ZARZĄDZENIE NR VIII/71/2023
BURMISTRZA MIASTA ORZESZE

z dnia 5 maja 2023 r.

w sprawie ustanowienia, wdrożenia, eksploatacji, monitorowania, przeglądu, utrzymania i doskonalenia „Systemu zarządzania bezpieczeństwem informacji" w Urzędzie Miejskim Orzesze

Na podstawie art. 30 ust. 1 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (tekst jednolity Dz. U. z 2023 r. poz. 40, 572) w związku z art. 24, art. 32 ust. 1 i art. 33 ust. 5 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) oraz § 20 ust. 1 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (tekst jednolity Dz. U. z 2017 r. poz. 2247).

zarządzam, co następuje:

§ 1. Ustanawiam „System zarządzania bezpieczeństwem informacji" w Urzędzie Miejskim Orzesze, który stanowi załącznik do zarządzenia.

§ 2. Wykonanie zarządzenia powierzam pracownikom Urzędu.

§ 3. Traci moc zarządzenie nr VII/84/2018 Burmistrza Miasta Orzesze z dnia 7 maja 2018 r. w sprawie wprowadzenia „Polityki ochrony danych osobowych" w Urzędzie Miejskim Orzesze.

§ 4. Upoważnienia i dostępy do systemów informatycznych nadane przed dniem wejścia w życie zarządzenia pozostają w mocy.

§ 5. Zarządzenie wchodzi w życie z dniem podpisania.

Burmistrz Miasta Orzesze

inż. Mirosław Blaski

Załącznik do zarządzenia nr VIII/71/2023 – „System zarządzania bezpieczeństwem informacji”

SYSTEM ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI

§ 1.

1. Informacje to aktywa, które, podobnie jak inne aktywa, są niezbędne dla prawidłowego funkcjonowania Urzędu Miejskiego Orzesze, zwanego w dalszej części Urzędem, i z tego powodu podlegają ochronie.
2. Informacja przybiera różne formy – może być wydrukowana lub zapisana na papierze, przechowywana elektronicznie, przesyłana pocztą i za pomocą nośników elektronicznych lub wypowiadana w rozmowie.
3. Bezpieczeństwo informacji oznacza ochronę informacji przed zagrożeniami w celu zapewnienia ciągłości działania, efektywnego wykorzystania informacji i minimalizacji ryzyka.

§ 2.

1. Celem „Systemu zarządzania bezpieczeństwem informacji” jest zapewnienie poufności, dostępności i integralności informacji, niezaprzeczalności odbioru i nadania informacji oraz rozliczalności działań.
2. Zapewnienie poufności oznacza zabezpieczenie informacji przed dostępem nieuprawnionych osób, podmiotów lub procesów.
3. Zapewnienie dostępności oznacza możliwość wykorzystania informacji w dowolnym momencie przez uprawnioną osobę.
4. Zapewnienie integralności oznacza zabezpieczenie informacji przed nieuprawnioną modyfikacją.
5. Niezaprzeczalność odbioru oznacza zdolność systemu informatycznego do udowodnienia, że adresat informacji otrzymał ją w określonym miejscu i czasie.
6. Niezaprzeczalność nadania oznacza zdolność systemu informatycznego do udowodnienia, że nadawca informacji faktycznie ją nadał lub wprowadził do systemu informatycznego w określonym miejscu i czasie.
7. Rozliczalność działań oznacza zapewnienie, że wszystkie działania istotne dla przetwarzania informacji zostały zarejestrowane w systemie informatycznym i możliwym jest zidentyfikowanie użytkownika, który działania wykonał.

§ 3.

1. „System zarządzania bezpieczeństwem informacji” został zaprojektowany tak, aby zapewnić adekwatne i proporcjonalne zabezpieczenia, które odpowiednio chronią informacje, oraz uzyskać zaufanie zainteresowanych stron.
2. „System zarządzania bezpieczeństwem informacji” opiera się na modelu planuj – wykonuj – sprawdzaj – działaj (PDCA).
3. „System zarządzania bezpieczeństwem informacji” jest poddawany przeglądowi i uaktualniany.
4. „System zarządzania bezpieczeństwem informacji” stosuje każdy pracownik przetwarzający informacje. Przez przetwarzanie informacji należy rozumieć operację lub zestaw operacji wykonywanych na informacji, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie. Przez pracownika należy rozumieć osobę

zatrudnioną w Urzędzie przez powołanie, na podstawie umowy o pracę, umowy zlecenie lub umowy o dzieło.

§ 4.

Zarządzanie bezpieczeństwem informacji jest realizowane poprzez zapewnienie przez Burmistrza warunków umożliwiających wykonanie i egzekwowanie następujących działań:

1) zapewnienia aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia,
2) utrzymywania aktualności inwentaryzacji środków przetwarzania informacji obejmującej ich rodzaj i konfigurację,
3) przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy,
4) podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji, a w razie konieczności bezzwłocznej zmiany tych uprawnień,
5) zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak:
   a) zagrożenia bezpieczeństwa informacji,
   b) skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna,
   c) stosowanie środków zapewniających bezpieczeństwo informacji, w tym minimalizujących ryzyko błędów ludzkich,
6) zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez:
   a) monitorowanie dostępu do informacji,
   b) czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji,
   c) zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji,
7) ustanowienia podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość,
8) zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikację, usunięcie lub zniszczenie,
9) zawierania w umowach serwisowych podpisanych z wykonawcami zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji,
10) ustalenia zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych,
11) zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach informatycznych, polegającego w szczególności na:
   a) dbałości o aktualizację oprogramowania,
   b) minimalizowaniu ryzyka utraty informacji w wyniku awarii,
   c) ochronie przed błędami, utratą, nieuprawnioną modyfikacją,
   d) stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisów prawa,
   e) zapewnieniu bezpieczeństwa plików systemowych,
   f) redukcji ryzyka wynikającego z wykorzystania opublikowanych podatności technicznych systemów informatycznych,

g) niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów informatycznych na możliwość naruszenia bezpieczeństwa,
h) kontroli zgodności systemów informatycznych z odpowiednimi normami i politykami bezpieczeństwa,

12) bezzwłocznego zgłaszania incydentów związanych z bezpieczeństwem informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących,
13) zapewnienia okresowego audytu w zakresie bezpieczeństwa informacji, nie rzadziej niż raz w roku.

§ 5.

1. W Urzędzie wyodrębnia się pięć grup informacji:
   1) informacje niejawne,
   2) tajemnice ustawowo chronione,
   3) dane osobowe,
   4) informacje o charakterze wewnętrznym (np. organizacyjnym, porządkowym),
   5) pozostałe informacje.
2. Poziom ochrony informacji szacuje się poprzez analizę atrybutów poufności, integralności i dostępności dla rozważanej grupy informacji i przyjmuje się, że:
   1) informacje niejawne, tajemnice ustawowo chronione, dane osobowe i informacje o charakterze wewnętrznym są informacjami poufnymi, chronionymi przed dostępem nieuprawnionych osób, dostępnymi w sposób nieprzerwany, chronionymi przed nieuprawnioną modyfikacją,
   2) pozostałe informacje są informacjami ogólnodostępnymi lub dostępnymi na wniosek, w sposób nieprzerwany, chronionymi przed nieuprawnioną modyfikacją.
3. Informacje niejawne przetwarzane i chronione są na podstawie odrębnych przepisów.
4. W przypadku, gdy dane osobowe przetwarzane są na podstawie zgody osoby, której dane dotyczą, za uzyskanie zgody odpowiada pracownik, który jako pierwszy przetwarzać będzie te dane.

§ 6.

1. Dostęp do informacji realizowany jest zgodnie z:
   1) zasadą wiedzy uzasadnionej – dostęp do informacji uzasadniony jest potrzebami wynikającymi z pełnionych obowiązków służbowych i wynika wprost z zakresu czynności lub innego dokumentu uzasadniającego dostęp do informacji,
   2) zasadą minimalnych uprawnień – zakres dostępu do informacji nie może wykraczać poza potrzeby wynikające z pełnionych obowiązków służbowych i powinien być najmniejszym zbiorem praw dostępu pozwalającym na efektywne pełnienie obowiązków służbowych.
2. Pracownik mający dostęp do informacji podpisuje oświadczenie o zachowaniu poufności.
3. Oświadczenie o zachowaniu poufności podpisuje także osoba współpracująca z Urzędem, jeśli w ramach współpracy uzyskuje dostęp do informacji Urzędu, chyba że obowiązuje ją ustawowy obowiązek zachowania tajemnicy.
4. Oświadczenie o zachowaniu poufności sporządzane jest na piśmie, w dwóch jednobrzmiących egzemplarzach: jeden przeznaczony jest dla osoby, która podpisuje oświadczenie o zachowaniu poufności, drugi – dla Urzędu. Oświadczenie o zachowaniu poufności pracownika Urzędu przechowywane jest w aktach osobowych pracownika, a osoby spoza Urzędu – wraz z dokumentem uzasadniającym dostęp do informacji (np. z umową).

5. Wzór oświadczenia o zachowaniu poufności stanowi załącznik nr 1 do „Systemu zarządzania bezpieczeństwem informacji”.
6. Dostęp do informacji przetwarzanych elektronicznie z wykorzystaniem systemów informatycznych Urzędu realizowany jest na podstawie pisemnego wniosku o przyznanie dostępu do systemów informatycznych.
7. Wniosek o przyznanie dostępu do systemu informatycznego przygotowuje bezpośredni przełożony pracownika, a dostępu udziela Referat Informatyki i Bezpieczeństwa Informacji. Wykaz zasobów danych pomocnych do przygotowania wniosku o przyznanie dostępu do systemu informatycznego, dostępny jest w udziałach sieciowych Referatu Informatyki i Bezpieczeństwa Informacji.
8. Wniosek o przyznanie dostępu do systemu informatycznego sporządzany jest w jednym egzemplarzu i przechowywany w Referacie Informatyki i Bezpieczeństwa Informacji.
9. Wzór wniosku o przyznanie dostępu do systemu informatycznego stanowi załącznik nr 2 do „Systemu zarządzania bezpieczeństwem informacji”.
10. Dostęp do danych osobowych może zostać dodatkowo potwierdzony pisemnym upoważnieniem do przetwarzania danych osobowych.
11. Upoważnienie do przetwarzania danych osobowych i odwołanie upoważnienia do przetwarzania danych osobowych przygotowuje Sekretarz Miasta lub Kierownik Biura rady, a podpisuje Burmistrz.
12. Upoważnienie do przetwarzania danych osobowych i odwołanie upoważnienia do przetwarzania danych osobowych sporządzane są w dwóch jednobrzmiących egzemplarzach: jeden przeznaczony jest dla osoby, której nadano lub odebrano upoważnienie do przetwarzania danych osobowych, drugi – dla Urzędu. Upoważnienie do przetwarzania danych osobowych i odwołanie upoważnienia do przetwarzania danych osobowych przechowywane są przez Sekretarza Miasta.
13. Wzory upoważnienia do przetwarzania danych osobowych i odwołania upoważnienia do przetwarzania danych osobowych stanowią załącznik nr 3 do „Systemu zarządzania bezpieczeństwem informacji”. Dopuszcza się stosowanie innych wzorów upoważnienia do przetwarzania danych osobowych i odwołania upoważnienia do przetwarzania danych osobowych, w szczególności, jeśli wzory takie wynikają z obowiązujących Urząd umów.

§ 7.

1. Pracownicy, którzy przetwarzają informacje, przechodzą obowiązkowe szkolenie z zakresu bezpieczeństwa informacji.
2. Tematyka szkolenia obejmuje w szczególności:
   1) aktualny system prawny bezpieczeństwa informacji w Polsce,
   2) wewnętrzne regulacje związane z bezpieczeństwem informacji w Urzędzie,
   3) zagrożenia dla bezpieczeństwa informacji w odniesieniu do specyfiki działalności Urzędu,
   4) role i zadania poszczególnych osób odpowiedzialnych za bezpieczeństwo informacji,
   5) zasady udzielania dostępu do informacji,
   6) zasady przetwarzania informacji w systemach informatycznych,
   7) procedury postępowania w sytuacji naruszenia bezpieczeństwa informacji,
   8) odpowiedzialność dyscyplinarna, finansowa i karna za nieprzestrzeganie zasad bezpieczeństwa informacji.
3. Szkolenie, w zależności od potrzeb i możliwości, może zostać przeprowadzone w formie tradycyjnego wykładu, udostępnienia materiałów szkoleniowych, wideokonferencji, kursu e-learningowego itp.
4. Szkolenie przeprowadza inspektor ochrony danych, a w przypadku nieobecności inspektora ochrony danych – podmiot zewnętrzny.

§ 8.

1. Budynki Urzędu przy ul. Św. Wawrzyńca 21 i 23 w Orzeszu zabezpieczone są systemem alarmowym.
2. Budynek Urzędu przy ul. Św. Wawrzyńca 21 w Orzeszu i teren wokół budynku zabezpieczone są dodatkowo monitoringiem wizyjnym.
3. Monitoring wizyjny obejmuje otoczenie budynku, a wewnątrz – ciągi komunikacyjne i pomieszczenie nr 21. Nagrania obrazu są przechowywane przez okres 14 dni od dnia nagrania.
4. W przypadku, w którym nagrania obrazu stanowią dowód w postępowaniu prowadzonym na podstawie prawa lub Burmistrz powziął wiadomość, iż mogą one stanowić dowód w postępowaniu, termin określony w ust. 2 ulega przedłużeniu do czasu prawomocnego zakończenia postępowania.
5. Wejścia do budynków Urzędu przy ul. Św. Wawrzyńca 21 i 23 w Orzeszu zabezpieczone są zamkami drzwiowymi, a wejście tylne do budynku Urzędu przy ul. Św. Wawrzyńca 21 – dodatkowo PIN-em.
6. Klucze do budynków Urzędu posiadają wyznaczeni pracownicy.
7. Otwarcia budynków Urzędu po porze nocnej dokonują wyznaczeni pracownicy, nie wcześniej niż na 60 minut przed godziną rozpoczęcia pracy Urzędu.
8. Pomieszczenia w budynkach Urzędu zabezpieczone są zamkami drzwiowymi, a pomieszczenie nr 20 – dodatkowo PIN-em.
9. Wyznaczeni pracownicy wydają pracownikom klucze do pomieszczeń.
10. Wyznaczony pracownik, po wydaniu kluczy, koduje kodem mechanicznym gablotę, w której przechowywane są klucze.
11. Po zakończonej pracy klucze zdawane są osobie sprzątającej.
12. Zamknięcia budynków Urzędu dokonują wyznaczeni pracownicy.
13. Klucze wydawane i zdawane są za potwierdzeniem w książce ewidencji kluczy.
14. Klucze zapasowe do budynków Urzędu znajdują się w zabezpieczonej kodem mechanicznym gablocie w pomieszczeniu nr 10 w budynku Urzędu przy ul. Św. Wawrzyńca 21 oraz w kasecie zdeponowanej na komisariacie policji przy ul. Matejki 1 w Orzeszu. Wykaz osób uprawnionych do pobrania kluczy zapasowych zdeponowanych na komisariacie policji stanowi załącznik nr 4 do „Systemu zarządzania bezpieczeństwem informacji”.
15. Klucze zapasowe do pomieszczeń w budynkach Urzędu znajdują się w zabezpieczonej kodem mechanicznym gablocie w pomieszczeniu nr 10 w budynku Urzędu przy ul. Św. Wawrzyńca 21.

§ 9.

1. Pracownik, który pobrał klucze do pomieszczenia, przed uruchomieniem zamków, sprawdza od strony wizualnej stan tych zamków i – jeśli są stosowane – dodatkowych zabezpieczeń, w tym plomb.
2. Po otwarciu pomieszczenia, pracownik, przed przystąpieniem do pracy, sprawdza stan zastosowanych zabezpieczeń sprzętu biurowego i komputerowego, przechowywanej dokumentacji i innego wyposażenia. W przypadku stwierdzenia zmian lub naruszenia stanu zabezpieczeń, pracownik zawiadamia bezpośredniego przełożonego.
3. Pomieszczenia pozostają zamknięte podczas nieobecności pracownika.
4. Okna w pomieszczeniach pozostają zamknięte podczas nieobecności pracownika, z zastrzeżeniem wymogów sanitarno-higienicznych.

§ 10.

1. Pracując z dokumentami zawierającymi tajemnice ustawowo chronione lub dane osobowe stosuje się zasadę czystego biurka – niewykorzystywane w danej chwili dokumenty przechowuje się pod zamknięciem, szczególnie jeśli pomieszczenie jest opuszczane, a w przypadku obsługi osoby nieuprawnionej – poza zasięgiem jej wzroku.
2. Dokumenty zawierające tajemnice ustawowo chronione lub dane osobowe po ustaniu ich przydatności do bieżącego przetwarzania oraz braku obowiązku prawnego ich dalszego archiwizowania, niszczy się w przeznaczonych do tego urządzeniach. Zabronione jest wyrzucanie do kosza na śmieci jakichkolwiek dokumentów zawierających tajemnice ustawowo chronione lub dane osobowe, bez względu na ich zawartość informacyjną czy upływ czasu od ich wytworzenia.
3. Nie należy umieszczać w gablotach oraz na tablicach korkowych i magnetycznych tajemnic ustawowo chronionych lub danych osobowych, chyba że obowiązek taki wynika z przepisów prawa.
4. Nie należy pozostawiać osoby nieuprawnionej w pomieszczeniu bez nadzoru, także wtedy, kiedy stanowisko komputerowe jest wyłączone lub wylogowane, a dokumenty zawierające tajemnice ustawowo chronione lub dane osobowe umieszczone w zamkniętej szafie.

§ 11.

1. Prowadząc rozmowę telefoniczną należy potwierdzić tożsamość osoby dzwoniącej jako osoby uprawnionej do otrzymania informacji poprzez pytania kontrolne, mające na celu uprawdopodobnienie, że jest osobą uprawnioną do otrzymania informacji.
2. Potwierdzenie tożsamości osoby dzwoniącej odbywa się z uwzględnieniem doświadczenia zawodowego i zdrowego rozsądku.
3. Potwierdzając tożsamość osoby dzwoniącej nie należy dokonywać nadmiernego pozyskiwania danych osobowych.
4. Prowadząc rozmowę telefoniczną, w trakcie której przekazywane są tajemnice ustawowo chronione lub dane osobowe, należy zwracać uwagę na możliwość podsłuchania rozmowy telefonicznej przez osoby nieuprawnione znajdujące się w bezpośrednim sąsiedztwie.
5. Nie wolno pozostawiać w automatycznych sekretarkach wiadomości zawierających tajemnice ustawowo chronione lub dane osobowe.

§ 12.

Korzystając z drukarki, kopiarki lub faksu należy być świadomym, że urządzenia te wyposażone są w podręczną pamięć, w której przechowywane są strony na wypadek błędów transmisji lub braku papieru, a drukują zaraz po usunięciu błędu – należy niezwłocznie usuwać dokumenty zawierające tajemnice ustawowo chronione lub dane osobowe.

§ 13.

1. Środki uwierzytelniania dostępu do pracy na komputerze i z wykorzystaniem oprogramowania służącego do przetwarzania informacji to identyfikator użytkownika i hasło dostępu. Zamiast hasła dostępu dopuszczalne jest stosowanie kart chipowych, PIN-ów.
2. Identyfikator użytkownika jest w sposób jednoznaczny przypisany danemu użytkownikowi. Ewidencję identyfikatorów użytkownika prowadzi Referat Informatyki i Bezpieczeństwa Informacji.
3. Użytkownik jest odpowiedzialny za wszystkie czynności wykonane przy użyciu identyfikatora użytkownika, którym się posługuje.
4. Przydzielanie użytkownikowi uprawnień do kasowania lub dezaktywacji rejestrów zdarzeń zawierających zapisy o jego własnych działaniach jest zabronione.

5. Identyfikator użytkownika po wyrejestrowaniu użytkownika z komputera i oprogramowania służącego do przetwarzania informacji nie może być przydzielony innemu użytkownikowi.
6. Identyfikator użytkownika, który utracił prawo dostępu do pracy na komputerze i z wykorzystaniem oprogramowania służącego do przetwarzania informacji, jest blokowany przez Referat Informatyki i Bezpieczeństwa Informacji na podstawie otrzymanej karty obiegowej.
7. Referat Informatyki i Bezpieczeństwa Informacji rejestruje użytkownika w komputerze i w oprogramowaniu służącym do przetwarzania informacji poprzez utworzenie identyfikatora użytkownika i nadaje jednorazowe hasło dostępu, które zostaje zmienione przy pierwszym logowaniu użytkownika. Zmianę hasła dostępu powinien wymuszać, jeżeli to technicznie możliwe, system operacyjny lub oprogramowanie służące do przetwarzania informacji.
8. Jednorazowe hasło dostępu nie może być przekazywane użytkownikowi za pośrednictwem osób trzecich.
9. Przed rozpoczęciem pracy na komputerze użytkownik sprawdza, czy nie ma oznak fizycznego naruszenia zabezpieczeń.
10. Po uruchomieniu komputera użytkownik powinien się zalogować – wprowadzić przydzielony identyfikator użytkownika i hasło dostępu.
11. Jeżeli w trakcie logowania wystąpi błąd, system nie powinien wskazywać, która część danych jest poprawna lub niepoprawna.
12. W trakcie logowania się do komputera lub oprogramowania służącego do przetwarzania informacji użytkownik nie powinien odchodzić od komputera.
13. Po poprawnym zalogowaniu się, użytkownik rozpoczyna pracę na komputerze lub z wykorzystaniem oprogramowania służącego do przetwarzania informacji.
14. W trakcie pracy ekran monitora komputera jest zasłonięty nakładką maskującą lub ustawiony w sposób uniemożliwiający osobie nieuprawnionej wgląd lub spisanie informacji wyświetlanych na ekranie monitora, a w przypadku korzystania z funkcji udostępniania ekranu lub podobnej – spisanie, odczytanie, sfotografowanie, skopiowanie, wydrukowanie itp. informacji.
15. W trakcie pracy użytkownik dba o prawidłową wentylację komputerów, w szczególności nie zasłania kratek wentylatorów meblami, zasłonami, nie stawia komputera tuż przy ścianie.
16. Do listew podtrzymujących napięcie nie wolno podłączać grzejników, czajników, wentylatorów itp.
17. Przy każdorazowym opuszczeniu pomieszczenia biurowego, użytkownik powinien zablokować komputer lub wylogować się. Przez pomieszczenie biurowe rozumie się pomieszczenia indywidualne lub wnętrza grupowe. W przypadku, gdy dwa pomieszczenia indywidualne lub grupowe połączone są drzwiami należy je traktować jak jedno pomieszczenie biurowe.
18. Blokada komputera następuje po naciśnięciu skrótu klawiszowego Windows + L lub klawiszy Ctrl + Alt + Delete i wybranie opcji „Zablokuj komputer”.
19. Zmianę użytkownika komputera każdorazowo powinno poprzedzać wylogowanie się poprzedniego użytkownika.
20. Przed zakończeniem pracy na komputerze użytkownik powinien zapisać wszystkie zmiany, następnie wylogować się z uruchomionego oprogramowania, wyłączyć komputer i odciąć napięcie listwy podtrzymującej napięcie.
21. Obowiązują następujące zasady tworzenia hasła dostępu:

1) hasło dostępu nie powinno składać się z żadnych danych personalnych (imienia, nazwiska, adresu zamieszkania użytkownika lub najbliższych osób) lub ich fragmentów ani być oparte na prostych skojarzeniach (numer telefonu, data urodzenia itp.),
2) hasło dostępu powinno składać się z co najmniej 10 znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne,
3) hasło dostępu nie powinno składać się z identycznych znaków lub ciągu znaków z klawiatury,
4) hasło dostępu nie powinno być jednakowe z identyfikatorem użytkownika,
5) hasło dostępu powinno być unikalne, tj. takie, które nie było poprzednio stosowane przez użytkownika,
6) hasło dostępu nie powinno być podatne na atak słownikowy, tj. nie powinno zawierać słów zamieszczonych w słownikach.

22. Hasło dostępu w trakcie wpisywania nie powinno być wyświetlane na ekranie.
23. Hasło dostępu powinno być utrzymywane w tajemnicy, również po utracie jego ważności.
24. Hasło dostępu nie powinno być przechowywane w systemach informatycznych w niechronionej postaci.
25. Hasło dostępu nie powinno być nigdzie zapisywane.
26. Hasło dostępu nie powinno być wprowadzone do jakichkolwiek zautomatyzowanych procesów logowania się do komputera i do oprogramowania służącego do przetwarzania informacji.
27. Hasło dostępu nie powinno być przechowywane w makrach ani przypisane do klawiszy funkcyjnych.
28. Zaleca się zmianę hasła dostępu nie rzadziej niż co 30 dni.
29. Hasło dostępu jest zmieniane przez użytkownika.

§ 14.

1. Informacje i oprogramowanie służące do przetwarzania informacji zabezpiecza się poprzez wykonywanie kopii zapasowych.
2. Kopie zapasowe bazy danych systemów informatycznych REKORD i SOD SEKAP-FINN oraz zawartości udziałów sieciowych wykonywane są automatycznie codziennie w nocy i przechowywane są na serwerze NAS oraz na macierzach dyskowych serwerów.
3. Dodatkowe kopie zapasowe przechowywane są budynku Urzędu przy ul. Św. Wawrzyńca 23 w Orzeszu na dysku zewnętrznym.

§ 15.

1. Tajemnice ustawowo chronione i dane osobowe przetwarzane są na nośnikach (telefon komórkowy, pendrive, dysk, pamięć typu flash, zewnętrzny dysk twardy, płyta CD lub DVD itp.) wyłącznie, gdy istnieje konieczność przeniesienia tajemnic ustawowo chronionych lub danych osobowych w postaci elektronicznej, a wykorzystanie do tego celu sieci Internet jest nieuzasadnione, niemożliwe lub zbyt niebezpieczne.
2. Przetwarzanie tajemnic ustawowo chronionych lub danych osobowych na nośnikach, które nie podlegają kryptograficznej ochronie jest zabronione.
3. Korzystanie z nośników, z wyjątkiem telefonów komórkowych, możliwe jest wyłącznie w stacjach roboczych pracowników kierujących komórkami organizacyjnymi Urzędu i pracowników zajmujących samodzielne stanowiska pracy.
4. Nośniki użyte do przetwarzania tajemnic ustawowo chronionych lub danych osobowych mogą być wykorzystywane do innych celów wyłącznie po skasowaniu danych osobowych lub nadpisaniu za pomocą technik uniemożliwiających ich odtworzenie.
5. Tajemnice ustawowo chronione lub dane osobowe zapisane na nośnikach, które mają być dostępne przez czas dłuższy niż czas życia nośników (zgodnie z danymi producenta),

przechowuje się w innym miejscu i w taki sposób, aby uniknąć utraty danych osobowych na skutek pogorszenia się jakości nośników lub utraty właściwości nośników.
6. Nośniki przechowuje się w zamkniętych szafach lub szufladach w sposób zabezpieczający nośnik przed nieuprawnionym przejęciem i zniszczeniem.
7. Nośniki przechowuje się zgodnie z zaleceniami producenta.
8. W trakcie transportu nośniki chroni się przed fizycznym uszkodzeniem, wpływem temperatury, wilgotności, pola elektromagnetycznego, które mogą pogorszyć skuteczność odtworzenia informacji z nośników, w szczególności poprzez opakowanie zgodne z zaleceniami producenta.
9. W trakcie przekazywania nośników stosuje się zasadę dostarczania do rąk własnych odbiorcy osobiście, pocztą tradycyjną, kurierską itp.
10. W przypadku przekazania nośników do ponownego użycia, kasuje się zapisane na nośnikach tajemnice ustawowo chronione, dane osobowe i licencjonowane oprogramowanie służące do przetwarzania informacji, do których przyszły użytkownik nie ma dostępu, a w przypadku zbycia lub zniszczenia – wszystkie tajemnice ustawowo chronione, dane osobowe i licencjonowane oprogramowanie służące do przetwarzania informacji kasuje się lub nadpisuje się za pomocą technik uniemożliwiających ich odtworzenie.
11. Nośniki likwiduje się poprzez spopielenie, pocięcie lub uszkodzenie w taki sposób, aby nie było możliwe ponowne wykorzystanie nośników.
12. W przypadku niszczenia dokumentów tradycyjnych odpowiadające im zapisy na nośnikach usuwa się lub zabezpiecza się przed ich odczytaniem, o ile jest to zasadne.

§ 16.

Korzystając z Internetu zabrania się:
1) prowadzić ataki, włamania i inne działania związane z ingerencją w dane komputerów innych użytkowników oraz komputerów lub urządzeń mobilnych w Internecie, a także świadomego lub nieświadomego prowadzenia innych działań destrukcyjnych,
2) utrudniać lub uniemożliwiać innym użytkownikom korzystanie z Internetu poprzez uruchamianie oprogramowania nadmiernie obciążającego transfer,
3) wprowadzać jakichkolwiek nieuzgodnionych z Referatem Informatyki i Bezpieczeństwa Informacji zmian we właściwościach połączeń sieciowych komputera, w szczególności adresu IP, MAC oraz nie rozpowszechniać tych ustawień konfiguracyjnych osobom trzecim,
4) przeglądać strony WWW potencjalnie niebezpiecznych w szczególności zawierających pornografię, hazard lub crack,
5) wykorzystywać Internetu do prowadzenia działalności niezgodnej z przepisami prawa, w szczególności do rozsyłania niechcianej poczty elektronicznej (spam) oraz wymiany plików w sieciach typu P2P,
6) uruchamiać oprogramowania umożliwiającego przejmowanie zdalnej kontroli nad komputerem lub urządzeniem przenośnym będącym własnością Urzędu, z zastrzeżeniem § 17 ust. 3.

§ 17.

1. Przy przetwarzaniu informacji poza budynkami Urzędu z wykorzystaniem urządzeń przenośnych, w tym laptopów, telefonów komórkowych itp.:
   1) stosuje się środki uwierzytelniania określone w § 13, o ile jest to technicznie możliwe,
   2) nie korzysta się z otwartych sieci internetowych Wi-Fi, tzw. hot spot,
   3) unika ryzyka podglądania ze strony nieuprawnionych osób,

4) nie pozostawia się zalogowanego urządzenia przenośnego bez nadzoru, w tym nie dopuszcza się do korzystania z zalogowanego urządzenia przenośnego przez nieuprawnione osoby,
5) stosuje się oprogramowanie antywirusowe określone w § 20,
6) przewozi się urządzenia przenośne zgodnie z zaleceniami producenta i jako bagaż podręczny,
7) stosuje się zalecenia producenta dotyczące ochrony urządzenia przenośnego, w tym ochrony przed wystawieniem na silne pola elektromagnetyczne, wpływem temperatury, wilgotności,
8) tworzy się kopie zapasowe na zasadach określonych w § 14, o ile jest to technicznie możliwe,
9) zbędne lub niepotrzebne informacje kasuje się.

2. Urządzenia przenośne podlegają prewencji programowej i technicznej. O przeprowadzeniu prewencji programowej i technicznej urządzeń przenośnych decyduje Referat Informatyki i Bezpieczeństwa Informacji.
3. Wszelkie czynności związane z instalacją oprogramowania i konfiguracją urządzeń przenośnych wykonuje Referat Informatyki i Bezpieczeństwa Informacji, w tym zdalnie z wykorzystaniem oprogramowania do zdalnego zarządzania lub serwis zewnętrzny.
4. Zabrania się przetwarzania tajemnic ustawowo chronionych lub danych osobowych z wykorzystaniem urządzeń przenośnych, w tym laptopów, telefonów komórkowych itp., które nie są własnością Urzędu.

§ 18.

Prowadzenie służbowych spotkań zdalnych realizowane jest w sposób zapewniający poufność informacji.

§ 19.

1. W przypadku konieczności wymiany tajemnic ustawowo chronionych lub danych osobowych w postaci elektronicznej (poczta elektroniczna), zalecane jest, jeśli jest to organizacyjnie i technicznie możliwe, korzystanie wyłącznie z formy załączników z uwzględnieniem poniższych zasad:
   1) przetwarzane załączniki zawierające tajemnice ustawowo chronione lub dane osobowe podlegają zabezpieczeniu kryptograficznemu z użyciem algorytmu AES256 lub silniejszego, uzgodnionego pomiędzy nadawcą i odbiorcą (np. oprogramowanie archiwizujące z wbudowanym algorytmem szyfrującym),
   2) hasło zabezpieczające (klucz szyfrujący), zapewniające ochronę przed nieuprawnionym odszyfrowaniem załącznika, składa się z co najmniej 10 znaków,
   3) nadawca, po uzyskaniu od odbiorcy potwierdzenia otrzymania zabezpieczonych załączników, przekazuje odbiorcy hasło zabezpieczające (klucz szyfrujący) poprzez przesłanie go innym kanałem niż poczta elektroniczna, w szczególności w drodze połączenia telefonicznego, z zachowaniem zasad i środków zabezpieczających przed ujawnieniem hasła podmiotom nieuprawnionym.
2. Przesyłając pocztą elektroniczną wiadomości zawierające tajemnice ustawowo chronione lub dane osobowe należy dodatkowo zwracać szczególną uwagę na poprawność adresu poczty elektronicznej adresata.
3. Odbierając wiadomości przesłane pocztą elektroniczną zabrania się uruchamiania wykonywalnych załączników (inaczej uruchamialnych; z rozszerzeniem .com i .exe lub z ustawionym atrybutem wykonywalności oznaczonym literą x) dołączonych do wiadomości.

4. W trakcie wysyłania wiadomości pocztą elektroniczną do kilku osób spoza Urzędu nie ujawnia się poszczególnych prywatnych adresów mailowych – adresując korespondencję należy korzystać z opcji UDW (lub BCC). W takim przypadku zabrania się korzystania z opcji DO (lub TO) oraz DW (lub CC).

§ 20.

1. Niedopuszczalne jest przetwarzanie informacji w postaci elektronicznej bez stosowania profilaktyki i ochrony przed złośliwym oprogramowaniem, chyba że jest to technicznie niemożliwe.
2. Profilaktyka i ochrona przed złośliwym oprogramowaniem obejmuje w szczególności:
   1) instalację, stosowanie i regularne uaktualnienia oprogramowania antywirusowego (wykrywającego i naprawczego),
   2) uświadamianie pracowników w zakresie bezpieczeństwa informacji, właściwych mechanizmach kontroli dostępu oraz zarządzania zmianami,
   3) stałe monitorowanie komunikatów pochodzących z zainstalowanego oprogramowania antywirusowego,
   4) zakaz korzystania z nieautoryzowanego przez Referat Informatyki i Bezpieczeństwa Informacji oprogramowania,
   5) zakaz korzystania z nielegalnego oprogramowania,
   6) zakaz korzystania z sieci Internet bez aktywnej ochrony oprogramowaniem antywirusowym,
   7) sprawdzanie (skanowanie) oprogramowaniem antywirusowym komputerów i elektronicznych nośników informacji, w tym tych otrzymywanych spoza Urzędu oraz wiadomości elektronicznych,
   8) korzystanie z list dyskusyjnych i sprawdzanie stron internetowych zamieszczających informacje o złośliwym oprogramowaniu,
   9) tworzenie kopii zapasowych.
3. Oprogramowanie antywirusowe, o którym mowa w § 20 ust. 2 pkt 1), ma zdolność:
   1) wykrycia i zablokowania każdego rodzaju szkodliwego ataku,
   2) integracji z systemem operacyjnym i kluczowym oprogramowaniem,
   3) ciągłego nadzoru „w tle” nad pracą systemu informatycznego,
   4) kontroli przepływu danych do i z sieci Internet,
   5) kontroli i blokowania niechcianej poczty elektronicznej,
   6) blokowania dostępu do określonych stron i aplikacji internetowych,
   7) analizy nośników,
   8) rejestracji udanych i nieudanych prób dostępu do systemu informatycznego przy wykorzystaniu sieci Internet,
   9) automatycznej aktualizacji wzorców złośliwego oprogramowania.
4. Szczególną uwagę zwraca się na ochronę przed wprowadzeniem złośliwego oprogramowania w trakcie konserwacji lub wykonywania procedur awaryjnych, kiedy możliwe jest obejście normalnych mechanizmów ochrony przed złośliwym oprogramowaniem.

§ 21.

Użytkownik powinien usuwać informacje permanentnie – także z folderu pn. kosz, pobrane, wymiana itp. lub od razu używać skrótu klawiszowego Shift + Delete.

§ 22.

1. Referat Informatyki i Bezpieczeństwa Informacji utrzymuje aktualność inwentaryzacji środków przetwarzania informacji z wykorzystaniem oprogramowania MagikINFO.

2. Przez środki przetwarzania rozumie się komputery stacjonarne i przenośne, drukarki, kopiarki, skanery, serwery, faksy, oprogramowanie oraz inne urządzenia służące do przetwarzania informacji.

§ 23.

Referat Informatyki i Bezpieczeństwa Informacji okresowo przegląda rejestry zdarzeń (logi) w celu wykrycia ewentualnych nadużyć. Przegląd należy udokumentować.

§ 24.

Referat Informatyki i Bezpieczeństwa Informacji regularnie śledzi i analizuje opublikowane podatności techniczne wykorzystywanego w Urzędzie oprogramowania.

§ 25.

Sieć lokalna Urzędu zabezpieczona jest centralną zaporą sieciową.

§ 26.

Stosowane materiały eksploatacyjne powinny odpowiadać normom określonym przez producenta. Zabronione jest stosowanie materiałów eksploatacyjnych niewiadomego pochodzenia.

§ 27.

Klucze kryptograficzne oraz programy związane z zaszyfrowanymi archiwami lub podpisami cyfrowymi przechowuje się w taki sposób, aby informacje można było odszyfrować w ciągu całego okresu przechowywania zapisów.

§ 28.

Wykorzystywane w Urzędzie oprogramowanie dziedzinowe pracuje w trybie automatycznych aktualizacji.

§ 29.

Referat Informatyki i Bezpieczeństwa Informacji zapewnia synchronizację zegarów stacji roboczych z serwerem.

§ 30.

Referat Informatyki i Bezpieczeństwa Informacji okresowo, nie rzadziej niż raz w roku testuje awaryjne zasilanie w energię elektryczną. Testowania należy udokumentować.

§ 31.

Dostęp do plików systemowych i dokumentacji systemowej posiada Burmistrz i Referat Informatyki i Bezpieczeństwa Informacji.

§ 32.

Okablowanie sieciowe zabezpieczone jest hasłem dostępu.

§ 33.

1. Hasło administratora jest to hasło, które umożliwia dostęp do konta użytkownika (administratora) o bardzo wysokich uprawnieniach i pozwala na wykonanie każdego działania w systemie informatycznym, w tym nadawania i zabierania uprawnień innym użytkownikom systemu informatycznego.
2. Z hasła administratora korzysta Referat Informatyki i Bezpieczeństwa Informacji.

3. Hasło administratora generuje Referat Informatyki i Bezpieczeństwa Informacji, chyba, że zostało nadane przez producenta środka przetwarzania informacji i z przyczyn technicznych wygenerowanie hasła administratora nie jest możliwe.
4. Hasło administratora przechowywane jest z wykorzystaniem oprogramowania KeePass Password Safe.
5. Dostęp do oprogramowania KeePass Password Safe posiadają Burmistrz, Zastępca Burmistrza, Sekretarz Miasta i Referat Informatyki i Bezpieczeństwa Informacji.

§ 34.

1. Pracownik w sytuacji dowiedzenia się o potencjalnym naruszeniu bezpieczeństwa informacji bezzwłocznie, najpóźniej w ciągu jednej godziny, zgłasza ten fakt Burmistrzowi, w szczególności podając wszystkie ważne szczegóły, takie jak rodzaj zdarzenia, typ niezgodności, błąd działania, wiadomość z ekranu czy dziwne zachowanie, a jeśli naruszenie bezpieczeństwa dotyczy danych osobowych – także inspektorowi ochrony danych.
2. Przez naruszenie bezpieczeństwa informacji rozumie się naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do informacji przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
3. W szczególności jako naruszenie bezpieczeństwa informacji kwalifikuje się utratę lub kradzież komputera, telefonu komórkowego, pendrive itp., na którym były zapisane informacje, utratę lub kradzież dokumentów papierowych, uzyskanie dostępu do informacji przez osobę, która nie jest do tego uprawniona, atak hackerski skutkujący zniszczeniem, utratą dostępu, zmodyfikowaniem lub ujawnieniem informacji, włamanie do pomieszczenia, w którym przechowywane są informacje, udostępnienie informacji osobom niepowołanym.
4. Podejmowanie przez pracownika jakichkolwiek własnych działań w celu usunięcia potencjalnego naruszenia bezpieczeństwa informacji jest zabronione, chyba że mają na celu ograniczenie skutków potencjalnego naruszenia.
5. W sytuacji dowiedzenia się o potencjalnym naruszeniu bezpieczeństwa informacji Burmistrz natychmiast przeprowadza wewnętrzne postępowanie w celu ustalenia okoliczności naruszenia oraz jego skutków, a także podejmuje niezwłoczne działania w celu naprawienia lub zapobieżenia skutkom naruszenia.
6. W przypadku naruszenia bezpieczeństwa danych osobowych Burmistrz bez zbędnej zwłoki – w miarę możliwości nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je Prezesowi Urzędu Ochrony Danych Osobowych, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych, których dane dotyczą.
7. Za datę i czas stwierdzenia naruszenia bezpieczeństwa danych osobowych uznaje się moment, w którym ustalono, że doszło z wystarczającą pewnością do naruszenia bezpieczeństwa danych osobowych.
8. Jeśli rodzaj i zasięg naruszenia bezpieczeństwa informacji, zidentyfikowany na którymkolwiek z etapów postępowania, uzasadnia potrzebę powiadomienia organów ścigania, to decyzję o sposobie i terminie powiadomienia podejmuje Burmistrz.
9. Przy zachowaniu należytej staranności w odniesieniu do poufności, naruszenie bezpieczeństwa informacji wykorzystuje się jako element podnoszenia świadomości pracowników, w szczególności jako przykład tego, co może się zdarzyć, jak reagować na takie naruszenia oraz jak unikać ich w przyszłości.

10. Na podstawie analizy zgłoszeń potencjalnych naruszeń bezpieczeństwa informacji, Burmistrz, a w przypadku danych osobowych – inspektor ochrony danych tworzy rekomendację dotyczącą szkoleń i doskonalenia zasad bezpieczeństwa informacji.

§ 35.

1. Okresowo przeprowadzana jest analiza ryzyka utraty integralności, dostępności lub poufności informacji oraz analiza ryzyka naruszenia praw i wolności osoby, której dane dotyczą.
2. Ryzyko to wskaźnik stanu lub zdarzenia, które może prowadzić do strat. Ryzyko jest proporcjonalne do prawdopodobieństwa wystąpienia tego zdarzenia i do wielkości strat, które może spowodować.
3. Zarządzanie ryzykiem to skoordynowane działania dotyczące kierowania i nadzorowania Urzędu w odniesieniu do ryzyka. W ramach zarządzania ryzykiem analizuje się, co może się zdarzyć i jakie mogą być możliwe następstwa, a następnie podejmuje decyzję, co i kiedy należy wykonać, aby zredukować ryzyko do akceptowalnego poziomu.
4. Prawdopodobieństwo ryzyka jest to oczekiwana częstotliwość wystąpienia zdarzenia zdefiniowanego jako ryzyko.
5. Strata, którą może spowodować ryzyko jest to wpływ zdarzenia zidentyfikowanego jako ryzyko na integralność, dostępność lub poufność informacji lub na osoby fizyczne w przypadku naruszenia ich praw i wolności.
6. Ocena ryzyka polega na określeniu prawdopodobieństwa wystąpienia ryzyka i starty, którą może spowodować ryzyko.

§ 36.

1. Oceny utraty integralności, dostępności lub poufności informacji dokonuje się poprzez przyznanie prawdopodobieństwu ryzyka i stracie, którą może spowodować ryzyko odpowiedniej liczby punktów.
2. Punktacja dla prawdopodobieństwa ryzyka utraty integralności, dostępności lub poufności informacji:
   1) prawie pewne – 3 pkt,
   2) możliwe – 2 pkt,
   3) rzadkie – 1 pkt.
3. Punktacja dla straty, którą może spowodować ryzyko utraty integralności, dostępności lub poufności informacji:
   1) utrata integralności, dostępności lub poufności informacji może skutkować co najmniej odpowiedzialnością karną lub wydatkami w kwocie 100.000,00 zł i więcej lub doniesieniami medialnymi w całym kraju – 3 pkt,
   2) utrata integralności, dostępności lub poufności informacji może skutkować co najmniej naruszeniem przepisów prawa lub wydatkami w kwocie od 10.000,00 zł do 100.000,00 zł lub informacjami w mediach ogólnokrajowych – 2 pkt,
   3) utrata integralności, dostępności lub poufności informacji może skutkować co najmniej odpowiedzialnością służbową lub wydatkami w kwocie do 10.000,00 zł lub informacjami w mediach regionalnych – 1 pkt.
4. Oceny ryzyka utraty integralności, dostępności lub poufności informacji dokonuje się odrębnie dla każdej grupy informacji i odrębnie dla utraty integralności, dostępności lub poufności informacji.

§ 37.

1. Oceny ryzyka naruszenia praw i wolności osoby, której dane dotyczą, dokonuje się poprzez przyznanie prawdopodobieństwu ryzyka i stracie, którą może spowodować ryzyko, odpowiedniej liczby punktów.
2. Punktacja dla prawdopodobieństwa ryzyka naruszenia praw i wolności osoby, której dane dotyczą:
   1) prawie pewne – 3 pkt,
   2) możliwe – 2 pkt,
   3) rzadkie – 1 pkt.
3. Punktacja dla straty, którą może spowodować ryzyko naruszenia praw i wolności osoby, której dane dotyczą:
   1) naruszenie z bardzo dużym prawdopodobieństwem może skutkować dyskryminacją, kradzieżą tożsamości lub oszustwem dotyczącym tożsamości, stratą finansową, naruszeniem dobrego imienia, naruszeniem poufności danych osobowych chronionych tajemnicą zawodową, nieuprawnionym odwróceniem pseudonimizacji lub wszelką inną znaczną szkodą gospodarczą lub społeczną – 3 pkt,
   2) naruszenie w zależności od kontekstu danego zdarzenia w niektórych przypadkach może skutkować dyskryminacją, kradzieżą tożsamości lub oszustwem dotyczącym tożsamości, stratą finansową, naruszeniem dobrego imienia, naruszeniem poufności danych osobowych chronionych tajemnicą zawodową, nieuprawnionym odwróceniem pseudonimizacji lub wszelką inną znaczną szkodą gospodarczą lub społeczną – 2 pkt,
   3) naruszenie nie będzie wpływało na prawa i wolności osób fizycznych – 1 pkt.
4. Oceny ryzyka naruszenia praw i wolności osoby, której dane dotyczą dokonuje się odrębnie dla utraty integralności, dostępności lub poufności danych osobowych.

§ 38.

Oceny ryzyka występujące Urzędzie:

a) ryzyko wysokie – suma przyznanych punktów od 5 do 6. Duża istotność. Konsekwencje poważne. Niezbędne są działania naprawcze,
b) ryzyko średnie – suma przyznanych punktów od 3 do 4. Średnia istotność. Przeciwdziałanie wskazane,
c) ryzyko niskie – suma przyznanych punktów od 1 do 2. Mała istotność. Przeciwdziałanie zależy od decyzji właściciela ryzyka.

§ 39.

1. W przypadku ryzyka wysokiego konieczne jest postępowanie z ryzykiem.
2. Metody postępowania z ryzykiem występujące w Urzędzie:
   a) unikanie – eliminacja zagrożeń,
   a) przeniesienie – przeniesienie ryzyka na inny podmiot, np. poprzez ubezpieczenie,
   b) łagodzenie – podjęcie działań mających na celu zmniejszenie negatywnych skutków wystąpienia zagrożenia,
   c) akceptacja – zaakceptowanie istniejącego ryzyka i wstrzymanie reakcji do chwili zaistnienia zagrożenia.
3. Postępowanie z ryzykiem jest proporcjonalne do ryzyka, tj. w większości przypadków ryzyka jest pod kontrolą, a nie eliminowane.
4. Postępując z ryzykiem bierze się pod uwagę w szczególności:
   1) ograniczenia czasowe (zabezpieczenie powinno zostać wdrożone w czasie „życia" informacji lub systemu),

2) ograniczenia finansowe (zabezpieczenia nie powinny być bardziej kosztowne do wdrożenia lub utrzymania niż strata, którą może przynieść ryzyko, z wyjątkiem sytuacji, gdy osiągnięcie zgodności jest wymagane przepisami prawa),
3) ograniczenia techniczne,
4) ograniczenia kulturowe (jeśli pracownicy nie rozumieją zabezpieczenia lub nie akceptują go, to zabezpieczenie staje się z czasem nieskuteczne),
5) ograniczenia prawne,
6) łatwość użycia,
7) ograniczenia przy integrowaniu nowych i istniejących zabezpieczeń.

§ 40.

1. Oceny ryzyka dokonują wyznaczeni przez Burmistrza pracownicy. Dopuszcza się udział innych osób – poza pracownikami – w ocenie ryzyka.
2. Ocenę ryzyka należy udokumentować.

§ 41.

W przypadku, gdy w związku z udzieleniem zamówienia publicznego lub współpracy dochodzi do przetwarzania informacji, wszelkie wymagania bezpieczeństwa informacji określa się w umowie.

§ 42.

Nie rzadziej niż raz w roku przeprowadza się audyt w zakresie bezpieczeństwa informacji.

§ 43.

Nie rzadziej niż raz w roku pełnomocnik ds. ochrony informacji niejawnych w zakresie informacji niejawnych, Referat Finansowy ds. Wymiarów, Opłat i Podatków Lokalnych oraz Referat Gospodarki Odpadami Komunalnymi w zakresie tajemnicy skarbowej, inspektor ochrony danych w zakresie danych osobowych oraz każda komórka organizacyjna Urzędu w zakresie przetwarzanych przez tę komórkę tajemnic ustawowo chronionych, za wyjątkiem danych osobowych, informacji o charakterze wewnętrznym i pozostałych informacji dokonują przeglądu „Systemu zarządzania bezpieczeństwem informacji" pod kątem zgodności z przepisami prawa. Przegląd należy udokumentować.

§ 44.

„System zarządzania bezpieczeństwem informacji" jest objęty bezwzględną tajemnicą.

Załącznik nr 1 do „Systemu zarządzania bezpieczeństwem informacji” – wzór oświadczenia o zachowaniu poufności

OŚWIADCZENIE O ZACHOWANIU POUFNOŚCI

Oświadczam, że zostałam zapoznana/zostałem zapoznany[1] z zasadami przetwarzania i ochrony informacji określonymi w przepisach prawa powszechnie obowiązującego i procedurach wewnętrznych obowiązujących w Urzędzie Miejskim Orzesze. Zobowiązuję się nie wykorzystywać informacji, do których uzyskam dostęp w celach innych niż te, które są częścią moich obowiązków, ujawniać informacje wyłącznie osobom uprawnionym, nie wykonywać żadnych kopii informacji, chyba że będzie to konieczne do wykonania moich obowiązków, podejmować wszelkie działania (środki) zgodne z przeznaczeniem informacji i stanem wiedzy w kontekście moich obowiązków, aby zapobiec przypadkowemu lub niezgodnemu z prawem wykorzystaniu tych informacji, podejmować wszelkie środki ostrożności zgodnie z przeznaczeniem informacji i stanem techniki w celu zachowania fizycznego i logicznego bezpieczeństwa tych informacji, upewniać się, w granicach moich obowiązków, że tylko bezpieczne środki komunikacji zostaną wykorzystane do przekazania tych informacji, a w przypadku zakończenia wykonywania obowiązków, do całkowitego zwrócenia informacji, plików komputerowych i wszelkich nośników informacji oraz do zachowania w tajemnicy przetwarzanych informacji oraz sposobów ich zabezpieczenia.

Zobowiązanie do zachowania poufności nie będzie naruszone w sytuacji, gdy obowiązek ujawnienia informacji wynika z powszechnie obowiązujących przepisów prawa.

Oświadczam, że jestem świadoma/świadomy[1] odpowiedzialności dyscyplinarnej, finansowej i karnej wynikającej z niewłaściwego postępowania przy przetwarzaniu informacji.

……
(data, imię i nazwisko oraz podpis)

[1] niepotrzebne skreślić lub skasować

Załącznik nr 2 do „Systemu zarządzania bezpieczeństwem informacji” – wzór wniosku o przyznanie dostępu do systemu informatycznego

WNIOSEK O PRZYZNANIE DOSTĘPU DO SYSTEMU INFORMATYCZNEGO

Proszę o przyznanie Pani/Panu[1] … *(imię i nazwisko)* dostępu do systemu informatycznego dla następujących zasobów lub zadań: … oraz konta pocztowego e-mail[1].

Dostęp powinien być lokalny/zdalny[1].

Przełożony użytkownika systemu

……
(data, pieczątka i podpis)

Dostęp przyznano zgodnie z wnioskiem – jeśli nie, wskazać powód odmowy lub modyfikacji dostępu: …[1]

Pracownik Referatu Informatyki
i Bezpieczeństwa Informacji

……
(data, pieczątka i podpis)

[1] niepotrzebne skreślić lub skasować

Załącznik nr 3 do „Systemu zarządzania bezpieczeństwem informacji" – wzór upoważnienia do przetwarzania danych osobowych i wzór odwołania upoważnienia do przetwarzania danych osobowych

Orzesze, … roku

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Na podstawie § 6 „Systemu zarządzania bezpieczeństwem informacji"[1] w związku z art. 29 oraz art. 32 ust. 1 i 4 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 roku 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) upoważniam Panią/Pana[2] … *(imię i nazwisko)* do przetwarzania danych osobowych ... *(cel przetwarzania, zakres itp. oraz – ewentualnie – od kiedy)*.

Administrator

……
(pieczątka i podpis)

Ja niżej podpisana/podpisany[2] zobowiązuję się do przetwarzania danych osobowych wyłącznie w zakresie nadanego mi upoważnienia, a także do zachowania w tajemnicy przetwarzanych danych oraz sposobów ich zabezpieczenia.

Oświadczam, że jestem świadoma/świadomy[2] odpowiedzialności dyscyplinarnej, finansowej i karnej wynikającej z niewłaściwego postępowania przy przetwarzaniu danych osobowych.

Upoważniona osoba

……
(podpis)

[1] w przypadku istnienia obowiązku upoważnienia wynikającego z ustawy lub innego aktu prawa powszechnie obowiązującego wpisać tę podstawę prawną
[2] niepotrzebne skreślić lub kasować

Orzesze, … roku

ODWOŁANIE UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH

Na podstawie § 6 „Systemu zarządzania bezpieczeństwem informacji”[1] w związku z art. 29 oraz art. 32 ust. 1 i 4 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 roku 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) odwołuję z/od[2] … *(data)* z godziną …[3] *(dokłada godzina w układzie 00:00)* upoważnienie do przetwarzania danych osobowych dla Pani/Pana[2] … *(imię i nazwisko oraz – ewentualnie – w jakim zakresie).*

Administrator

……
(pieczątka i podpis)

[1] w przypadku istnienia obowiązku upoważnienia wynikającego z ustawy lub innego aktu prawa powszechnie obowiązującego wpisać tę podstawę prawną
[2] niepotrzebne skreślić lub skasować
[3] opcjonalnie; jeśli nie – skreślić lub skasować

Załącznik nr 4 do „Systemu zarządzania bezpieczeństwem informacji” – wykaz osób uprawnionych do pobrania kluczy zapasowych zdeponowanych na komisariacie policji

WYKAZ OSÓB UPRAWNIONYCH DO POBRANIA KLUCZY ZAPASOWYCH ZDEPONOWANYCH NA KOMISARIACIE POLICJI

Lp.	Imię i nazwisko	Nr dowodu osobistego
1.	Mirosław Blaski	CCG080187
2.	Sylwia Krawczyk	DER116035
3.	Jolanta Szubert	DBX540734
4.	Iwona Burszka	DEY242111
5.	Aleksandra Blacha	CGJ548406
6.	Mariola Kolonko	DER016027