systemu odpowiada za wykonywanie kopii zapasowych danych roboczych użytkowników (kopie robocze) przechowywanych na serwerach zlokalizowanych w sieci komputerowej MZBK (bazy danych, katalogi użytkowników, katalogi grup).

Kopie danych są wykonywane automatycznie według procedury opisanej w § 3.

Za wykonywanie kopii zapasowych danych znajdujących się na poszczególnych stacjach roboczych poza serwerownią odpowiadają użytkownicy tych stacji roboczych. Częstotliwość tworzenia kopii zapasowych na stacjach roboczych zależy od ilości i wagi przetwarzanych informacji. Niedopuszczalne jest przechowywanie kopii zapasowych na tych samych nośnikach na których są one przetwarzane. Użytkownicy mogą zlecać administratorowi systemu wykonanie kopii przetwarzanych przez nich danych (np. kopii folderów osobistych na stacjach roboczych). Zlecenie należy złożyć w formie elektronicznej za pomocą wiadomości e-mail lub systemu obiegu dokumentów.

§ 5

Testowanie kopii (Zachowanie ciągłości)

Kopie zapasowe sprawdzane są okresowo pod kątem ich dalszej przydatności przez administratora systemu nie rzadziej niż raz na miesiąc. Polega to na testowym odtworzeniu zawartości kopii na innym urządzeniu. Administrator systemu sporządza notatkę po każdym teście. Po stwierdzeniu nieprzydatności kopii zapasowych zbiorów nośnik zostaje pozbawiony danych lub wybrakowany w inny sposób uniemożliwiający dalszy odczyt informacji.

§ 6

Odzyskiwanie danych i systemów informatycznych z kopii zapasowych.
Odzyskiwanie danych z kopii zapasowych jest wykonywane w następujących przypadkach:

1. utraty całości lub części danych na serwerze;
2. utraty integralności całości lub części danych na serwerze;
3. w celu odtworzenia poprzedniej wersji danych na wniosek podpisany przez kierownika komórki organizacyjnej i zatwierdzony przez dyrektora. złożyć w formie elektronicznej za pomocą systemu obiegu dokumentów;
4. na wniosek organu kontrolnego (np.: NIK);
5. przy przenoszeniu danych na nowy serwer.

Odzyskiwanie całego systemu informatycznego jest wykonywane w wypadku awarii sprzętowej lub systemowej nośników danych na których jest on zlokalizowany, uniemożliwiającej korzystanie z danego systemu.

Za odzyskiwanie danych z kopii zapasowych odpowiada ASI.

DYREKTOR
Stanisław Węgrzyn