Biuro projektu: DG PMC Sp. z o.o.
Ul. Tylne Chwaliszewo 25, 61-103 Poznań
tel. (61) 839 90 24, fax (61) 839 92 97
email: pmc@dgpmc.pl, www.dgpmc.pl

Projekt jest współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego

Zarządzenie Nr 12/W/2015

Burmistrza Krobi

z dnia 10 kwietnia 2015r.

w sprawie : wdrożenia instrukcji podstawowych zasad bezpieczeństwa informacji w Urzędzie Miejskim w Krobi

Na podstawie art.31 oraz art.33 ust.3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U z 2013 r.,poz.594 z późn.zm.) , w związku z realizacją Projektu Cyfryzacja Administracji Samorządowej Elektroniczna Optymalizacja w ramach Programu Operacyjnego Kapitał Ludzki zarządzam , co następuje:

§ 1

1.Wprowadzam do stosowania „Instrukcję podstawowych zasad bezpieczeństwa informacji w Urzędzie Miejskim w Krobi stanowiącą załącznik nr 1 do zarządzenia.

2.Wprowadzam do stosowania „Metodologię przeprowadzania klasyfikacji informacji oraz analizy i oceny ryzyka dla bezpieczeństwa informacji w Urzędzie Miejskim w Krobi stanowiącą załącznik nr 2 do zarządzenia .

§ 2

Wykonanie zarządzenia powierzam Koordynatorowi Projektu oraz Informatykowi .

§ 3

Nadzór nad wykonaniem zarządzenia powierzam Sekretarzowi Gminy.

§ 4

2.Zarządzenie wchodzi w życie z dniem podpisania

BURMISTRZ
Sebastian Czwojda

Otrzymują :

1)Naczelnicy UM w Krobi

2) WO –a/a

Biuro projektu: DG PMC Sp. z o.o.
Ul. Tylne Chwaliszewo 25, 61-103 Poznań
tel. (61) 839 90 24, fax (61) 839 92 97
email: pmc@dgpmc.pl, www.dgpmc.pl

Projekt jest współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego

Załącznik Nr 1 do Zarządzenia nr 12/W/2015 z dnia 10 kwietnia 2015.

INSTRUKCJA PODSTAWOWYCH ZASAD BEZPIECZEŃSTWA INFORMACJI W URZĘDZIE MIEJSKIM W KROBI

PRZEDMIOT INSTRUKCJI

Przedmiotem instrukcji jest:
- stosowanie i nadzorowanie podstawowych zasad bezpieczeństwa informacji,
- zdefiniowanie podstawowych zasad bezpieczeństwa informacji.

ZAKRES INSTRUKCJI

Instrukcja definiuje podstawowe zasady bezpieczeństwa informacji, które stanowią minimalne wymagania dotyczące sposobu postępowania z informacjami.
Instrukcja dotyczy wszystkich pracowników Urzędu Miejskiego w Krobi.
Z uwagi na charakter Urzędu i niezbędność zagwarantowania jawności i przejrzystości funkcjonowania, wynikającej z Ustawy o dostępie do informacji publicznej, zakłada się nadrzędność zapisów przywoływanej ustawy nad wymaganiami stawianymi przez zasady opisane w niniejszej instrukcji.

STOSOWANIE I NADZOROWANIE STOSOWANIA PODSTAWOWYCH ZASAD BEZPIECZEŃSTWA

1. Każdego z pracowników, zobowiązuje się do stosowania podstawowych zasad bezpieczeństwa informacji.
2. Nadzór nad przestrzeganiem przez pracowników zasad określonych w niniejszej instrukcji sprawuje Sekretarz Gminy.

Podstawowe Zasady Bezpieczeństwa Informacji:
1. **Zasada wiedzy koniecznej** – ograniczanie dostępu do informacji jedynie do tych, które są niezbędne do wykonywania obowiązków na danym stanowisku.
2. **Zasada odpowiedzialności za zasoby** - pracownik jest odpowiedzialny za przetwarzane/powierzone mu informacje i zobowiązany jest przestrzegać ustanowionych procedur bezpieczeństwa informacji.
3. **Zasada zamkniętego pomieszczenia** – niepozostawianie osób postronnych samych w pomieszczeniu (pod nieobecność osoby upoważnionej), bezwzględne zamykanie pomieszczeń na klucz przy ich opuszczaniu i niepozostawianie kluczy w zamkach.
4. **Zasada czystego biurka** – niepozostawianie bez nadzoru dokumentów papierowych oraz nośników danych na biurku (płyt CD, DVD, pamięci flash USB itp.).
5. **Zasada prywatności kont w systemach** – każdy pracownik zobowiązany jest do pracy w

systemach teleinformatycznych na przypisanych jemu kontach. Zabronione jest udostępnianie kont osobom, które nie zostały do nich przypisane.

6. **Zasada poufności haseł i kodów dostępu** – zachowanie poufności i nieprzekazywanie osobom nieuprawnionym haseł i kodów dostępu. W szczególności zasada ta dotyczy osobistych haseł dostępu do systemów teleinformatycznych.
7. **Zasada czystego ekranu** – blokowanie komputera przed każdym opuszczeniem pomieszczenia. W przypadku dłuższej nieobecności w pomieszczeniu konieczne jest wylogowanie się z systemu.
8. **Zasada czystego pulpitu** – na pulpicie komputera mogą znajdować się jedynie ikony standardowego oprogramowania i aplikacji służbowych oraz skróty do folderów pod warunkiem, że w nazwie nie zawierają informacji, które mogą zostać w sposób niekontrolowany ujawnione (np. podczas prezentacji).
9. **Zasada czystych drukarek** – zabieranie dokumentów z drukarek zaraz po ich wydrukowaniu. W szczególności zasada ta dotyczy dokumentów pozostawianych w drukarkach znajdujących się w innym pomieszczeniu.
10. **Zasada czystego kosza** – dokumenty papierowe z wyjątkiem materiałów promocyjnych powinny być niszczone w niszczarkach lub za pośrednictwem firmy zewnętrznej.
11. **Zasada legalności oprogramowania** – zabrania się samodzielnego instalowania oprogramowania, w tym w szczególności przechowywania na komputerze treści naruszających prawa autorskie oraz innych nielegalnych danych.
12. **Zasada zgłaszania incydentów bezpieczeństwa** – każdy z pracowników zobowiązany jest do zgłaszania incydentów związanych z bezpieczeństwem informacji, tj. nieuprawnionym ujawnieniem, zniszczeniem lub modyfikacją informacji, zgodnie z trybem określonym w Polityce bezpieczeństwa ochrony danych osobowych.
13. **Zasada korzystania z zasobów dopuszczonych przez Urząd** – Informacje których właścicielem jest Urząd mogą być przetwarzane wyłącznie w środkach przetwarzania dopuszczonych do wykorzystania w Urzędzie. W szczególności wzbrania się korzystania w tym celu z prywatnych środków przetwarzania informacji.
14. **Zasada przekazywania informacji do wiadomości publicznej** - Przekazywanie informacji do wiadomości publicznej (w tym: upublicznianie na stronach internetowych) możliwe jest wyłącznie z zastosowaniem przepisów w zakresie udostępnienia informacji publicznej.
15. **Zasada korzystania z zasobów Urzędu do celów prywatnych** – Zabrania się wykorzystywania służbowego komputera przenośnego do celów prywatnych.

PODSTAWOWE ZASADY BEZPIECZENSTWA INFORMACJI W PRZYPADKU UŻYTKOWANIA SLUZBOWYCH KOMPUTEROW PRZENOSNYCH

1. Praca na sprzęcie przenośnym może być wykonywana jedynie na służbowym komputerze skonfigurowanym przez informatyka.

Biuro projektu: DG PMC Sp. z o.o.
Ul. Tylne Chwaliszewo 25, 61-103 Poznań
tel. (61) 839 90 24, fax (61) 839 92 97
email: pmc@dgpmc.pl, www.dgpmc.pl

Projekt jest współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego

2. Korzystanie ze służbowych komputerów przenośnych w miejscach publicznych jest dozwolone, o ile otoczenie, w którym znajduje się pracownik stwarza warunki minimalizujące ryzyko zapoznania się z danymi przez osoby nieupoważnione.
3. Osoba użytkująca służbowy komputer przenośny powinna zachować szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza Urzędem.
4. Urządzenia przenośne lub komputerowe nośniki danych, na których przechowywane są informacje, należy chronić przed uszkodzeniami fizycznymi.

Załączniki do Instrukcji:
1) INSTRUKCJA ZARZĄDZANIA STACJAMI ROBOCZYMI W URZĘDZIE MIEJSKIM W KROBI
2) INSTRUKCJA ZBYWANIA I PRZEKAZYWANIA SPRZĘTU WYKORZYSTYWANEGO DO PRZETWARZANIA INFORMACJI W URZĘDZIE MIEJSKIM W KROBI
3) PZRYKAŁADY ZAPISÓW W UMOWACH W ZAKRESIE BEZPIECZEŃSTWA INFORMACJI W URZĘDZIE MIEJSKIM W KROBI
4) PROCEDURA ZARZĄDZANIA KLUCZAMI DO POMIESZCZEŃ URZĘDU

CAS CYFRYZACJA ADMINISTRACJI SAMORZĄDOWEJ

Biuro projektu: DG PMC Sp. z o.o.
Ul. Tylne Chwaliszewo 25, 61-103 Poznań
tel. (61) 839 90 24, fax (61) 839 92 97
email: pmc@dgpmc.pl, www.dgpmc.pl

Projekt jest współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego

Załącznik nr 2
do zarządzenia NR 12/W/2015
BURMISTRZA KROBI
z dnia 10 kwietnia 2015r.

METODOLOGIA PRZEPROWADZANIA KLASYFIKACJI INFORMACJI ORAZ ANALIZY I OCENY RYZYKA DLA BEZPIECZEŃSTWA INFORMACJI W URZĘDZIE MIEJSKIM W KROBI

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

pmc
Doradztwo Gospodarcze

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Biuro projektu: DG PMC Sp. z o.o.
Ul. Tylne Chwaliszewo 25, 61-103 Poznań
tel. (61) 839 90 24, fax (61) 839 92 97
email: pmc@dgpmc.pl, www.dgpmc.pl

Projekt jest współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego

I. CEL DOKUMENTU

Celem dokumentu jest określenie metodologii postępowania przy klasyfikowaniu informacji, które są głównym zasobem informacyjnym Urzędu Miejskiego w Krobi, w celu uregulowania sposobu postępowania z tymi informacjami, których ujawnienie mogłoby narazić Urząd na szkodę. Ponadto dokument ten określa sposób przeprowadzania analizy ryzyka w obszarze bezpieczeństwa informacji, której celem jest oszacowanie ryzyka utraty informacji na podstawie istniejących zagrożeń oraz określenie poziomów ryzyka akceptowalnego. W przypadku zidentyfikowania ryzyka nieakceptowalnego określeniu sposobu postępowania, wdrożenia działań doskonalących, w celu doprowadzenia tego ryzyka do poziomu akceptowalnego.

II. DEFINICJE

BEZPIECZEŃSTWO INFORMACJI - zachowanie poufności, integralności i dostępności informacji; dodatkowo, mogą być brane pod uwagę inne własności, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.

AKTYW – wszystko to co ma wartość dla organizacji.
Istnieje wiele typów informacji:

a) Informacje: bazy danych i pliki z danymi, kontrakty i umowy, dokumentacje systemowe, informacje badawcze, podręczniki użytkownika, materiały szkoleniowe, procedury operacyjne i wspierające, plany ciągłości działania, plany odtworzenia, zapisy auditowe oraz informacje archiwizowane;
b) Oprogramowanie: oprogramowanie systemowe, aplikacje, narzędzia rozwojowe i inne;
c) Aktywa fizyczne: sprzęt komputerowy, urządzenia komunikacyjne, nośniki wymienne i inne urządzenia;
d) Usługi: usługi przetwarzania i przesyłania, usługi ogólne: np. ogrzewanie, oświetlenie, zasilanie i klimatyzacja;
e) Ludzie i ich kwalifikacje, umiejętności i doświadczenie;
f) Wartości niematerialne, takie jak reputacja oraz wizerunek organizacji.

KLASYFIKACJA INFORMACJI – proces, którego celem jest zapewnienie, że informacje mają odpowiedni poziom ochrony.

POUFNOŚĆ - właściwość, że informacja nie jest udostępniana lub wyjawiana nieupoważnionym osobom, podmiotom lub procesom.

INTEGRALNOŚĆ - właściwość zapewnienia dokładności i kompletności aktywów.

Biuro projektu: DG PMC Sp. z o.o.
Ul. Tylne Chwaliszewo 25, 61-103 Poznań
tel. (61) 839 90 24, fax (61) 839 92 97
email: pmc@dgpmc.pl, www.dgpmc.pl

Projekt jest współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego

DOSTĘPNOŚĆ - właściwość bycia dostępnym i użytecznym na żądanie upoważnionego podmiotu.

WŁAŚCICIEL INFORMACJI - osoba lub podmiot, która ma zatwierdzoną przez kierownictwo odpowiedzialność za nadzorowanie produkcji, rozwój, utrzymanie, korzystanie i bezpieczeństwo informacji; pojęcie to nie oznacza, że osoba ta rzeczywiście posiada jakiekolwiek prawa własności do informacji.

III. METODOLOGIA KLASYFIKACJA INFORMACJI W URZĘDZIE MIEJSKIM W KROBI.

W celu przeprowadzenia klasyfikacji informacji w Urzędzie należy zidentyfikować wszystkie grupy informacji dostępne na poszczególnych stanowiskach pracy z przypisaniem właścicieli tych informacji, a następnie należy dla każdej ze zidentyfikowanych grup informacji dokonać oceny w aspekcie wartości poszczególnych atrybutów bezpieczeństwa informacji tzn. poufności integralności i dostępności. Oceny tej dokonuje właściciel informacji określając poziom istotności (zgodnie z podanym poniżej wzorem), biorąc pod uwagę przytoczone w tabeli skale do oceny poufności, integralności i dostępności informacji. Poziomy istotności są tożsame ze skutkiem utraty danej grupy informacji.

Biuro projektu: DG PMC Sp. z o.o.
Ul. Tylne Chwaliszewo 25, 61-103 Poznań
tel. (61) 839 90 24, fax (61) 839 92 97
email: pmc@dgpmc.pl, www.dgpmc.pl

Projekt jest współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego

Skala wartości dla poszczególnych atrybutów bezpieczeństwa informacji

Poufność (P)	**1**	Informacje publicznie dostępne.
	3	Dokumenty, w stosunku do których Urząd może zastosować ochronę przed nieautoryzowanym dostępem, nie podyktowaną jednak wprost wymogami prawnymi.
	5	Dokumenty wymagające ochrony przed nieautoryzowanym dostępem podyktowanej wymogami prawnymi, np. Ustawą o ochronie danych osobowych, Ustawą o zamówieniach publicznych.
Integralność (I)	**1**	Nieautoryzowana zmiana dokumentu nie powoduje strat ani nie wpływa na jakość świadczonych usług przez Urząd.
	3	Nieautoryzowana zmiana dokumentu może spowodować nieznaczne straty lub nieznacznie wpłynąć na wewnętrzne funkcjonowanie Urzędu.
	5	Nieautoryzowana zmiana dokumentu może spowodować, straty finansowe, konsekwencje prawne lub też wpłynąć na wizerunek Urzędu.
Dostępność (D)	**1**	Niedostępność informacji przez kilka dni nie wpłynie znacząco na funkcjonowanie Urzędu.
	3	Niedostępność informacji przez 1 dzień wpłynie znacząco na funkcjonowanie Urzędu.
	5	Informacje muszą być dostępne jeszcze tego samego dnia.

Poziom istotności danej informacji lub grupy informacji obliczamy wg wzoru:

$$S = (P+I+D)/3$$

Gdzie:

- P to atrybut poufności informacji
- I to atrybut integralności informacji
- D to atrybut dostępności informacji

Biuro projektu: DG PMC Sp. z o.o.
Ul. Tylne Chwaliszewo 25, 61-103 Poznań
tel. (61) 839 90 24, fax (61) 839 92 97
email: pmc@dgpmc.pl, www.dgpmc.pl

Projekt jest współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego

Sposoby postępowania ze sklasyfikowanymi grupami informacji - poziom ochrony

Na podstawie określonego przez właściciela informacji poziomu istotności określony zostaje poziom ochrony, który warunkuje możliwy sposób postępowania z informacją, która jest głównym zasobem informacyjnym Urzędu.

1. **Podstawowy – (poziom istostności S <= 2,33) - informacje ogólnodostępne (publiczne)** – do tej grupy należy zakwalifikować informacje spełniające następujące atrybuty:
   - informacja jest przeznaczona do powszechnego wykorzystywania. Okresowa utrata dostępności do informacji nie stanowi zagrożenia dla ciągłości działania Urzędu i ryzyko z tym związane określono jako akceptowalne.
   - Zachowanie integralności informacji posiada ograniczone (np. wizerunkowe) znaczenie dla Urzędu. Utrata integralności nie rodzi skutków finansowych lub prawnych dla Urzędu.
   - Poufność nie jest zachowana.

Przykłady informacji tego typu to: informacje marketingowe, broszury informacyjne, zawartość stron www oraz BIP, publicznie dostępne raporty finansowe, itp.
Wyjątkowego potraktowania wymagają informacje udostępniane w BIP, które z mocy ustawy dostępne są bez ograniczeń, jednak niewątpliwie muszą posiadać atrybut kontroli integralności.

Zarządzanie kopiami informacji udostępnianych publicznie
Informacje zaliczone do tej grupy mogą być powielane bez ograniczeń w dowolnej formie. Odpowiedzialność za zarządzanie kopią informacji (w szczególności za jej aktualność) spoczywa na odbiorcy informacji, który tę kopię wykonał.

Dystrybucja informacji udostępnianych publicznie
Nie podlega ograniczeniom, jeśli nie narusza ogólnych przepisów prawa.

Usuwanie informacji udostępnianych publicznie
Nie określa się żadnych dodatkowych wymagań – w przypadku informacji w formie elektronicznej w postaci pliku wystarcza standardowe skasowanie go z wykorzystaniem standardowej funkcji systemu operacyjnego, nośniki zawierające informacje zakwalifikowane do tej grupy (papier, tworzywa sztuczne, urządzenia elektroniczne, itp.) mogą być przekazywane do recyclingu.

2. **Rozszerzony – (poziom istotności S > 2,33) – informacje wewnętrzne** – informacje, których przetwarzanie i udostępnianie podlega restrykcjom z uwagi na szczególne znaczenie dla pracodawcy (właściciela informacji):
   a) **informacje wewnętrzne dostępne** – informacje dostępne dla wszystkich pracowników Urzędu
   b) **informacje wewnętrzne wrażliwe** - informacje dostępne dla grupy pracowników upoważnionych z uwagi na realizowane zadania regulaminowe,
   c) **informacje stanowiące tajemnicę pracodawcy** - informacje, których przetwarzanie i udostępnianie może narazić pracodawcę na szkodę;

Atrybuty jakości informacji zakwalifikowanych do tej grupy określa się następująco:
- dostępność – ograniczona do osób posiadających odpowiednie upoważnienie, dystrybucja informacji jedynie do osób upoważnionych,
- integralność – weryfikacja integralności informacji jest obowiązkowa,
- poufność – odbiorcy informacji są zobowiązani do ochrony otrzymywanych informacji należących do tej grupy. Korzystanie z informacji jest dozwolone jedynie w pomieszczeniach, do których dostęp jest kontrolowany i w których nie mogą przebywać bez nadzoru osoby nieuprawnione.

Przykłady informacji, które powinny znaleźć się w tej grupie to wszelkie informacje niezbędne do sprawnego działania Urzędu – obowiązujące procedury, zarządzenia, materiały szkoleniowe, okólniki, raporty, kontrakty i porozumienia z podmiotami zewnętrznymi, wewnętrzne listy mailingowe i książki telefoniczne, dokumentacje projektowe i wykonawcze, dokumentacje wymieniane z innymi podmiotami (wydawane decyzje itp.), dane osobowe, itp.

Dodatkowe mechanizmy ochrony

Powinna istnieć lista osób upoważnionych do dostępu do danej grupy informacji. Posiadacz tego rodzaju informacji jest odpowiedzialny za odpowiednie jej zabezpieczenie podczas jej przetwarzania i przechowywania, niezależnie od formy i nośnika, na którym informacja jest przechowywana.

Zarządzanie kopiami

Kopie informacji „do użytku wewnętrznego" mogą być wykonywane jedynie przez pracowników Urzędu lub przez współpracujące z nią podmioty, których upoważnieni przedstawiciele podpisali z Urzędem odpowiedni dokument o zachowaniu poufności. Kopia informacji „do użytku wewnętrznego" podlega takim samym zasadom ochrony jak jej oryginał.

Dystrybucja informacji „do użytku wewnętrznego"

Wewnątrz Urzędu:
1. w przypadku przekazywania informacji na nośniku należy go umieścić w odpowiedniej kopercie poczty wewnętrznej,
2. do dystrybucji w postaci elektronicznej dopuszczalne jest jedynie wykorzystywanie wewnętrznego systemu poczty elektronicznej wyposażonego w mechanizm zapobiegający przypadkowemu lub niezamierzonemu wysyłaniu informacji na adres zewnętrzny.

Na zewnątrz Urzędu:
1. na nośnikach – odpowiednio zabezpieczony list polecony za potwierdzeniem odbioru lub

przesyłka kurierska,

2. w postaci elektronicznej – poczta elektroniczna wyposażona w działający mechanizm szyfrowania przesyłek.
3. Telefaxem – pod warunkiem uwierzytelniania numeru odbiorcy.

Usuwanie informacji „do użytku wewnętrznego"

Należy zastosować mechanizmy uniemożliwiające odzyskanie usuwanej informacji „do użytku wewnętrznego". Informacja i wszystkie jej kopie muszą być bezwarunkowo usunięte po upływie terminu jej ważności lub na udokumentowane polecenie jej właściciela. Za archiwizację informacji „do użytku wewnętrznego" odpowiada jej właściciel.

1. Dokumenty w postaci papierowej – należy użyć niszczarki dokumentów,
2. Dokumenty na nośnikach elektronicznych – w przypadku wycofania nośnika (np. krążka CD/DVD) z dalszego użycia należy go przekazać do likwidacji. Nośniki, na których nie jest możliwe skasowanie danych (np. CD Read Only) należy przed przekazaniem uszkodzić fizycznie. Z nośników, na których możliwe jest kasowanie danych należy przed przekazaniem do likwidacji skasować wszelkie informacje stosując standardowe mechanizmy systemu operacyjnego (np. procedurę formatowania).
3. Jeśli nośnik (np. komputer), na którym znajduje się informacja „do użytku wewnętrznego" podlegająca usunięciu będzie w dalszym ciągu wykorzystywany przez tego samego użytkownika należy skasować tę informację posługując się standardowymi mechanizmami systemu operacyjnego. W przypadku przekazywania nośnika (komputera, dysku przenośnego, itp.) innemu użytkownikowi należy skasować wszelkie zawarte na nim informacje „do użytku wewnętrznego" i przekazać go wyznaczonemu działowi w celu zakończenia procedury kasowania zawartych w nim informacji.

Biuro projektu: DG PMC Sp. z o.o.
Ul. Tylne Chwaliszewo 25, 61-103 Poznań
tel. (61) 839 90 24, fax (61) 839 92 97
email: pmc@dgpmc.pl, www.dgpmc.pl

Projekt jest współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego

IV. METODOLOGIA ANALIZY I OCENY RYZYKA

Po dokonaniu klasyfikacji informacji dokonuje się analizy i oceny ryzyka, która obejmuje ocenę skuteczności środków zabezpieczających dla poszczególnych zagrożeń, a następnie ocenę prawdopodobieństwa realizacji tych zagrożeń dla poszczególnych grup informacji.
W procesie szacowania ryzyka analizie należy poddać następujące zagrożenia w poszczególnych, niżej wymienionych obszarach.

Zagrożenia w obszarze systemów i usług informatycznych

- Błędy w aplikacjach lub w oprogramowaniu systemowym (w kodzie źródłowym), których rezultatem jest niepożądane zachowywanie się systemów informatycznych
- Nieautoryzowane zmiany, nielegalne wykorzystanie lub nadużywanie oprogramowania/ systemów informatycznych/ stacji roboczej/ infrastruktury sieciowej
- Utrata danych lub długotrwały brak dostępu do danych, będący wynikiem awarii systemu informatycznego/infrastruktury teleinformatycznej (brak możliwości odtworzenia systemu i/lub danych, brak infrastruktury zapasowej, brak umów SLA itp.)
- Nieautoryzowany dostęp do wewnętrznej sieci teleinformatycznej lub systemu informatycznego przez pracownika Urzędu lub osoby trzecie
- Awaria sprzętowa urządzeń sieci teleinformatycznej / urządzeń sieciowych / serwerów dedykowanych dla systemów informatycznych.
- Przerwa w świadczeniu usług dostarczanych przez firmy trzecie w zakresie sieci teleinformatycznej
- Atak wirusowy / szkodliwe oprogramowanie / inne podatności systemów informatycznych
- Nieodpowiednie warunki techniczne w serwerowni (wilgotność, temperatura)

Zagrożenia w obszarze realizacji procesów

- Naruszenie prawa w ramach realizowania usług przez Urząd (m.in. w zakresie ustawy o ochronie danych osobowych oraz legalności oprogramowania)

Zdarzenia zewnętrzne

- Włamanie, wtargnięcie lub inne nieuprawnione wejście na teren Urzędu, kradzież zasobów
- Pożar, powódź, zalanie i inne zagrożenia środowiskowe
- Awaria zasilania energetycznego

Zagrożenia w obszarze zasobów ludzkich

- Ujawnienie informacji osobom nieuprawnionym, zniszczenie lub nieuprawniona zmiana informacji wynikające z błędu (z uwzględnieniem braku szkoleń, niskiej świadomości pracowników) lub zamierzonego działania pracownika Urzędu.
- Ujawnienie informacji osobom nieuprawnionym, zniszczenie lub nieuprawniona zmiana informacji wynikające z błędu (z uwzględnieniem braku szkoleń, niskiej świadomości) lub zamierzonego działania pracownika stron trzecich (firmy współpracujące, kontrahenci).

Biuro projektu: DG PMC Sp. z o.o.
Ul. Tylne Chwaliszewo 25, 61-103 Poznań
tel. (61) 839 90 24, fax (61) 839 92 97
email: pmc@dgpmc.pl, www.dgpmc.pl

Projekt jest współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego

Dokonując oceny skuteczności środków zabezpieczających dla poszczególnych zagrożeń, a następnie oceny prawdopodobieństwa realizacji tych zagrożeń dla poszczególnych grup informacji należy skorzystać z poniższych tabel określających skalę wartości.

Skala wartości dla oceny prawdopodobieństwa realizacji zagrożenia [P]

Skala	Prawdopodobieństwo realizacji zagrożenia
1	Zagrożenie praktycznie się nie zrealizuje.
2	Nie istnieją dogodne uwarunkowania do realizacji zagrożenia (zagrożenie nie występowało wcześniej w Urzędzie).
3	Zagrożenie może się zrealizować (zagrożenie może pojawić się raz w roku).
4	Istnieją dogodne uwarunkowania do realizacji zagrożenia (można się spodziewać, że zagrożenie wystąpi w Urzędzie kilka (1-3) razy w roku).
5	Ryzyko na pewno się zrealizuje (zagrożenie, którego może wystąpić w Urzędzie raz w miesiącu lub częściej).

Skala wartości dla oceny skuteczności środków zabezpieczających [E]

Skuteczność	Przesłanki
1	Nie funkcjonują środki zabezpieczające informacje przed zagrożeniem
2	Wdrożono tylko podstawowe zabezpieczenia lub dla wdrożonych zabezpieczeń stwierdzono znaczące uchybienia/podatności wpływające na ich skuteczność.
3	Wdrożono mechanizmy zabezpieczające. Stwierdzono nieznaczne uchybienia/podatności wpływające na ich skuteczność.
4	Wdrożono mechanizmy zabezpieczające. Nie stwierdzono uchybień w ich skuteczności/ stosowaniu.
5	Wdrożono zarówno podstawowe jak i dodatkowe/zaawansowane mechanizmy zabezpieczające. Nie stwierdzono uchybień w ich skuteczności/stosowaniu.

Biuro projektu: DG PMC Sp. z o.o.
Ul. Tylne Chwaliszewo 25, 61-103 Poznań
tel. (61) 839 90 24, fax (61) 839 92 97
email: pmc@dgpmc.pl, www.dgpmc.pl

Projekt jest współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego

Następnie na podstawie analiz przeprowadzonych dla istotności grup informacji, skuteczności środków zabezpieczających oraz prawdopodobieństwa realizacji zagrożeń dokonać należy obliczenia wartości ryzyka zgodnie ze wzorem:

$$\mathbf{R = [Pr \times S] / E}$$

gdzie:

Pr	to prawdopodobieństwo zajścia/realizacji zagrożenia dla danej informacji lub grupy informacji,
E	to skuteczność środków zabezpieczających przed zagrożeniem ,
S	to skutek wynikający z istotności/znaczenia grupy informacji

Kryteria oceny ryzyka

Po wyznaczeniu wartości ryzyk należy dokonać określenia rankingu ryzyk z podziałem, na ryzyka akceptowalne i nieakceptowane. Podziału dokonanać należy zgodnie z tabelą.

Poziom ryzyka R	Ocena ryzyka
<= 3	Akceptowalne
> 3	Nieakceptowalne

Biuro projektu: DG PMC Sp. z o.o.
Ul. Tylne Chwaliszewo 25, 61-103 Poznań
tel. (61) 839 90 24, fax (61) 839 92 97
email: pmc@dgpmc.pl, www.dgpmc.pl

Projekt jest współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego

V. POSTĘPOWANIE Z RYZYKIEM

Po przeprowadzeniu klasyfikacji informacji oraz anlizy i oceny ryzyka wyniki należy przedstawić Burmistrzowi, ze wskazaniem planu postępowania z ryzykiem utraty bezpieczeństwa informacji tzn. wskazaniem niezbędnych działań doskonalących, pozwalających osiągnąć ryzyko akceptowalne.

Możliwe sposoby postępowania z ryzykiem:

1. **Redukcja ryzyka**
   Może być realizowana na kilka sposobów, ale najczęściej jest to implementacja odpowiednich korekt w naszym systemie (np. wykonanie aktualizacji nieaktualnego oprogramowania, załatanie podatności w aplikacjach).
2. **Akceptacja ryzyka**
   W przypadku, kiedy ryzyko jest małe, a potencjalna reedukacja ryzyka kosztowna, możemy chcieć je zaakceptować.
3. **Przekazanie ryzyka**
   Może mieć formę ubezpieczenia od ryzyka (postać znana np. w przypadku ubezpieczenia nieruchomości od zdarzeń losowych), ale również outsourcingu, czyli ryzyko przekazuję do innej firmy, a odpowiedzialność za nie zawieram w odpowiednich zapisach umownych.
4. **Uniknięcie ryzyka**
   Jeśli ryzyko jest duże, a system, w którym ono występuje, nie przynosi im odpowiednich korzyści, być może najkorzystniejszym rozwiązaniem będzie w ogóle zrezygnowanie z eksploatacji danego systemu (a zarazem uniknięcie ryzyka).

VI. PONOWNE PRZEPROWADZENIE ANALIZY RYZYKA

Przynajmniej raz w roku należy dokonać weryfikacji aktualności i adekwatności przeprowadzonej analizy ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmujących działań minimalizujących to ryzyko. Ponadto analiza ta powinna być przeglądana każdorazowo w sytuacjach gdy następują zmiany w zasobie informacyjnym Urzędu. Każdorazowo za zainicjowanie i skuteczne przeprowadzenie procesu klasyfikacji informacji oraz analizy i oceny ryzyka odpowiedzialny jest Sekretarz Gminy. W procesie przeprowadzenia oceny biorą udział również właściciele odpowiednich zidentyfikowanych grup informacji.

Biuro projektu: DG PMC Sp. z o.o.
Ul. Tylne Chwaliszewo 25, 61-103 Poznań
tel. (61) 839 90 24, fax (61) 839 92 97
email: pmc@dgpmc.pl, www.dgpmc.pl

Projekt jest współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego

Załącznik Nr 1 do Instrukcji podstawowych zasad bezpieczeństwa w UM w Krobi

INSTRUKCJA ZARZĄDZANIA STACJAMI ROBOCZYMI W URZĘDZIE MIEJSKIM W KROBI

PRZEDMIOT INSTRUKCJI

Przedmiotem instrukcji jest uregulowanie zasad przygotowania sprzętu komputerowego, kontroli zmian w infrastrukturze, dystrybuowanie poprawek i baz definicji antywirusowych dla stacji roboczych.

ZAKRES INSTRUKCJI

Stacje robocze wykorzystywane dla celów Urzędu Miejskiego w Krobi.

SPOSÓB POSTĘPOWANIA

1. Proces przydzielania stacji roboczej użytkownikowi

O przydzieleniu użytkownikowi stacji roboczej decyduje Sekretarz Gminy , w porozumieniu z Informatykiem.

2. Zasady instalowania i aktualizacji oprogramowania

Każda stacja robocza oddawana jest do użytkowania z podstawowym oprogramowaniem:

- System Operacyjny Microsoft Windows,
- Microsoft Word lub OpenOffice Writer,
- Microsoft Excel lub OpenOffice Calc,
- Acrobat Reader,
- Program Antywirusowy

Jeżeli istnieje potrzeba instalacji na danej stacji roboczej oprogramowania dziedzinowego to administrator danego systemu instaluje na stacji roboczej niezbędne oprogramowanie. Zgodę na instalację takiego oprogramowania udziela Informatyk. Każde zainstalowane oprogramowanie powinno zostać wpisane na „Kartę Sprzętu" danej stacji roboczej (Załącznik nr 1).

3. Aktualizacje oprogramowania

a) antywirusowego - powinny odbywać się automatycznie. Poprawki mogą być pobierane z wewnętrznego serwera bądź bezpośrednio z odpowiednich serwerów producenta danego systemu antywirusowego,
b) systemu operacyjnego – powinny być pobierane automatycznie i informować użytkownika stacji roboczej o możliwości uaktualnienia systemu. Użytkownik powinien móc sam zaktualizować system na stacji roboczej,
c) oprogramowania dziedzinowego – powinny odbywać się w przypadku pojawienia się jego nowych wersji. Aktualizacji dokonuje administrator danego oprogramowania dziedzinowego.

4. Licencje na oprogramowanie

Administrator każdego z systemów informatycznych zobowiązany jest to utrzymywania dokumentacji, dzięki której jest w stanie na bieżąco kontrolować zgodność ilości zainstalowanego oprogramowania z posiadanymi licencjami.

5. Zasady modyfikacji podzespołów w stacjach roboczych

Modyfikacji podzespołów w stacjach roboczych dokonuje osoba odpowiedzialna za serwis sprzętu za zgodą Informatyka, na wniosek Sekretarza Gminy w którym dana stacja robocza jest użytkowana. Każda modyfikacja powinna zostać wpisana na „Kartę Sprzętu" danej stacji roboczej (Załącznik nr 1).

Załącznik nr 1

Biuro projektu: DG PMC Sp. z o.o.
Ul. Tylne Chwaliszewo 25, 61-103 Poznań
tel. (61) 839 90 24, fax (61) 839 92 97
email: pmc@dgpmc.pl, www.dgpmc.pl

Projekt jest współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego

Karta Sprzętu *sporządzona:* ……	
Nazwa [Producent/Model]	
Numer fabryczny	
Numer inwentarzowy	
Osoba odpowiedzialna	
Osoba użytkująca	
Lokalizacja [Pokój]	
Wydział	
Grupa własna [Komputer, monitor, drukarka, itd.]	
Podstawowe paramerty:	Procesor:..... Pamięć:..... HDD:..... Napęd zewnętrzny:..... Inne:..... .

Biuro projektu: DG PMC Sp. z o.o.
Ul. Tylne Chwaliszewo 25, 61-103 Poznań
tel. (61) 839 90 24, fax (61) 839 92 97
email: pmc@dgpmc.pl, www.dgpmc.pl

Projekt jest współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego

Oprogramowanie podstawowe:	**System Operacyjny:** ☐ Windows 98 ☐ Windows 2000 ☐ Windows XP Professional ☐ Windows 2003 Server ☐ Windows Vista ☐ Windows NT ☐ Windows 7 ☐ Windows 8 **Pakiet Biurowy:** ☐ MS Office XP ☐ MS Office 2003 ☐ MS Office 2007 ☐ MS Office 2010 ☐ MS Office 2013 ☐ OpenOffice **Inne:** ☐ Acrobat Reader ☐ Antyvirus:.....
Oprogramowanie dziedzinowe:	

Biuro projektu: DG PMC Sp. z o.o.
Ul. Tylne Chwaliszewo 25, 61-103 Poznań
tel. (61) 839 90 24, fax (61) 839 92 97
email: pmc@dgpmc.pl, www.dgpmc.pl

Projekt jest współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego

Lp	Data przeglądu oprogramowania	Uwagi
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		
13		
14		
15		
16		
17		
18		
19		
20		
20		
21		
22		
23		

Biuro projektu: DG PMC Sp. z o.o.
Ul. Tylne Chwaliszewo 25, 61-103 Poznań
tel. (61) 839 90 24, fax (61) 839 92 97
email: pmc@dgpmc.pl, www.dgpmc.pl

Projekt jest współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego

Załącznik Nr 2 do Instrukcji podstawowych zasad bezpieczeństwa w UM w Krobi

INSTRUKCJA ZBYWANIA I PRZEKAZYWANIA SPRZĘTU WYKORZYSTYWANEGO DO PRZETWARZANIA INFORMACJI W URZĘDZIE MIEJSKIM W KROBI

PRZEDMIOT INSTRUKCJI

Przedmiotem instrukcji jest ustalenie zasad postępowania ze sprzętem komputerowym w okoliczności:

1. użyczenia sprzętu komputerowego na zewnątrz na czas określony lub zmianą pracownika
2. przekazania sprzętu komputerowego na zewnątrz bez obowiązku zwrotu
3. wydania sprzętu komputerowego do naprawy
4. przeznaczenia do likwidacji.

ZAKRES INSTRUKCJI

Instrukcja dotyczy komputerów wyposażonych w dysk twardy.

SPOSÓB POSTĘPOWANIA

Użyczenie sprzętu komputerowego na zewnątrz na czas określony lub zmiana pracownika.

1. Dane zawarte na dysku twardym komputera administrator systemu informatycznego przegrywa na serwer lub klasyfikuje do skasowania.
2. Informatyk kasuje zawartość dysku odpowiednim oprogramowaniem, a w przypadku zmiany pracownika usuwa dane.
3. Informatyk przygotowuje komputer do wydania zgodnie z uzyskaną zgodą.
4. Informatyk wydaje sprzęt komputerowy po otrzymaniu podpisanego przez obie strony protokołu użyczenia.
5. Po zwrocie komputera z użyczenia Informatyk kasuje dysk twardy.

Przekazanie sprzętu komputerowego na zewnątrz bez obowiązku zwrotu

1. Dane zawarte na dysku twardym administrator systemu informatycznego przegrywa na serwer lub klasyfikuje do kasacji.
2. Informatyk kasuje zawartość dysku twardego dedykowanym oprogramowaniem.
3. Informatyk wydaje sprzęt komputerowy po otrzymaniu podpisanego przez obie strony protokołu darowizny lub przekazania.

Wydanie sprzętu komputerowego do naprawy serwisowej dotyczące komputera

Biuro projektu: DG PMC Sp. z o.o.
Ul. Tylne Chwaliszewo 25, 61-103 Poznań
tel. (61) 839 90 24, fax (61) 839 92 97
email: pmc@dgpmc.pl, www.dgpmc.pl

Projekt jest współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego

posiadającego pamięć masową

Wydanie sprzętu komputerowego do naprawy serwisowej dotyczy:

A. Awaria serwera:

1. w przypadku konieczności naprawy serwera poza siedzibą Urzędu należy zdemontować dyski twarde przed wydaniem go do serwisu,
2. na czas naprawy dyski twarde należy przechowywać w szafie pancernej opisane numerem inwentarzowym serwera.
3. w przypadku uszkodzeniu dysków twardych serwera należy je w miarę możliwości skasować, a następnie przekazać do likwidacji.

B. Awaria stacji roboczej lub notebooka:

1. W przypadku naprawy poza siedzibą Urzędu należy zdemontować dyski twarde przed wydaniem urządzenia do serwisu.
2. W przypadku niemożliwości demontażu dysku należy od firmy serwisowej uzyskać zobowiązanie o zachowaniu danych w poufności zgodnie z załącznikiem nr 1.

Przeznaczanie do likwidacji

1. Dysk twardy przeznaczony do likwidacji należy oznaczyć numerem inwentarzowym zgodnym z numerem inwentarzowym komputera, z którego został wymontowany.
2. Dane zawarte na dysku twardym administrator systemu informatycznego przegrywa na serwer lub klasyfikuje do kasacji.
3. Pracownik zajmujący się serwisem sprzętu komputerowego kasuje zawartość dysku twardego.
4. Dyski twarde przeznaczone do likwidacji przechowuje się w szafie pancernej.
5. Po przeprowadzonej likwidacji dysków twardych przed ich wydaniem do utylizacji należy zniszczyć je fizycznie w obecności Administratora Systemu Informatycznego, Administratora Bezpieczeństwa Informacji oraz Przewodniczącego komisji likwidacyjnej.
6. Przewodniczący komisji likwidacyjnej odnotowuje ten fakt w swojej dokumentacji.

Biuro projektu: DG PMC Sp. z o.o.
Ul. Tylne Chwaliszewo 25, 61-103 Poznań
tel. (61) 839 90 24, fax (61) 839 92 97
email: pmc@dgpmc.pl, www.dgpmc.pl

Projekt jest współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego

Załącznik nr 1

Oświadczenie o zachowaniu danych w poufności

Urząd Miejski w Krobi

.....
nazwa firmy

.....
adres firmy

Do zlecenie usługi nr: /

Nazwa sprzętu:	nr inwentarzowy	Opis uszkodzenia

Przedstawiciel (firmy)
wykonał na miejscu / pobrał sprzęt do naprawy w dniu: ..... r

Zobowiązujemy się w imieniu firmy którą reprezentuję do zachowania w tajemnicy wszystkich danych i informacji uzyskanych podczas naprawy zgodnie z obowiązującymi przepisami o ochronie danych osobowych oraz innymi tajemnicami prawnie chronionymi.

.....
imię, nazwisko, pieczęć, podpis

---

zwrot sprzętu z naprawy nastąpił w dniu (data i podpis): ..... r

Biuro projektu: DG PMC Sp. z o.o.
Ul. Tylne Chwaliszewo 25, 61-103 Poznań
tel. (61) 839 90 24, fax (61) 839 92 97
email: pmc@dgpmc.pl, www.dgpmc.pl

Projekt jest współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego

Załącznik Nr 3 do Instrukcji podstawowych zasad bezpieczeństwa w UM w Krobi

PZRYKAŁADY ZAPISÓW W UMOWACH W ZAKRESIE BEZPIECZEŃSTWA INFORMACJI W URZĘDZIE MIEJSKIM W KROBI

USTAWA O DOSTĘPIE DO INFORMACJI PUBLICZNEJ

Na podstawie art. 5 i art. 22 Ustawy o dostępie do informacji publicznej.

PRZYKŁAD 1

1. Wykonawca zobowiązuje się do nieograniczonej w czasie: ochrony i zachowania w ścisłej tajemnicy wszelkich informacji dotyczących Zamawiającego uzyskanych w trakcie współpracy niezależnie od formy przekazania tych informacji i ich źródła.
2. Ujawnienie informacji, o których mowa w punkcie 1 możliwe jest wyłącznie przy każdorazowym uzyskaniu pisemnej zgody Zamawiającego.
3. Zapisy ust. 1 oraz ust.2 powyżej, nie dotyczą informacji:

a) które znajdowały się w nieograniczonym posiadaniu Stron/Strony przed ich otrzymaniem od drugiej Strony;
b) które są powszechnie znane lub zostaną podane przez Zamawiającego do wiadomości publicznej;
c) które Strona/Strony mogła otrzymać od strony trzeciej bez powiadomienia o towarzyszących ograniczeniach co do ich użycia lub ujawniania;
d) co do których dana Strona jest w stanie udowodnić, że te informacje zostały przez nią opracowane niezależnie od ich otrzymania.

4. Wykonawca zobowiązuje się podjąć wszelkie niezbędne kroki dla zapewnienia, że żadna z osób otrzymujących informacje wrażliwe nie ujawni tych informacji, ani ich źródła, zarówno w całości, jak i w części osobom trzecim bez uzyskania uprzednio wyraźnego upoważnienia na piśmie od Zamawiającego.
5. Wykonawca zobowiązuje się ujawniać informacje jedynie tym pracownikom, którym będą one niezbędne do wykonywania powierzonych im czynności i tylko w zakresie, w jakim odbiorca informacji musi mieć do nich dostęp dla celów realizacji zadań wynikających z przedmiotu Umowy.
6. Każdy z pracowników wykonawcy uczestniczący w realizacji umowy zobowiązany jest do podpisania zobowiązania o zachowaniu poufności informacji Zamawiającego.
7. Wykonawca zobowiązuje się nie kopiować, nie powielać ani w jakikolwiek sposób nie rozpowszechniać jakiejkolwiek części określonych informacji z wyjątkiem uzasadnionej potrzeby do celów związanych z zakresem współpracy, po uprzednim uzyskaniu pisemnej zgody od Zamawiającego.

Biuro projektu: DG PMC Sp. z o.o.
Ul. Tylne Chwaliszewo 25, 61-103 Poznań
tel. (61) 839 90 24, fax (61) 839 92 97
email: pmc@dgpmc.pl, www.dgpmc.pl

Projekt jest współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego

8. Zobowiązanie do poufności trwa nadal pomimo rozwiązania lub wygaśnięcia Umowy. Strony odpowiadają za zachowanie poufności przez swoich pracowników, pełnomocników oraz osób działających w ich imieniu.
9. Wykonawca na pisemne wezwanie wystosowane przez Zamawiającego, zobowiązuje się do niezwłocznego zwrotu wszystkich informacji utrwalonych w formie pisanej, oraz ich kopii i usunięcia informacji w formie elektronicznej
10. Wszystkie osoby uczestniczące w realizacji Umowy z ramienia Wykonawcy będą zobowiązane do podpisania „Zobowiązania do zachowania tajemnicy", której treść stanowi Załącznik do Umowy.

PRZYKŁAD 2

1. Strony Umowy zobowiązują się, że wszelkie dane i informacje uzyskane w związku z wykonywaniem niniejszej umowy na temat stanu, organizacji i interesów drugiej strony nie zostaną ujawnione, udostępnione lub upublicznione ani w części, ani w całości bez pisemnej zgody drugiej strony, o ile nie wynika to z niniejszej Umowy lub nie służy jej realizacji.

PRZYKLADOWA TRESC ZOBOWIAZANIA DO ZACHOWANIA TAJEMNICY

Ja, ...nr PESEL ..... w związku z wykonywaniem powierzonych mi zadań, zobowiązuję się do zachowania w tajemnicy wszelkich informacji, z którymi zapoznam się w trakcie wykonywania zadań na rzecz Urzędu Miejskiego w Krobi, chyba że informacje te są lub staną się powszechnie dostępne bez mojego udziału.
Oświadczam również, że poniosę wobec Urzędu Miejskiego w Krobi pełną odpowiedzialność (w tym finansową) w przypadku naruszenia niniejszego zobowiązania.
Oświadczam ponadto, że jest mi znana treść i rozumiem znaczenie art. 266 § 1 kodeksu karnego, zgodnie z którym: „Kto wbrew przepisom ustawy lub przyjętemu na siebie zobowiązaniu ujawnia lub wykorzystuje informację, z którą zapoznał się w związku z pełnioną funkcją, wykonywaną pracą, działalnością publiczną, społeczną, gospodarczą lub naukową, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2".

Biuro projektu: DG PMC Sp. z o.o.
Ul. Tylne Chwaliszewo 25, 61-103 Poznań
tel. (61) 839 90 24, fax (61) 839 92 97
email: pmc@dgpmc.pl, www.dgpmc.pl

Projekt jest współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego

USTAWA O OCHRONIE DANYCH OSOBOWYCH
Na podstawie art. 31 Ustawy (Dz. U. z 2014r. poz. 1182 ze zm.)

POWIERZENIE PRZETWARZANIA DANYCH OSOBOWYCH

1. Niniejszą umową Urząd Miejski w Krobi powierza: ..... przetwarzanie danych osobowych znajdujących się w zbiorach danych osobowych Urzędu: .....,a ....., zwany dalej Wykonawcą, zobowiązuje się do przetwarzania tych danych osobowych, wyłącznie w następującym zakresie i celu:.....
2. Wykonawca niniejszym oświadcza, że przed rozpoczęciem przetwarzania danych osobowych, o których mowa w pkt 1 niniejszej umowy, podjął środki zabezpieczające zbiory danych Urzędu Miejskiego w Krobi, o których mowa w art. 36-39 Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014r. poz. 1182 ze zm.) oraz spełnił wymagania określone w przepisach Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. Nr 100, poz. 1024).
3. Wykonawca niniejszym oświadcza, że dane osobowe, o których mowa w pkt 1 niniejszej umowy, są w szczególności zabezpieczone przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem w/w. ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.
4. Wykonawca będzie realizował wszelkie zobowiązania wynikające z postanowień niniejszej umowy samodzielnie, bez udziału podwykonawców oraz jakichkolwiek osób trzecich, z zastrzeżeniem postanowień pkt 5 niniejszej umowy.
5. Do wykonywania zobowiązań wynikających z postanowień niniejszej umowy mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez Wykonawcę, za działania i zaniechania, których Wykonawca ponosi odpowiedzialność.
6. Wykonawca zobowiązuje się do prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych, która powinna zawierać:
   imię i nazwisko osoby upoważnionej,
   datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych,
   identyfikator, jeżeli dane są przetwarzane w systemie informatycznym.
   W tym celu Wykonawca wyznaczy osobę administrującą w/w. ewidencją.
7. Wykonawca zobowiązuje się do odnotowywania, w formie dziennika, wszelkich informacji na temat dostępu do zbioru danych osobowych Urzędu Miejskiego w Krobi, w szczególności daty i zakresu dostępu oraz osoby mającej taki dostęp z jej własnoręcznym

podpisem. W tym celu Wykonawca wyznaczy osobę administrującą w/w dziennikiem.

8. Wykonawca zobowiązuje się do wykonania wszelkich niezbędnych działań, aby osoby, które zostaną upoważnione do przetwarzania danych osobowych oraz osoby administrujące ewidencją, o której mowa w pkt 6, oraz dziennikiem, o którym mowa w pkt 7, zachowały w tajemnicy te dane osobowe oraz sposoby ich zabezpieczenia, także po wygaśnięciu zawartych z tymi osobami umów o pracę oraz innych tytułów kształtujących stosunek pracy, jak również wszelkich innych umów, porozumień i tytułów, na podstawie których osoby te świadczyły usługi na rzecz Wykonawcy.
9. Urząd Miejski w Krobi zastrzega sobie prawo kontroli Wykonawcy co do poprawności procesu przetwarzania danych osobowych w zakresie i celach przewidzianych postanowieniami niniejszej umowy.
10. W sprawach nieuregulowanych niniejszą umową stosuje się przepisy Kodeksu cywilnego, Ustawy z dnia 27 lipca 2001r. o ochronie baz danych oraz Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych oraz rozporządzeń wydanych na podstawie powyższych ustaw.

USTAWA O PRAWIE AUTORSKIM I PRAWACH POKREWNYCH
Dz. U. 2006 r. Nr 90 poz. 631 z późn. zm.

Wykonawca udzieli Zamawiającemu prawa do korzystania – licencji, w rozumieniu Ustawy z dnia 24 lutego 1994r. o prawie autorskim i prawach pokrewnych, z dokumentacji powstałej w wyniku realizacji umowy.
Licencja zostanie udzielona na czas nieokreślony.
Zamawiający wymaga, aby udzielona licencja obejmowała prawa do dokumentacji papierowej i elektronicznej na następujących polach eksploatacji: modyfikowanie, kopiowanie, przetwarzanie, utrwalanie na nośnikach elektronicznych i papierowych, publikowanie, opracowywanie szkoleń i prezentacji.
Wykonawca przeniesie na Zamawiającego autorskie prawa majątkowe dla .....

Załącznik Nr 4 do
Instrukcji
podstawowych zasad
bezpieczeństwa w UM
w Krobi

Urząd Miejski w Krobi

Procedura zarządzania kluczami do pomieszczeń Urzędu

Logo	**Procedura zarządzania kluczami do pomieszczeń Urzędu** *tytuł dokumentu / procedury*	**Wersja: 1**

OPRACOWAŁ		**SPRAWDZIŁ**		**ZATWIERDZIŁ**	
referat / stanowisko		*referat / stanowisko*		**Wójt/Burmistrz/Prezydent**	
Imię i nazwisko:		Imię i nazwisko:		**ZARZĄDZENIE** *Dokument*	
Podpis:		Podpis:		Nr:	
Data:		Data:		Z dnia:	

Obowiązuje od dnia:	Poziom ochrony: II
Wycofano dnia:	

SPIS TREŚCI

1. Cel procedury

Celem procedury jest określenie zasad postępowania z kluczami do pomieszczeń Urzędu.

2. Obszar zastosowania

Zarządzanie kluczami do pomieszczeń Urzędu.

3. Odpowiedzialność

Pracownik Biura Obsługi Klienta

4. Sposób postępowania

1. Klucze do pomieszczeń zlokalizowanych w budynku Urzędu Miejskiego w Krobi , wydaje pracownik Biura Obsługi Klienta , na podstawie listy osób uprawnionych do pobrania kluczy z konkretnego pokoju, aktualizowanej w miarę potrzeby raz na kwartał .
2. W budynku Urzędu Miejskiego w Krobi klucze do poszczególnych pomieszczeń znajdują się w szafce w pomieszczeniu Biura Obsługi Klienta .
3. Pobranie kluczy jest odnotowywane w dzienniku "Ewidencja wydawania i przyjęcia kluczy" poprzez wpisanie numeru pokoju do którego pobierany jest klucz i złożenie podpisu przez osobę uprawnioną do jego pobrania. Sprawdzenie tożsamości osoby pobierającej klucz wymagane jest jedynie w sytuacji, kiedy nie jest ona znana pracownikowi ochrony.
4. Okresowa weryfikacja uprawnień dostępu do pomieszczeń Urzędu przeprowadzana będzie raz na kwartał przez Sekretarza Gminy.
5. Pracownik opuszczający pomieszczenie jako ostatni zobowiązany jest do zamknięcia pomieszczenia na klucz. W przypadku, gdy pomieszczenie współdzielone jest pomiędzy kilku pracowników, a pracownik zamykający pomieszczenie pozostaje na terenie budynku Urzędu, powinien on poinformować, gdzie przebywa, osoby z pokoju obok.
6. Zakazuje się dorabiania kluczy do pomieszczeń Urzędu na własny użytek.
7. Komplet zapasowych kluczy do wszystkich pomieszczeń znajduje się w zamykanej kasetce, która znajduje się w zamykanej szafie osoby odpowiedzialnej za przechowywanie powyższych kluczy, tj. Pracownika Biura Obsługi Klienta Urzędu Miejskiego w Krobi.

5. Przypadki szczególne

W przypadku powstania sytuacji alarmowej nie unormowanej niniejszą procedurą lub dokumentem wymienionym w niniejszej procedurze pracownicy zobowiązani są do niezwłocznego kontaktu Burmistrzem lub Sekretarzem Gminy.

Załącznik:
Rejestr kluczy oraz rejestr kluczy zapasowych.