Zarządzenie NR OR.0050.41.2016
Burmistrza Miasta Łaskarzew
z dnia 30 września 2016 roku

w sprawie wprowadzenia Polityki bezpieczeństwa informacji w Urzędzie Miasta Łaskarzew

Na podstawie art. 30 ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz.U. z 2016 r. poz. 446 z późn. zm.) oraz art. 36 ust. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2015 r. poz. 2135 ze zm.) oraz § 5 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku 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. z 2004 r. Nr 100 poz. 1024) zarządzam co następuje:

§ 1

Wprowadzam Politykę bezpieczeństwa informacji w Urzędzie Miasta Łaskarzew stanowiącą załącznik nr 1 do niniejszego zarządzenia.

§ 2

Wykonanie zarządzenia powierza się Administratorowi Bezpieczeństwa Informacji.

§ 3

Traci moc Zarządzenie Nr OR.0050.44.2013 Burmistrza Miasta Łaskarzew z dnia 12 grudnia 2013 r. w sprawie wprowadzenia i wdrożenia do stosowania Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych oraz Polityki bezpieczeństwa danych osobowych.

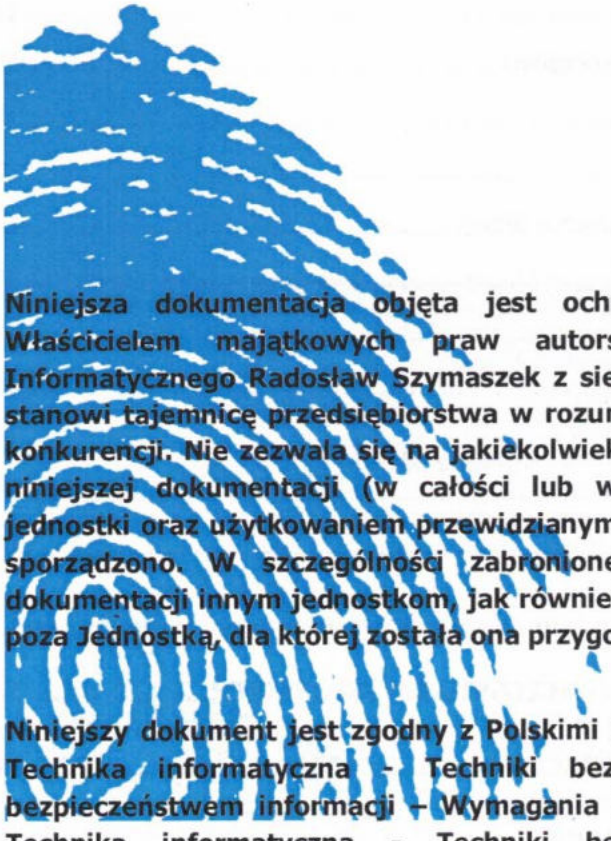
§ 4

Zarządzenie wchodzi w życie z dniem podjęcia.

Burmistrz Miasta Łaskarzew
mgr Lidia Sopel-Sereja

Załącznik nr 1
do Zarządzenia NR OR.0050.41.2016
Burmistrza Miasta Łaskarzew
z dnia 30 września 2016 roku

Polityka Bezpieczeństwa Informacji



Niniejsza dokumentacja objęta jest ochroną wynikającą z praw autorskich. Właścicielem majątkowych praw autorskich jest Centrum Bezpieczeństwa Informatycznego Radosław Szymaszek z siedzibą w Krasnymstawie. Dokumentacja stanowi tajemnicę przedsiębiorstwa w rozumieniu ustawy o zwalczeniu nieuczciwej konkurencji. Nie zezwala się na jakiekolwiek powielanie, zmiany, czy wykorzystanie niniejszej dokumentacji (w całości lub w części), poza dozwolonym użytkiem jednostki oraz użytkowaniem przewidzianym do celów, dla których dokumentację tę sporządzono. W szczególności zabronione jest ujawnianie całości czy części dokumentacji innym jednostkom, jak również wdrażanie zawartych w niej rozwiązań poza Jednostką, dla której została ona przygotowana.

Niniejszy dokument jest zgodny z Polskimi Normami PN – ISO / IEC 27001 : 2014 Technika informatyczna - Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji – Wymagania oraz PN – ISO / IEC 27002 : 2014-12 Technika informatyczna - Techniki bezpieczeństwa – Praktyczne zasady zabezpieczania informacji oraz Ustawą o ochronie danych osobowych z dnia 29 sierpnia 1997r. (tekst jednolity: Dz. U. 2014 r. poz.1182)

212

Spis treści

1 POSTANOWIENIA OGÓLNE 8

1.1 Informacje wstępne 8

1.2 Opis organizacji 8

1.3 Misja Jednostki 8

1.4 Kontekst wewnętrzny funkcjonowania Jednostki 9

Ogólny profil 9

Struktura organizacyjna 9

Obowiązki jednostki 9

Zasoby i wiedza - Aktywa 11

Kompetencje pracowników 11

Procesy podejmowania decyzji (wykaz procesów) 12

Przepływ informacji 12

Normy etyczne 12

Forma i zakres relacji zawartych w umowach o pracę. 13

1.5 KONTEKST ZEWNĘTRZNY 13

Środowisko zewnętrzne 13

Trendy mające wpływ na cele: 13

Relacje z zewnętrznymi interesariuszami 14

1.6 Podstawy prawne 14

1.7 Ochrona danych osobowych 16

2 DEFINICJE 25

3 ZAKRES SYSTEMU ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI 32

4 DEKLARACJA NAJWYŻSZEGO KIEROWNICTWA 34

5 POLITYKI BEZPIECZEŃSTWA INFORMACJI 35

5.1 Kierunki bezpieczeństwa informacji określone przez kierownictwo 35

6 ORGANIZACJA BEZPIECZEŃSTWA INFORMACJI 37

6.1 Organizacja wewnętrzna 37

Role i odpowiedzialność za bezpieczeństwo informacji 37

213

Administrator Bezpieczeństwa Informacji (ABI) 38
Administrator Systemu Informatycznego 40
Zespół ds. Bezpieczeństwa Informacji, Ciągłości Działania i Zarządzania Incydentami (Zespół ds. Bezpieczeństwa) 42
Pracownicy Jednostki 44
Osoby trzecie 45
6.2 Rozdzielenie obowiązków 45
6.3 Kontakty z organami władzy 45
6.4 Bezpieczeństwo informacji w zarządzaniu projektami 46
6.5 Urządzenia mobilne i telepraca 46
Polityka stosowania urządzeń mobilnych 46
Telepraca 47
7 BEZPIECZEŃSTWO ZASOBÓW LUDZKICH 48
7.1 Przed zatrudnieniem 48
Postępowanie sprawdzające 48
Warunki zatrudnienia 48
7.2 Podczas zatrudnienia 48
Odpowiedzialność kierownictwa 48
Uświadamianie, kształcenie i szkolenie z zakresu bezpieczeństwa informacji 49
Postanowienia ogólne 49
Szkolenia wewnętrzne 50
Postępowanie dyscyplinarne 50
7.3 Zakończenie zatrudnienia lub zmiana zakresu obowiązków 51
8 ZARZĄDZANIE AKTYWAMI 52
8.1 Odpowiedzialność za aktywa 52
Inwentaryzacja aktywów 52
Własność aktywów 52
Akceptowalne użycie aktywów 52
Zwrot aktywów 53
8.2 Klasyfikacja informacji 53
Klasyfikowanie informacji 53

Oznaczanie informacji 54
Postępowanie z aktywami 54
8.3 Postępowanie z nośnikami 54
Zarządzanie nośnikami wymiennymi 54
Wycofywanie nośników 54
Przekazywanie nośników 54
ROZPOWSZECHNIENIE I ZARZĄDZANIE DOKUMENTEM POLITYKI 55
9 KONTROLA DOSTĘPU 56
9.1 Wymagania biznesowe wobec kontroli dostępu 56
Polityka kontroli dostępu 56
Dostęp do sieci i usług sieciowych 57
9.2 Zarządzanie dostępem użytkowników 57
Rejestrowanie i wyrejestrowanie użytkowników i przydzielanie praw dostępu 57
Przydzielanie dostępu użytkownikom 58
Zarządzanie prawami uprzywilejowanego dostępu 59
Zarządzanie poufnymi informacjami uwierzytelniającymi użytkowników 59
Przegląd praw dostępu użytkowników 59
Odbieranie lub dostosowanie dostępu 60
9.3 Odpowiedzialność użytkowników 61
Stosowanie poufnych informacji uwierzytelniających 61
9.4 Kontrola i ograniczenie dostępu do systemów i aplikacji 61
Procedury bezpiecznego logowania 61
System zarządzania hasłami 61
Użycie uprzywilejowanych programów narzędziowych 62
Kontrola dostępu do kodów źródłowych programów 62
10 KRYPTOGRAFIA 63
10.1 Zabezpieczenia kryptograficzne 63
Polityka stosowania zabezpieczeń kryptograficznych 63
Zarządzanie kluczami 63
11 BEZPIECZEŃSTWO FIZYCZNE I ŚRODOWISKOWE 64
11.1 Obszary bezpieczne, fizyczne wejście, biura, pomieszczenia i obiekty 64

215

Fizyczna granica obszaru bezpiecznego 64
Fizyczne zabezpieczenia wejść 65
Zabezpieczenie biur, pomieszczeń i obiektów 65
Zabezpieczenie serwerowni 65
Ochrona przed zagrożeniami zewnętrznymi i środowiskowymi 65
Praca w obszarach bezpiecznych 66
Obszary dostaw i załadunku 66
11.2 Sprzęt 66
Lokalizacja i ochrona sprzętu 66
Systemy wspomagające zabezpieczania/awarie zasilania 66
Bezpieczeństwo okablowania 67
Bezpieczne zbywanie lub przekazywanie do ponownego użycia 67
Pozostawianie sprzętu użytkownika bez opieki 67
Dobre praktyki dotyczące bezpieczeństwa informacji: Polityka „czystego biurka" i polityka „czystego ekranu" 68
12 BEZPIECZNA EKSPLOATACJA 69
12.1 Procedury eksploatacyjne, odpowiedzialność i dokumentowanie procedur 69
Dokumentowanie procedur eksploatacyjnych 69
Zarządzanie zmianami 70
Zarządzanie pojemnością 70
Oddzielanie środowisk rozwojowych, testowych i produkcyjnych 70
12.2 Ochrona przed szkodliwym oprogramowaniem 70
12.3 Kopie zapasowe 71
Likwidacja nośników zawierających kopie 71
Przechowywanie elektronicznych nośników informacji zawierających dane osobowe 71
12.4 Rejestrowanie zdarzeń i monitorowanie oraz rejestrowanie działań administratorów i operatorów 72
Rejestrowanie zdarzeń 72
Synchronizacja zegarów 73
12.5 Nadzór i instalacja oprogramowania produkcyjnego 73
Instalacja oprogramowania w systemach produkcyjnych 73
12.6 Zarządzanie podatnościami technicznymi 74

216

Ograniczenia w instalowaniu oprogramowania 74

12.7 Audyty systemów informacyjnych 75

13 BEZPIECZEŃSTWO KOMUNIKACJI 76

13.1 Zarządzanie bezpieczeństwem sieci 76

13.2 Przesyłanie informacji 76

14 POZYSKIWANIE, ROZWÓJ I UTRZYMANIE SYSTEMÓW 79

14.1 Wymagania bezpieczeństwa systemów informacyjnych 79

Analiza i specyfikacja wymagań bezpieczeństwa informacji 79

Zabezpieczanie usług aplikacyjnych w sieciach publicznych 80

Ochrona transakcji usług aplikacyjnych 80

14.2 Bezpieczeństwo w procesach rozwoju i wsparcia 81

Polityka bezpieczeństwa prac rozwojowych 81

Zasady projektowania bezpiecznych systemów 82

14.3 Dane testowe 83

15 RELACJE Z DOSTAWCAMI 84

15.1 Bezpieczeństwo w porozumieniach z dostawcami 84

16 ZARZĄDZANIE INCYDENTAMI ORAZ UDOSKONALENIAMI 85

16.1 Odpowiedzialność i procedury 85

16.2 Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji 85

17 Aspekty bezpieczeństwa informacji w zarządzaniu ciągłością działania 89

17.1 Ciągłość w bezpieczeństwie informacji 89

18 ZGODNOŚĆ 91

18.1 Zgodność z przepisami prawa 91

Postanowienia ogólne 91

Przeglądy zgodności zasobów 91

Postępowanie w przypadku wykrycia niezgodności 91

Niezależny przegląd bezpieczeństwa informacji 92

Zgodność z politykami bezpieczeństwa i standardami 92

Sprawdzanie zgodności technicznej 92

19 Wykaz załączników 93

1 POSTANOWIENIA OGÓLNE

1.1 Informacje wstępne

Polityka bezpieczeństwa informacji jest dokumentem wewnętrznym **UrzęduMiasta Łaskarzew**(dalej w treści dokumentu zwany „jednostką") i jest objęta obowiązkiem zachowania w poufności przez wszystkie osoby, którym zostanie ujawniona.

Każda osoba mająca dostęp do informacji zobowiązana jest zapoznać się z niniejszym dokumentem oraz złożyć stosowne oświadczenie, potwierdzające znajomość jego treści.

Właścicielem dokumentu Polityki Bezpieczeństwa Informacji jest Burmistrz.

1.2 Opis organizacji

Urząd jest jednostką działającą na podstawie przepisów prawa, realizującą zadania własne i zlecone.

1.3 Misja Jednostki

Misją Jednostki jest realizacja zadań publicznych, wynikających z przepisów ustaw oraz aktów wykonawczych. Nadto, zadaniem podmiotu jest budowanie wizerunku nowoczesnej administracji publicznej poprzez skuteczną i zgodnąz przepisami prawa obsługę interesantów w sposób: profesjonalny, nowoczesny
i przyjazny, przy jednoczesnym dążeniu do zapewnienia wysokiej jakości obsługi.

Ochrona informacji jest jednym z kluczowych obowiązków Jednostki. Dlatego też szczególną wagę ona przykłada do następujących zasad:

1. W zakresie bezpieczeństwa precyzyjnie określa odpowiedni podział odpowiedzialności.
2. Ryzyko utraty bezpieczeństwa informacji traktuje jako stały element funkcjonowania i zarządza tym ryzykiem, co oznacza prowadzenie

regularnych audytów bezpieczeństwa informacji, ocenę ryzyka, analizę zagrożeń i skutków, ustalenie odpowiedniego postępowania i stałego nadzoru.

3. Za główny cel systemu zarządzania bezpieczeństwem informacji stawia zapobieganie zagrożeniom naruszeń bezpieczeństwa informacji, a nie likwidowanie ich skutków.
4. Jednostka stosuje różnorodne narzędzia zapewniające bezpieczeństwa informacji. Od organizacyjnych – procedury, zakresy odpowiedzialności, szkolenia – po czysto techniczne.
5. Informacja, zarówno ta która jest własnością Jednostki, jak i informacja którą interesanci jej powierzają, jest chroniona skuteczniej dzięki wdrożonemu Systemowi Zarządzania Bezpieczeństwem Informacji (dalej: SZBI).

1.4 Kontekst wewnętrzny funkcjonowania Jednostki

Ogólny profil

Gmina jest jednostką samorządu terytorialnego posiadającą osobowość prawną, przy pomocy której Burmistrz – będący organem wykonawczym Gminy– wykonuje swoje zadania. Gmina działa w ramach szeroko pojętego prawa publicznego.

Struktura organizacyjna

Struktura organizacyjna Jednostkiwynika z Regulaminu Organizacyjnego.

Obowiązki jednostki

Obowiązki jednostki podzielone są na dwie zasadnicze grupy, tj. obowiązki ogólne jednostki oraz obowiązki szczegółowe, przypisane do konkretnych stanowisk. Literalne i szczegółowe wyliczenie zakresu obowiązków jednostki wynikaz Regulaminu Organizacyjnego.

Ogólne zadania Jednostki:

Do obowiązków Jednostki należy zaspokajanie zbiorowych potrzeb wspólnoty należy do zadań własnych gminy. W szczególności zadania własne obejmują sprawy:

1) ładu przestrzennego, gospodarki nieruchomościami, ochrony środowiska i przyrody oraz gospodarki wodnej;

2) gminnych dróg, ulic, mostów, placów oraz organizacji ruchu drogowego;

3) wodociągów i zaopatrzenia w wodę, kanalizacji, usuwania i oczyszczania ścieków komunalnych, utrzymania czystości i porządku oraz urządzeń sanitarnych, wysypisk i unieszkodliwiania odpadów komunalnych, zaopatrzenia w energię elektryczną i cieplną oraz gaz;

3a) działalności w zakresie telekomunikacji;

4) lokalnego transportu zbiorowego;

5) ochrony zdrowia;

6) pomocy społecznej, w tym ośrodków i zakładów opiekuńczych;

6a) wspierania rodziny i systemu pieczy zastępczej;

7) gminnego budownictwa mieszkaniowego;

8) edukacji publicznej;

9) kultury, w tym bibliotek gminnych i innych instytucji kultury oraz ochrony zabytków i opieki nad zabytkami;

10) kultury fizycznej i turystyki, w tym terenów rekreacyjnych i urządzeń sportowych;

11) targowisk i hal targowych;

12) zieleni gminnej i zadrzewień;

13) cmentarzy gminnych;

14) porządku publicznego i bezpieczeństwa obywateli oraz ochrony przeciwpożarowej i przeciwpowodziowej, w tym wyposażenia i utrzymania gminnego magazynu przeciwpowodziowego;

15) utrzymania gminnych obiektów i urządzeń użyteczności publicznej oraz obiektów administracyjnych;

16) polityki prorodzinnej, w tym zapewnienia kobietom w ciąży opieki socjalnej, medycznej i prawnej;

17) wspierania i upowszechniania idei samorządowej, w tym tworzenia warunków do działania i rozwoju jednostek pomocniczych i wdrażania programów pobudzania aktywności obywatelskiej;

18) promocji gminy;

19) współpracy i działalności na rzecz organizacji pozarządowych oraz podmiotów wymienionych w art 3 ust. 3 ustawy z dnia 24 kwietnia 2003 r. o działalności pożytku publicznego i o wolontariacie (Dz. U. z 2010 r. Nr 234, poz. 1536, z późn. zm.);

20) współpracy ze społecznościami lokalnymi i regionalnymi innych państw.

Zasoby i wiedza - Aktywa

Aktywami jednostki, tj. wszystkim tym, co stanowi dla niej wartość z punktu widzenia bezpieczeństwa danych osobowych a w szczególności zbiory danych osobowych stanowi**załącznik nr 1: Rejestr aktywów-wykaz i struktura zbiorów danych osobowych.**

Kompetencje pracowników

Pracownicy posiadają wymagane kwalifikacje i kompetencje dla realizacji zadań, wynikających z przepisów ustaw oraz innych przepisów wykonawczych.

212

Powyższe pozwala jednocześnie prowadzić bieżącą obsługę administracyjną petentów. Pracownicy są systematycznie szkoleni dla zapewnienia odpowiednich kwalifikacji oraz doskonalenia posiadanych umiejętności zawodowych i indywidualnych.

Procesy podejmowania decyzji (wykaz procesów)

Wszelkie formy aktywności jednostki (wydane decyzje administracyjne, postanowienia, czy inne akty administracyjne) wydawane są w imieniu Burmistrza.

Do załatwiania spraw, w których Burmistrz– jako kierownik jednostki – nie bierze udziału osobiście, właściwym jest umocowany pracownik, posiadający stosowne upoważnienie.

Przepływ informacji

Komunikacja w Jednostce pomiędzy kierownictwem i pracownikami odbywa się na zasadach opisanych w Regulaminie Organizacyjnym, którzy wykonują je za pomocą podległych sobie zastępców i innych pracowników.

Wszyscy pracownicy zobowiązani są do wzajemnej współpracy w zakresie realizowanych zadań. Jednym z elementów współpracy są spotkania, podczas których przekazywane są informacje o planach, realizowanych zadaniach, sposobach i terminach ich realizacji oraz informacje dotyczące spraw bieżących i organizacyjnych.

Normy etyczne

Relacje służbowe opierają się na współpracy, koleżeństwie, wzajemnym szacunku, pomocy oraz dzieleniu się doświadczeniami i wiedzą. Pracownik wykonuje zadania sumienni i sprawnie, wykorzystując w pełni posiadaną wiedzę i doświadczenie. Swoje decyzjei ustalenia opiera na ustalonej prawdzie obiektywnej. Informacje uzyskane w wyniku prowadzonych czynności pracownik wykorzystuje wyłącznie do celów służbowych.

Forma i zakres relacji zawartych w umowach o pracę.

Kryteria stosowane wobec kandydata do pracy:

a) wykształcenie;
b) wiedza specjalistyczna;
c) doświadczenie zawodowe w pracy na stanowisku urzędniczym;
d) umiejętność pracy na dokumentach oraz obsługi urządzeń technicznych i oprogramowania – w tym: obsługi programów prawniczych;
e) dokładność oraz staranność;
f) rzetelność;
g) komunikatywność;
h) otwartość w podejściu do petentów;
i) umiejętność wykonywania poleceń służbowych przełożonych;
j) umiejętność logicznego myślenia;
k) kreatywność.

1.5 KONTEKST ZEWNĘTRZNY

Środowisko zewnętrzne

Miasto Łaskarzew położone jest w województwie mazowieckim, w powiecie garwolińskim.Leży nad rzeką Promnik, prawym dopływem Wisły.

Trendy mające wpływ na cele:

a) zwiększająca się świadomość prawna społeczeństwa oraz istota bezpieczeństwa informacji, stanowiąca dla wielu mieszkańców rodzaj dobra osobistego, podlegającego ochronie;
b) zmieniające się przepisy prawne, stawiające coraz większe wymagania zakresie bezpieczeństwa informacji;
c) planowane zmiany i rosnące zagrożenia związane z bezpieczeństwem informacji, zwłaszcza w kontekście rozwoju technicznego i technologicznego;

224

d) monopol na obsługę administracyjną w zakresie zadań przypisanych Jednostce.

Relacje z zewnętrznymi interesariuszami

Budowa trwałych relacji na płaszczyźnie Jednostka – interesant (petent, klient),polega na dostosowywaniu poziomu usług administracji do potrzeb, wymagań i oczekiwań interesantów, poprzez uwzględnienie priorytetów. Potwierdzeniem zadowolenia klientów z realizowanych usług administracyjnych jest zmniejszająca się liczba skarg na działalnie Jednostki, jako organuadministracji publicznej.

1.6 Podstawy prawne

Polityka Bezpieczeństwa Informacji oraz inne dokumenty szczegółowe związane z bezpieczeństwem informacji są zgodne z obowiązującymi w tym zakresie z aktami prawnymi.

Do tworzenia i rozwijania Systemu Zarządzania Bezpieczeństwem Informacji stosowane będą wymagania:

1. Polskiej Normy PN – ISO / IEC 27001 : 2014 Technika informatyczna - Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji –Wymagania;
2. oraz wytyczne Polskiej Normy PN – ISO / IEC 27002 : 2014 Technika informatyczna -Techniki bezpieczeństwa – Praktyczne zasady zarządzania bezpieczeństwem informacji.
3. Ustawie z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t. j. Dz. U. z 2013 r. poz. 235, z późn. zm.);
4. Rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2012r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej

225

oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2012 r. poz.526);

5. Ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz. U. 2014 r. poz.1182);
6. Rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. 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);
7. Rozporządzeniu Prezydenta Rzeczpospolitej Polskiej z dnia 3 listopada 2006 r. w sprawie nadania statutu Biuru Generalnego Inspektora Ochrony Danych Osobowych (Dz. U. z 2006 r. Nr 203, poz. 1494)-art. 13.3 ustawy;
8. Rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 22 kwietnia 2004r. w sprawie wzoru imiennego upoważnienia i legitymacji służbowej inspektora Biura Generalnego Inspektora Ochrony Danych Osobowych (Dz. U. z 2004 r, Nr 94, poz. 923)-art. 22a ustawy;
9. Rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. 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. z 2004 r. Nr 100, poz. 1024)-art. 39 a ustawy;
10. Rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 11 grudnia 2008w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz. U. z 2008 r., Nr 229, poz. 1536)-art. 46a ustaw;
11. Rozporządzeniu Ministra Administracji i Cyfryzacji z dnia 10 grudnia 2014 roku w sprawie wzorów zgłoszeń powołania i odwołania administratora bezpieczeństwa informacji.

1.7 Ochrona danych osobowych

Przetwarzanie danych

Przetwarzanie danych jest dopuszczalne tylko wtedy gdy (art. 23.1 ustawy o ochronie danych osobowych):

1) Osoba, której dane dotyczą, wyrazi na to zgodę, chyba że chodzi o usunięcie dotyczących jej danych. Zgoda może obejmować również przetwarzanie danych w przyszłości, jeżeli nie zmienia się cel przetwarzania. Zgoda nie może być domniemana lub dorozumiana. Jeżeli przetwarzanie danych jest niezbędne dla ochrony żywotnych interesów osoby, której dane dotyczą, a uzyskanie zgody nie jest możliwe, można przetwarzać dane bez zgody tej osoby, do czasu, gdy uzyskanie zgody będzie możliwe,

2) Jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisów prawa,

3) Jest to konieczne dla realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą,

4) Jest to niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego.

5) Jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez Administratora Danych albo odbiorców danych, a przetwarzanie danych nie narusza praw i wolności osoby, której dane dotyczą. Za prawnie usprawiedliwiony cel uważa się w szczególności; marketing bezpośredni produktów lub usług administratora danych oraz dochodzenie roszczeń z tytułu prowadzonej działalności gospodarczej.

Przetwarzanie danych jest zabronione w przypadku danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym. Przetwarzanie tych danych jest jednak dopuszczalne, jeżeli:

1) Osoba, której dane dotyczą, wyrazi na to zgodę na piśmie, chyba że chodzi
o usunięcie dotyczących jej danych,

2) Przepis szczególny innej ustawy zezwala na przetwarzanie takich danych bez zgody osoby, której dane dotyczą i stwarza pełne gwarancje ich ochrony,

3) Przetwarzanie takich danych jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą lub innej osoby, gdy osoba, której dane dotyczą, nie jest fizycznie lub prawnie zdolna do wyrażenia zgody, do czasu ustanowienia opiekuna prawnego lub kuratora,

4) Jest to niezbędne do wykonania statutowych zadań kościołów i innych związków wyznaniowych, stowarzyszeń, fundacji lub innych niezarobkowych organizacji lub instytucji o celach politycznych, naukowych, religijnych, filozoficznych lub związkowych, pod warunkiem, że przetwarzanie danych dotyczy wyłącznie członków tych organizacji lub instytucji albo osób utrzymujących z nimi stałe kontakty w związku z działalnością i zapewnione są pełne gwarancje ich ochrony,

5) Przetwarzanie dotyczy danych, które są niezbędne do dochodzenia praw przed sądem,

6) Przetwarzanie jest niezbędne do wykonania zadań administratora danych odnoszących się do zatrudnienia pracowników i innych osób, a zakres przetwarzanych danych jest określony w ustawie,

7) Przetwarzanie jest prowadzone w celu ochrony stanu zdrowia, świadczenia usług medycznych lub leczenia pacjentów przez osoby trudniące się zawodowo leczeniem lub świadczeniem innych usług medycznych, zarządzania udzieleniem usług medycznych i są stworzone pełne gwarancje ochrony danych osobowych.

8) Przetwarzanie dotyczy danych, które zostały podane do wiadomości publicznej przez osobę, której dane dotyczą,

9) Jest to niezbędne do prowadzenia badań naukowych, w tym do przygotowania rozprawy wymaganej do uzyskania dyplomu ukończenia szkoły wyższej lub stopnia naukowego, publikowanie wyników badań naukowych nie może następować w sposób umożliwiający identyfikację osób, których dane zostały przetworzone,

10) Przetwarzanie danych jest prowadzone przez stronę w celu realizacji praw i obowiązków wynikających z orzeczenia wydanego w postępowaniu sądowym lub administracyjnym.

Obowiązki informacyjne przy przetwarzaniu danych

W przypadku zbierania danych od osoby, której dane dotyczą Administrator Danych jest zobowiązany poinformować tę osobę o:

1) Adresie swojej siedziby i pełnej nazwie, a w przypadku gdy Administratorem Danych jest osoba fizyczna- o miejscu swojego zamieszkania oraz imieniu i nazwisku,

2) Celu zbierania danych, a w szczególności o znanych mu w czasie

229

udzielania informacji lub przewidywanych odbiorach lub kategoriach odbiorców danych,

3) Prawie dostępu do treści swoich danych oraz ich poprawiania,

4) Dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.

Podanych wyżej zasad nie stosuje się, jeżeli przepis innej ustawy zezwala na przetwarzanie danych bez ujawniania faktycznego celu ich zbierania lub jeżeli osoba, której dane dotyczą, posiada już te informacje.

W przypadku zbierania danych nie od osoby, której te dane dotyczą Administrator Danych jest zobowiązany poinformować tę osobę bezpośrednio po utrwaleniu danych o:

1) Adresie swojej siedziby i pełnej nazwie, a w przypadku gdy Administratorem Danych jest osoba fizyczna- o miejscu swojego zamieszkania oraz imieniu i nazwisku,

2) Celu i zakresie zbierania danych , a w szczególności o odbiorach lub kategoriach odbiorców danych,

3) Źródle danych,

4) Prawie dostępu do treści swoich danych oraz ich poprawiania,

5) Prawie wniesienia, pisemnego, umotywowanego żądania zaprzestania przetwarzania jej danych ze względu na jej szczególną sytuację,

6) Prawie wniesienia sprzeciwu wobec przetwarzania jej danych w przypadku gdy, Administrator Danych zamierza je przetwarzać w celach marketingowych lub wobec przekazywania jej danych osobowych innemu administratorowi danych.

Wymienionych zasad nie stosuje się, jeżeli:

1) Dane są przetwarzane przez administratora na podstawie przepisów prawa,

2) Przepis innej ustawy przewiduje lub dopuszcza zbieranie danych osobowych bez wiedzy osoby, której dane dotyczą,

3) Dane te są niezbędne do badań naukowych, dydaktycznych, historycznych, statystycznych lub badania opinii publicznej, ich przetwarzanie nie narusza praw lub wolności osoby której dane dotyczą, a spełnienie obowiązku informacyjnego wymagałoby nadmiernych nakładów lub zagrażałoby realizacji celu badania.

Upoważnienia do przetwarzania danych osobowych

1. Każdy pracownik przetwarzający dane osobowe powinien zostać upoważniony na piśmie do ich przetwarzania przez Administratora Danych Osobowych, zgodnie z art. 37 uodo. Wzór upoważnienia stanowi załącznik nr 14 do niniejszej Polityki.
2. W przypadku zmiany stanowiska, bądź zakresu obowiązków pracowniczych, przyjęcia do pracy nowego pracownika lub stażysty, lub w sytuacji, która wpływa bezpośrednio na rodzaj i zakres przetwarzanych danych osobowych, Administrator Danych Osobowych zobowiązany jest wydać nowe lub cofnąć upoważnienie.
3. Administrator Danych Osobowych nadaje upoważnienia na czas określony.

Ewidencja osób upoważnionych

Zgodnie z art. 39 ustawy o ochronie danych osobowych wprowadza się ewidencję osób upoważnionych do przetwarzania danych, która stanowi załącznik nr 16 do niniejszej Polityki.

231

1) Administrator Danych Osobowych lub wyznaczony pracownik prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych zgodnie z art. 39 ustawy o ochronie danych osobowych

2) Ewidencja, o której mowa w pkt 1 powinna zawierać

   a) Imię i nazwisko osoby upoważnionej

   b) Datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych

   c) Identyfikator, jeżeli dane przetwarzane są w systemie informatycznym

Osoba upoważniona do przetwarzania danych osobowych

Osoba upoważniona do przetwarzania danych osobowych jest zobowiązana przestrzegać następujących zasad:

1) przetwarza dane osobowe wyłącznie w zakresie ustalonym indywidualnie przez Administratora Danych w upoważnieniu i tylko w celu wykonywania nałożonych na nią obowiązków. Zakres dostępu do danych przypisany jest do niepowtarzalnego identyfikatora użytkownika, niezbędnego do rozpoczęcia pracy w systemie. Rozwiązanie stosunku pracy, odwołanie z pełnionej funkcji powoduje wygaśnięcie upoważnienia do przetwarzania danych osobowych;

2) pracownik musi zachować tajemnicę danych osobowych oraz przestrzegać procedur ich bezpiecznego przetwarzania. Przestrzeganie tajemnicy danych osobowych obowiązuje przez cały okres zatrudnienia u Administratora Danych, a także po ustaniu stosunku pracy lub odwołaniu z pełnionej funkcji;

3) stosuje określone przez Administratora Danych oraz Administratora

231

Bezpieczeństwa Informacji procedury oraz wytyczne mające na celu zgodne z prawem, w tym zwłaszcza adekwatne, przetwarzanie danych;

4) korzysta z systemu informatycznego w sposób zgodny ze wskazówkami Administratora Bezpieczeństwa Informacji oraz Administratora Systemu Informatycznego;

5) zabezpiecza dane przed ich udostępnianiem osobom nieupoważnionym.

Powierzenie przetwarzania danych osobowych:

1) Administrator danych osobowych może powierzyć przetwarzanie danych osobowych innemu podmiotowi wyłącznie w drodze umowy zawartej w formie pisemnej.

2) Podmiot, o którym mowa w pkt. 1, jest zobowiązany do zastosowania środków organizacyjnych i technicznych, zabezpieczających zbiór przed dostępem osób nie upoważnionych na zasadach określonych w przepisach ustawy o ochronie danych osobowych.

3) Podmiot, o którym mowa w pkt. 1 jest zobowiązany przetwarzać dane osobowe wyłącznie w zakresie określonym w umowie.

4) W przypadkach opisanych w pkt 1-3 odpowiedzialność za ochronę przetwarzanych danych osobowych spoczywa na Administratorze Danych Osobowych, co nie wyłącza odpowiedzialności podmiotu, z którym z zawarto umowę z tytułu przetwarzania danych niezgodnie z ustawą.

5) Przy kontroli zgodności przetwarzanych danych przez upoważniony, przez Administratora Danych Osobowych podmiot, o którym mowa w pkt 1 stosuje się odpowiednio przepisy art. 14 – 19 ustawy o ochronie danych osobowych.

235

Rejestracja zbiorów danych osobowych:

1) Rejestr zbiorów danych składa się z wykazu zbiorów danych osobowych przetwarzanych w jednostce, zawierającego odrębnie dla każdego zbioru danych informacje określone w Załącznik nr 17 do niniejszej Polityki.

2) Rejestr prowadzony jest w postaci elektronicznej i papierowej.

3) Za prowadzenie rejestru zgodnie z obowiązującymi przepisami i jego aktualizację odpowiada powołany przez Administratora Danych Osobowych – Administrator Bezpieczeństwa Informacji.

4) Administrator bezpieczeństwa informacji w ramach prowadzenia rejestru dokonuje:

    a. Wpisania zbioru danych w przypadku rozpoczęcia przetwarzania w nim danych osobowych.

    b. Aktualizacji informacji dotyczących zbioru danych w przypadku zmiany informacji objętych wpisem.

    c. Wykreślenia zbioru danych, w przypadku zaprzestania przetwarzania w nim danych osobowych.

5) Wpisu do rejestru dokonuje się niezwłocznie po zaistnieniu zdarzenia, o którym mowa w pkt 4 pkt a powodującego obowiązek dokonania wpisu.

6) W rejestrze prowadzi się wykaz zmian, który zawiera:

    a. Wskazanie rodzaju zmiany (nowy wpis, aktualizacja, wykreślenie)

    b. Datę dokonania zmiany

    c. Zakres zmiany

Powyższy rejestr jest prowadzony w przypadku gdy Administrator Danych Osobowych powołał i zgłosił do rejestracji Generalnego Inspektora Ochrony Danych Osobowych - Administratora Bezpieczeństwa Informacji .

235

2 DEFINICJE

1. **Akceptowanie ryzyka** – ogłoszona decyzja o podjęciu określonego *ryzyko*;
2. **Analiza ryzyka** – proces dążący do poznania charakteru *ryzyka* oraz określenia *poziomu ryzyka*;
3. **Atak** – próba zniszczenia, ujawnienia, zmiany, uniemożliwienia dostępu, kradzieży lub uzyskania nieautoryzowanego dostępu albo nieautoryzowanego użycia aktywów;
4. **Atrybut** – cecha lub właściwość *obiektu*, która może być rozróżniana ilościowo lub jakościowo przez człowieka lub automatycznie;
5. **Audyt** – systematyczny, niezależny i udokumentowany *proces* uzyskiwania dowoduz audytu oraz jego obiektywnej oceny w celu określenia stopnia spełnienia kryteriów audytu;
6. **Autentyczność –** właściwość, która polega na tym, że podmiot jest tym, za kogo się podaje;
7. **Bezpieczeństwo informacji** – zachowanie *poufności*, *integralności* i *dostępności* informacji;
8. **Cel** – to co ma być osiągnięte;
9. **Cel przeglądu** – stwierdzenie opisujące to, co ma być osiągnięte w wyniku przeglądu;
10. **Cel stosowania zabezpieczenia** – deklaracja opisująca co ma być rezultatem wdrożenia *zabezpieczenia;*
11. **Ciągłe doskonalenie** – powtarzane działanie mające na celu poprawę *wyniku* działania;
12. **Ciągłość bezpieczeństwa informacji** – procesy i procedury zapewniające ciągłość *bezpieczeństwa informacji*;
13. **Dane** – zbiór wartości przypisanych do miar podstawowych, miar złożonych i/lub wskaźników;

14. **Dostępność** – właściwość bycia dostępnym i użytecznym na żądanie autoryzowanego podmiotu;
15. **Działanie korygujące** – działanie w celu wyeliminowania przyczyny niezgodności
    i zapobieżenie powtórzeniu;
16. **Funkcja pomiaru** – algorytm lub obliczenie wykonane w celu połączenia dwóch lub więcej *miar podstawowych*;
17. **Identyfikowanie ryzyka** – proces wyszukiwania, rozpoznawania i opisywania *ryzyka;*
18. **Incydenty związane z bezpieczeństwem informacji** – pojedyncze niepożądane lub niespodziewane *zdarzenie związane z bezpieczeństwem informacji* lub seria takich zdarzeń, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają *bezpieczeństwu informacji*;
19. **Informowanie o ryzyku i konsultowanie ryzyka** – ciągłe i prowadzone w sposób iteracyjny procesy, które są przez organizację prowadzone w celu zapewnienia, przekazywania lub uzyskania informacji, jak również w celu porozumiewania sięz *interesariuszami*, odnoszące się do zarządzania *ryzykiem;*
20. **Integralność** – właściwość polegająca na zapewnieniu dokładności i kompletności;
21. **Interesariusz** – osoba lub organizacja, która może wpływać, podlega wpływowi lub postrzega siebie jako podlegającą wpływowi decyzji lub działalności;
22. **Jednostka pomiaru** – szczególna ilość, określona i przyjęta przez konwencję, z którą inne ilości tego samego rodzaju są porównywane w celu wyrażenia ich wielkości w stosunku do tej ilości;
23. **Kierownictwo wykonawcze** – osoba lub grupa osób, na którą *organ nadzorczy* przeniósł odpowiedzialność za realizację strategii i polityki w celu osiągnięcia celu organizacji;

237

24. **Kompetencja** – zdolność stosowania wiedzy i umiejętności w celu osiągnięcia zamierzonych rezultatów;
25. **Kontekst wewnętrzny** – środowisko wewnętrzne, w którym organizacja dąży do osiągnięcia swoich celów;
26. **Kontekst zewnętrzny** – środowisko zewnętrzne, w którym organizacja dąży do osiągnięcia swoich celów;
27. **Kontrola dostępu** – środki mające na celu zapewnienie, że dostęp do aktywów jest autoryzowany i ograniczony w oparciu o wymagania biznesowe i wymagania bezpieczeństwa;
28. **Korekcja** – działanie w celu wyeliminowania wykrytej *niezgodności*;
29. **Kryteria decyzyjne** – progi, cele lub wzory stosowane do określenia potrzeby działań lub dalszych badań, lub opisania poziomu zaufania do otrzymanego rezultatu;
30. **Kryteria ryzyka** – poziomy odniesienia, względem których określa się ważność *ryzyka;*
31. **Metoda pomiaru** – logiczna sekwencja operacji, opisana ogólnie, stosowana do ilościowego wyliczenia atrybutu w stosunku do określonej skali;
32. **Miara** – zmienna, której przypisano wartość w wyniku *pomiaru*;
33. **Miara podstawowa** – *miara* (2.47) zdefiniowana w odniesieniu do *atrybutu* i metody wyznaczenia jego wielkości;
34. **Miara złożona** – *miara*, która jest określana jako funkcja dwóch lub więcej wartości *miar podstawowych*;
35. **Model analityczny** – algorytm lub metoda obliczania, w skład której wchodzi co najmniej jedna *miara podstawowa* i/lub miara złożona ze związanymi kryteriami decyzyjnymi;
36. **Monitorowanie** – określenie statusu systemu, procesu lub działalności;

37. **Nadzór nad bezpieczeństwem informacji** – system za pomocą, którego działania organizacji w zakresie bezpieczeństwa informacji są kierowane i kontrolowane;
38. **Najwyższe kierownictwo** – osoba lub grupa osób, która określa kierunek i steruje *organizacją* na najwyższym poziomie;
39. **Następstwo** – rezultat *zdarzenia* mający wpływ na *cele*;
40. **Niezaprzeczalność** – zdolność do udowodnienia, że wystąpiły deklarowane zdarzenia lub działania oraz że wywołał je dany podmiot;
41. **Niezawodność** – właściwość oznaczająca spójne, zamierzone zachowanie i skutki;
42. **Niezgodność** - niespełnienie *wymagania;*
43. **Obiekt** – element charakteryzowany za pomocą *pomiaruatrybutów* tego elementu;
44. **Obiekt przeglądu** – określony element podlegający przeglądowi;
45. **Ocena ryzyka** – proces porównywania wyników *analizy ryzykaz kryteriami ryzyka*w celu stwierdzenia, czy *ryzyko* i/lub jego wielkość są akceptowalne lub tolerowane;
46. **Organ nadzorujący** – osoba lub grupa osób odpowiedzialnych za wynik działaniai zgodność organizacji;
47. **Organizacja** – osoba lub grupa osób dla której określono funkcje, odpowiedzialność, zwierzchników i relacje, po to, aby osiągnęła ona swoje *cele*;
48. **Podatność** – słabość aktywu lub *zabezpieczenia*, która może być wykorzystana przez co najmniej jedno *zagrożenie*.
49. **Podmiot zapewniający zaufaną wymianę informacji** – autonomiczna organizacja wspierająca wymianę informacji w ramach społeczności współużytkującej informacje ;
50. **Polityka** – zamierzenia i kierunki organizacji formalnie wyrażone przez jego *najwyższe kierownictwo*;
51. **Pomiar** – proces określania wartości;

239

52. **Postępowanie z ryzykiem** – *proces* modyfikowania *ryzyka;*
53. **Potrzeba informacyjna** – zrozumienie konieczne do zarządzania celami, ryzykiemi problemami;
54. **Poufność** – właściwość polegająca na tym, że informacja nie jest udostępniana ani ujawniana nieautoryzowanym osobom, podmiotom lub *procesom;*
55. **Poziom ryzyka** – wielkość *ryzyka* wyrażona w kategoriach kombinacji *następstw* oraz ich *prawdopodobieństw*;
56. **Prawdopodobieństwo** – możliwość wystąpienia zdarzenia;
57. **Proces** – zbiór działań wzajemnie powiązanych lub wzajemnie oddziałujących, które przekształcają wejścia w wyjścia;
58. **Proces zarządzania ryzykiem** – systematyczne stosowanie zasad zarządzania, procedur i praktyk na rzecz działań w zakresie informowania, konsultowania, tworzenia kontekstu oraz identyfikowania, analizy, oceny, postepowania z ryzkiem, monitorowania i przeglądania *ryzyka*;
59. **Projekt SZBI** – działania strukturalne podjęte przez organizację w celu wdrożenia SZBI;
60. **Przegląd** – działanie podejmowane w celu określenia przydatności, adekwatności oraz *skuteczności* w dziedzinie osiągania ustalonych celów;
61. **Ryzyko** – wpływ niepewności na cele;
62. **Ryzyko rezydualne** – *ryzyko* pozostające po zastosowaniu działań określonychw *postępowaniu z ryzykiem*;
63. **Skala** – uporządkowany zbiór wartości, ciągły lub dyskretny, lub zestaw kategorii, do których jest odwzorowywany *atrybut*;
64. **Skuteczność** – stopień, w jakim zaplanowane działania zostały zrealizowanei planowane wyniki osiągnięte;
65. **Standard wdrożenia zabezpieczeń** – dokument określający dopuszczalne sposoby realizacji zabezpieczenia;

66. **Strona zainteresowana** – osoba lub organizacja, która może wpływać, podlega wpływowi lub postrzega siebie jako podlegającą wpływowi decyzji lub działalności;
67. **system informacyjny** – aplikacje, usługi, aktywa technik informacyjnych lub inne komponenty przetwarzające informacje;
68. **System zarządzania** – zbiór wzajemnie powiązanych lub oddziałujących na siebie elementów organizacji powołany w celu ustanowienia *polityk*, *celów* i *procesów* osiągnięcia tych celów;
69. **Szacowanie ryzyka** – całościowy proces identyfikowania ryzyka, analizy ryzyka i oceny ryzyka;
70. **Środek przetwarzania informacji** – każdy system przetwarzania informacji, usługa lub infrastruktura albo ich fizyczna lokalizacja;
71. **Udokumentowana informacja** – informacja, która wymaga kontrolowaniai utrzymywania przez *organizację* oraz nośnik, na którym jest ona zapisana;
72. **Uwierzytelnienie** – pewność, że deklarowana charakterystyka podmiotu jest poprawna;
73. **Walidacja** – potwierdzenia przez przedstawienie dowodu obiektywnego, że zostały spełnione wymagania dotyczące konkretnego zamierzonego użycia lub zastosowania;
74. **Weryfikacja** – potwierdzenie, przez przedstawienie dowodu obiektywnego, że zostały spełnione określone wymagania;
75. **Właściciel ryzyka** – osoba lub podmiot odpowiedzialne za zarządzanie ryzykiemi uprawnione do zarządzania *ryzkiem*;
76. **Wskaźnik** – miara, która zapewnia oszacowanie lub obliczenie określonych *atrybutów* pochodzących z *modelu analitycznego* w odniesieniu do określonych *potrzeb informacyjnych*;
77. **Wspólnota współużytkująca informacje** – grupa organizacji, która uzgodniła wspólny dostęp do informacji;

78. **Wymaganie** – potrzeba lub oczekiwanie, które jest wyrażone, ogólnie rozumiane lub obowiązkowe;
79. **Wynik działania** – mierzalny wynik
80. **Wynik pomiaru** – co najmniej jeden wskaźnik i związane z nim interpretacje, odnoszące się do *potrzeby informacyjnej*;
81. **Zabezpieczenie** – środek, który modyfikuje *ryzyko*;
82. **Zagrożenie** – potencjalna przyczyna niepożądanego incydentu, który może wywołać szkodę w systemie lub organizacji;
83. **Zakres audytu** – obszar i granice *audytu*;
84. **Zarządzanie incydentami związanymi z bezpieczeństwem informacji** – procesy wykrywania, raportowania, szacowania, reagowania, podejmowania akcjii wyciągania wniosków z incydentów związanych z bezpieczeństwem informacji;
85. **Zarządzanie ryzykiem** – skoordynowane działania dotyczące kierowaniai nadzorowania *organizacji* w odniesieniu do *ryzyka*;
86. **Zdarzenie** – wystąpienie lub zmiana konkretnego zestawu okoliczności;
87. **Zdarzenie związane z bezpieczeństwem informacji** – stwierdzone wystąpienie stanu systemu, usługi lub sieci, który wskazuje na możliwe naruszenie polityki bezpieczeństwa informacji lub błąd zabezpieczenia, lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem informacji;
88. **Zgodność** – spełnienie *wymagań*;
89. **Zlecanie na zewnątrz** – realizacja porozumienia, w którym organizacja zewnętrzna wykonuje część funkcji organizacji lub *procesu*;

3 ZAKRES SYSTEMU ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI

Zakres SZBI obejmuje zarządzanie bezpieczeństwem danych osobowych (zwykłych oraz wrażliwych). Z zakresu wyłącza się inne informacje w tym w szczególności informacje niejawne (chronione na podstawie Ustawy z dnia 5 sierpnia 2010r. o ochronie informacji niejawnych).

Polityka Bezpieczeństwa InformacjiJednostki obejmuje wszystkie obszary funkcjonowania, pracowników i podmioty współpracujące, przetwarzające dane osobowe lub mające jakikolwiek z nimi kontakt.

PBI jest integralną częścią System Zarządzania Bezpieczeństwem Informacjii ustanawia zalecenia dotyczące standardów bezpieczeństwa informacji w Jednostce oraz praktyk zarządzania bezpieczeństwem informacji, w tym wyboru, wdrażania i zarządzania zabezpieczeniami z uwzględnieniem środowisk w których w **Jednostce** występują ryzykaw bezpieczeństwie informacji. Umożliwia ona zorganizowane i bezpieczne gromadzenie, przetwarzanie, przesyłanie i przechowywanie informacji, sprawne i kontrolowane jej zarządzanie, a także ochronę i bezpieczeństwo.

Do stosowania zasad określonych przez dokumenty Polityki Bezpieczeństwa Informacji zobowiązani są wszyscy pracownicy Jednostki w rozumieniu przepisów Kodeksu Pracy, oraz inne podmioty prawne mające dostęp do informacji jednostki zgodnie z zobowiązaniami umownymi.Zakres Systemu Zarządzania Bezpieczeństwem Informacji odnosi się w szczególności do:

a) pracowników znajdujących się w strukturze organizacyjnej;
b) dokumentów papierowych i elektronicznych będących własnością jednostki lub petenta Jednostki, o ile zostały przekazane na podstawie przepisów prawnych lub umów;

143

c) sprzętu komputerowego oraz innych nośników danych na których znajdują się informacje podlegające ochronie;

d) technologii służących pozyskiwaniu, selekcjonowaniu, analizowaniu, przetwarzaniu, zarządzaniu i udostępnianiu informacji, do których zalicza się zarówno systemy papierowe jak i elektroniczne wspomagające realizację zadań urzędu.

244

4 DEKLARACJA NAJWYŻSZEGO KIEROWNICTWA

Mając na uwadze misje oraz cele Jednostki Burmistrz i członkowie organów zarządczych ustanawiają Politykę Bezpieczeństwa Informacji oraz zobowiązuje się podejmować wszelkie działania związane z wdrożeniem oraz doskonaleniem Systemu Zarządzania Bezpieczeństwem Informacji.

Burmistrz i członkowie organów zarządczych deklarują zapewnienie optymalnych warunkówi niezbędnych środków finansowych dla realizacji celów zawartych w Polityce Bezpieczeństwa Informacji oraz stałą współpracę z osobami i zespołem powołanymi w celu opracowania, wdrożenia i doskonalenia Systemu Zarządzania Bezpieczeństwem Informacji.

Burmistrz i członkowie organów zarządczych jednocześnie deklaruje chęć dołożenia wszelkich starań w celu:

a) **wdrożenia systemu zarządzania bezpieczeństwem informacji zgodnego z normą PN ISO/IEC 27001:2014, jego utrzymania, eksploatacji i doskonalenia.**
b) **przestrzegania zgodności systemu zarządzania z normą PN ISO/IEC 27001:2014.**

245

5 POLITYKI BEZPIECZEŃSTWA INFORMACJI

5.1 Kierunki bezpieczeństwa informacji określone przez kierownictwo

Celem opracowania dokumentu Polityki Bezpieczeństwa Informacji jest zdefiniowanie ogólnych wymagań i zasad ochrony informacji, które będą fundamentem dla wszystkich dokumentów związanych z bezpieczeństwem informacji oraz dla Systemu Zarządzania Bezpieczeństwem Informacji.

Mając na uwadze fakt, że sprawna realizacja Misji Jednostki oraz zapewnienie zgodności prowadzonych działań z przepisami prawnymi i innymi wymaganiami obowiązującymi jednostkę, zależy od niezakłóconego działania systemów informacyjnych oraz właściwego zabezpieczenia przetwarzanych informacji. Jednostka stawia przed Systemem Zarządzania Bezpieczeństwem Informacji następujące cele:

a) zapewnienie poufności, dostępności i integralności informacji przetwarzanychzgodnie z procedurami oraz odpowiednim i przepisami prawa;
b) zapewnienie ciągłości realizacji Misji poprzez tworzenie, utrzymywanie i testowanie planów zachowania ciągłości działania;
c) zapewnienie zgodności z przepisami prawnymi, wymaganiami kontraktowymi i innymi wymaganiami obowiązującymi a odnoszącymi się do bezpieczeństwa informacji;
d) zidentyfikowanie wszelkich aktywów w rozumieniu systemu zarządzania bezpieczeństwem informacji oraz określenie ich wartości i znaczenia poprzez przeprowadzenie oceny ryzyka, według kryteriów przyjętych w procesie zarządzania ryzykiem, zrozumienie ich podatności oraz zagrożeń, które mogą narazić je na ryzyko;
e) zarządzanie ryzykiem na akceptowalnym poziomie poprzez zaprojektowanie, wdrożenie i utrzymanie formalnego systemu zarządzania;

f) wprowadzenie mechanizmów gwarantujących ochronę zasobów informacyjnych;

g) wdrożenie systemu zarządzania incydentami naruszającymi bezpieczeństwo informacji oraz słabościami systemu;

h) prowadzenie stałych działań zmierzających do poprawy poziomu bezpieczeństwa informacji przetwarzanych w jednostce oraz doskonalenia Systemu Zarządzania Bezpieczeństwem Informacji.

Polityka niniejsza została opracowana dla:

1. Zapewnienia ochrony informacji przed nieupoważnionym dostępem.
2. Zapewnienia poufności, dostępności i integralności informacji przetwarzanychw Jednostce zgodnie z określonymi wymaganiami.
3. Zapewnienia, że eksploatowane przez Jednostkę systemy gwarantują niezaprzeczalność odbioru, niezaprzeczalność nadania oraz rozliczalność zadań.
4. Zapewnienia, że szkolenia z zakresu bezpieczeństwa informacji są zagwarantowane pracownikom.
5. Zapewnienia możliwości rejestracji wszelkiego rodzaju naruszeń bezpieczeństwa informacji.
6. Zapewnienia, że wszelkie naruszenia bezpieczeństwa informacji oraz jego słabe punkty są raportowane i badane a ich ryzyka analizowane i zarządzane.
7. Zapewnienia, że plany zachowania ciągłości działania są tworzone, utrzymywane
   i testowane w stopniu umożliwiającym nieprzerwaną realizację zadań.
8. Wdrożenie niniejszej Polityki Bezpieczeństwa Informacji jest ważne dla wykazania należytej dbałości o poufność, integralność i dostępność informacji podczas kontaktów z klientami oraz instytucjami współpracującymi.

247

6 ORGANIZACJA BEZPIECZEŃSTWA INFORMACJI

6.1 Organizacja wewnętrzna

Role i odpowiedzialność za bezpieczeństwo informacji

Organizacja wewnętrzna Jednostki została zdefiniowana w Regulaminie Organizacyjnym. Do skutecznego zarządzania Systemem Bezpieczeństwa powołano Zespół ds. Bezpieczeństwa Informacji i Ciągłości Działania. Taka struktura zapewnia uwzględnienie wszelkich potrzeb oraz oczekiwań różnych środowisk w organizacji.

Podstawowymi zasadami przy tworzeniu struktur zarządzających bezpieczeństwem są:

a) bezwzględne oddzielenie funkcji zarządzających i kontrolnych od funkcji wykonawczych;
b) uniemożliwienie nadużyć i maksymalne ograniczenie błędów popełnianych przez pojedyncze osoby w ramach ich odpowiedzialności;
c) zapewnienie niezależności i bezinteresowności osób dokonujących audytu bezpieczeństwa przy zapewnieniu gwarancji zachowania tajemnicy.

Burmistrzjest odpowiedzialny za prowadzenie całokształtu spraw związanychz opracowaniem, wdrożeniem i doskonaleniem Systemu Zarządzania Bezpieczeństwem Informacji. Wytycza kierunki zmierzające do zapewnienia odpowiedniej ochrony informacji oraz nadzoruje przestrzeganie zasad wynikających z prawa powszechnego, Regulaminu Organizacyjnego oraz PBI. W tym, realizuje zadania w zakresie zarzadzania bezpieczeństwem informacji takie jak:

a) podejmuje decyzje o celach i środkach bezpieczeństwa przetwarzania informacji z uwzględnieniem przede wszystkim zmian w obowiązującym prawie, organizacji jednostki oraz technik zabezpieczenia informacji;

b) upoważnia poszczególne osoby do przetwarzania danych określonym indywidualnie zakresie, odpowiadającym zakresowi jej obowiązków, **Załącznik nr 14 –Wzór upoważnienia**;
c) odwołuje upoważnienia do przetwarzania danych;
d) na podstawie wydanych upoważnień zobowiązany jest prowadzić ewidencje osób upoważnionych do przetwarzania danych osobowych- **Załącznik nr 16 wzór ewidencji**;
e) powołujeAdministratora Bezpieczeństwa Informacji jako właściwego do prowadzenia dokumentacji z zakresu zarządzania bezpieczeństwem informacji;
f) podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia procedur bezpiecznego przetwarzania informacji;
g) wyznacza Administratora Systemu Informatycznego oraz określa zakres jego zadań i czynności;
h) podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia procedur bezpiecznego przetwarzania danych osobowych;
i) nadzoruje prowadzenie ewidencji i innej dokumentacji z zakresu ochrony danych osobowych.

Administrator Bezpieczeństwa Informacji (ABI)

Administrator Bezpieczeństwa Informacji jest odpowiedzialny za prowadzenie całokształtu spraw związanych z opracowaniem, wdrożeniem i doskonaleniem Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), a w szczególności za:

a) planowanie i koordynowanie działań związanych z opracowaniem, funkcjonowaniemi doskonaleniem Systemu Zarządzania Bezpieczeństwem Informacji;
b) sprawowanie nadzoru merytorycznego nad opracowaniem, wdrażaniemi funkcjonowaniem Systemu Zarządzania Bezpieczeństwem Informacji;

249

c) przygotowanie i aktualizowanie dokumentacji bazowej Systemu Zarządzania Bezpieczeństwem Informacji;
d) ustalanie i wdrażanie procesów wymaganych w Systemie Zarządzania Bezpieczeństwem Informacji;
e) zapewnienie zgodności SZBI z przepisami prawa;
f) zatwierdzanie dokumentów dotyczących zasad ochrony grup informacji, regulaminów, instrukcji,;
g) analiza raportów zdarzeń związanych z bezpieczeństwem informacyjnym;
h) zapewnienie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych(**załącznik nr 4wzórOświadczeniao zaznajomieniu się z dokumentem Polityki bezpieczeństwa informacji**).
i) prowadzenie szkoleń uświadamiających z zakresu bezpieczeństwa informacyjnego dla nowozatrudnionych pracowników oraz szkoleń okresowych dla pozostałych pracowników;
j) sporządzanie rocznego harmonogramu audytów wewnętrznych SZBI;
k) opracowywanie program audytu wewnętrznego SZBI;
l) zatwierdzenie raportu z audytu;
m) inicjonowanie, monitorowanie, weryfikowanie skuteczności oraz prowadzenie rejestru działań korygujących lub zapobiegawczych,
n) opracowywanie okresowych raportów, analiz ze zgłoszonych incydentów lub zdarzeń oraz przedstawianie wniosków do rekomendacji kierownictwu Jednostki;
o) opracowywanie rocznych harmonogramów testowania planów ciągłości działania instytucji;
p) inicjowanie okresowej analizy ryzyka;
q) sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla administratora danych

250

r) prowadzenie rejestru zbiorów danych przetwarzanych przez administratora danych, z wyjątkiem zbiorów, o których mowa w art. 43 ust. 1 u.o.d.o.

Administrator Bezpieczeństwa Informacji po uzgodnieniu Burmistrzem przeprowadza wewnętrzny audyt zgodności przetwarzania danych. Zakres, przebiegi rezultaty audytu dokumentowane są na piśmie w protokole. Burmistrzna wniosek Administratora Bezpieczeństwa Informacji, może zlecić przeprowadzenie audytu zewnętrznego przez wyspecjalizowany podmiot.Administratora Bezpieczeństwa informacji powołuje się na mocy zarządzenia Burmistrza i podlega on organizacyjnie bezpośrednio pod niego.

Administrator Danych Osobowych powołał Administratora Bezpieczeństwa Informacji. Funkcję tę, pełni pracownik firmy zewnętrznej na zasadzie outsourcingu usług.

Administrator Systemu Informatycznego

Administrator Systemu Informatycznego jest odpowiedzialny za nadzorowanie bezpiecznej eksploatacji systemów informatycznych i wspomaganie Burmistrzaoraz Administratora Bezpieczeństwa Informacji w zakresie zarządzania bezpieczeństwem informacji, a w szczególności za:

a) działanie zgodne z obowiązującą Polityką Bezpieczeństwa Informacji;
b) analizowanie tendencji rozwojowych technologii informatycznych i technik bezpieczeństwa, pod kątem podatności, zagrożeń i zabezpieczeń;
c) okresowe raportowanie o stanie bezpieczeństwa systemów teleinformatycznych, odnotowanych incydentach bezpieczeństwa oraz statusie podejmowanych działań w odpowiedzi na incydenty;
d) współdziałanie z Administratorem Bezpieczeństwa Informacji w zakresie opracowywania i wdrażania polityk, procedur i instrukcji;
e) przygotowanie procedur określających zasady zarządzania systemami lokalnymi;

251

f) przygotowanie procedur bezpieczeństwa danego systemu przetwarzania informacji;

g) formułowanie, w uzgodnieniu z Administratorem Danych Osobowych i/lub osobami upoważnionymi przez Administratora Danych Osobowych uprawnień w systemach informatycznych;

h) realizację decyzji Administratora Danych Osobowych dotyczących nadania użytkownikom uprawnień dostępu do danych i wybranych funkcji, w środowisku IT:

-tworzenie kont użytkowników w systemach informatycznych,

-przypisywanie do kont startowych haseł uwierzytelniających użytkowników kont,

-przypisywanie do założonych kont polityk odnośnie jakości haseł i częstotliwości ich zmiany,

-resetowanie utraconych haseł,

-usuwanie kont i uprawnień dla kont osób, które zakończyły pracę w Urzędzie,

-przekazanie ABI informacji sprzętowo-programowych do oceny prawidłowości ich funkcjonowania,

i) monitorowanie stanu środowiska IT, stanu sprzętu IT i wykorzystywanego oprogramowania oraz aktywności sieciowej użytkowników;

j) monitorowanie legalności oprogramowania wykorzystywanego na stacjach roboczych;

k) zapewnienie serwerom i stacjom roboczym niezbędnych licencji programowych;

l) systematyczne aktualizowanie oprogramowania systemowego, aplikacyjnego i ochronnego;

m) udział w pracach Zespołu ds. Bezpieczeństwa Informacji i Ciągłości Działania;

252

n) koordynację działań zapewniających sprawne funkcjonowanie i zabezpieczenie systemów teleinformatycznych przed niepowołanym dostępem;

o) nadzorowanie zgłaszanych incydentów i zdarzeń bezpieczeństwa dotyczących systemów teleinformatycznych;

p) umożliwienie we współpracy z Burmistrzem przeprowadzenia kontroli systemów teleinformatycznych Jednostki przez służby Biura Generalnego Inspektora Danych Osobowych;

q) zapewnienie, że do informacji chronionych mają dostęp wyłącznie osoby upoważnione i że mogą one wykonywać wyłącznie uprawnione operacje;

r) kontrolę procesu przyznawania praw dostępu;

s) przeciwdziałanie próbom naruszenia bezpieczeństwa informacji;

t) nadzór nad wykonywaniem napraw, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe, nad wykonywaniem kopii zabezpieczających, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu informatycznego;

u) szczegółowa politykę wykonywanych kopii zapasowych;

v) działania służące zapewnieniu niezawodności zasilania komputerów, innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych oraz zapewnieniu bezpiecznej wymiany danych w sieci wewnętrznej i bezpiecznej teletransmisji;

w) inwentaryzację sprzętu komputerowego i oprogramowania

x) współtworzenie analizy ryzyka dla systemu informatycznego.

Zespół ds. Bezpieczeństwa Informacji, Ciągłości Działania i Zarządzania Incydentami (Zespół ds. Bezpieczeństwa)

Skład Zespołu powołany jest zarządzeniem Burmistrza.Zespół ds. Bezpieczeństwa jest odpowiedzialny za inicjowanie i wspieranie wszelkich działań związanych z bezpieczeństwem informacji w Jednostce, a w szczególności za:

153

a) opiniowanie dokumentów SZBI, w tym Polityki Bezpieczeństwa Informacji, polityk niższego rzędu, metodyk, procedur, instrukcji;
b) uzgadnianie podziału odpowiedzialności w zakresie bezpieczeństwa informacji ciągłości działania;
c) wspieranie procesów zarządzania ryzykiem, w tym analizy ryzyka, monitorowania zmian stopnia narażenia zasobów na podstawowe zagrożenia;
d) okresową analizę danych na temat naruszeń bezpieczeństwa informacji i ciągłości działania oraz monitorowanie naruszeń bezpieczeństwa informacji i ciągłości działania;
e) analizę, ocenę i opiniowanie projektów zmierzających do podniesienia poziomu bezpieczeństwa informacji i ciągłości działania (działań korygujących i zapobiegawczych);
f) dobór zabezpieczeń;
g) koordynację procesów doskonalenia SZBI, w tym wdrażania określonych zabezpieczeń w systemach lub usługach;
h) zabezpieczanie realizacji jednolitej Polityki Bezpieczeństwa Informacji;
i) zgłaszanie do Administratora Bezpieczeństwa Informacji poprawek i aktualizacji do opracowanych dokumentów SZBI, w tym do Polityki Bezpieczeństwa Informacji;
j) wspieranie inicjatyw dotyczących propagowania tematyki bezpieczeństwa informacji i ciągłości działania w całej jednostce;
k) wspieranie Burmistrzaw planowaniu budżetu zapewniającego prawidłowe funkcjonowanie SZBI w jednostce;
l) przeciwdziałanie próbom naruszenia bezpieczeństwa informacji i ciągłości działania;
m) zarządzanie ciągłością działania (budowa świadomości pracowników o wadze zarządzania ciągłością działania).

254

Pracownicy Jednostki

Każdy z pracowników Jednostki jest odpowiedzialny za sprawne funkcjonowanie SZBI zgodnie z przydzielonymi mu obowiązkami na podstawie Regulaminu Organizacyjnego i zakresu obowiązków wynikających z umowy o pracę.

Dodatkowo pracownicy są odpowiedzialni za realizację zadań służbowych w zgodziez wymaganiami stawianymi przez system SZBI, a w szczególności za:

a) stosowanie się do obowiązującej Polityki Bezpieczeństwa Informacji, oraz uzupełniającymi je dokumentami;
b) zachowanie w poufności wszelkich informacji do których mają dostęp (**załącznik nr 5 wzórOświadczenia o zachowaniu poufności informacji**).
c) zgłaszanie wszelkich przypadków działań niezgodnych z politykami i regulaminami, mogących być zdarzeniami lub incydentami bezpieczeństwa;
d) zgłaszanie przełożonemu konieczności/propozycji zmian w dokumencie (procesie, procedurze, zarządzeniu, itp.) lub uwag do opracowywanego dokumentu;
e) ochronę identyfikatorów osobistych (loginów do systemów/aplikacji) oraz haseł przed ujawnieniem;
f) uczestnictwo w organizowanych przez Jednostkę szkoleniach z zakresu bezpieczeństwa informacji;
g) przeciwdziałanie próbom naruszenia bezpieczeństwa informacji;
h) raportowanie incydentów związanych z bezpieczeństwem oraz wszelkich zidentyfikowanych słabych punktów SZBI.

Wszelkie celowe działania zagrażające bezpieczeństwu informacji, która jest własnością Jednostkę lub instytucji z nim współpracujących podlegają stosownym konsekwencjom dyscyplinarnym i/lub prawnym.

255

Osoby trzecie

Przed uzyskaniem dostępu do informacji każda osoba trzecia, musi podpisać zobowiązanie do ochrony informacji(**Załącznik nr 5 wzór Oświadczenia o zachowaniu poufności informacji; por. wyżej**)w trybie art. 266 § KK; 267 § KK; 268 § KK, 269 § KK i zapisów ustawy o zwalczaniu nieuczciwej konkurencji z dnia 16 kwietnia 1993 r. (Dz. U. z 2003 r., Nr 153, poz. 1503, z późn. zm.) oraz Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz. U. 2014 r. poz.1182) oraz:

a) zapoznać się z Polityką Bezpieczeństwa Informacji oraz podpisać zobowiązanie o jej przestrzeganiu;
b) stosować się do obowiązującej Polityki Bezpieczeństwa Informacji oraz uzupełniających ją innych dokumentów, jeśli takowe mają zastosowanie;
c) zgłaszać wszelkich przypadków działań niezgodnych z politykami i regulaminami, mogących być zdarzeniami lub incydentami bezpieczeństwa;
d) przeciwdziałać próbom naruszenia bezpieczeństwa informacji.

6.2 Rozdzielenie obowiązków

Obowiązki i odpowiedzialność za bezpieczeństwo informacji zostały przypisane osobom w zakresie niepowodującym konfliktu z wykonywanymi czynnościami w innym zakresie.

6.3 Kontakty z organami władzy

Kontakty z właściwymi organami władzy są utrzymywane w formie i zakresie określonym stosownymi przepisami prawa powszechnego. Z uwzględnieniem zasad:

1. Za kontakty z organami regulacyjnymi i normalizacyjnymi oraz organami nadzorującymi odpowiedzialny jest Burmistrzoraz Administrator Bezpieczeństwa Informacji.

256

2. Za kontakty z organami ścigania odpowiedzialna jest każda osoba która zauważy naruszenie prawa.
3. Za kontakty z innymi organami władzy odpowiedzialni są pracownicy Jednostki zgodnie z ich obowiązkami zawartymi w umowie o pracę, regulaminie organizacyjnym, Polityki bezpieczeństwa oraz innych wewnętrznych dokumentów.

Kontakty z grupami zainteresowanych specjalistów są utrzymywane poprzez udziałw spotkaniach studialnych, forach i konferencjach o tematyce dotyczącej bezpieczeństwa informacji.

6.4 Bezpieczeństwo informacji w zarządzaniu projektami

Jednostka deklaruje stosowanie wysokich standardów bezpieczeństwa informacji podczas stosowania metodyk zarządzania projektami. Na powyższe metodyki nakładane są normy zarządzania bezpieczeństwem informacji zgodnie ze stosowanymi zabezpieczeniami opisanymi w niniejszej dokumentacji.

6.5 Urządzenia mobilne i telepraca

Polityka stosowania urządzeń mobilnych

Jednostka dba i kontroluje korzystanie z urządzeń mobilnych w sposób bezpieczny.

W pierwszej kolejności zapewnienia ochronę urządzeń z zastosowaniem środków technicznychi organizacyjnych adekwatnych do zagrożeń i podatności oraz potencjalnych strat, jakie Jednostka poniesie w razie naruszenia bezpieczeństwa. Do najistotniejszych czynności, które wykonywane są w Jednostce należą:

a) aktualizacja polityki bezpieczeństwa o zapisy dotyczące urządzeń mobilnych;
b) wdrożenie centralnego systemu zarządzania urządzeniami mobilnymi (m.in. aktualizacja urządzeń, kontrola aplikacji i działań użytkowników, śledzenie i zdalne usuwanie danych);

257

c) wdrożenie lokalnych zabezpieczeń na urządzeniach mobilnych (m.in. kontrola dostępu, VPN, szyfrowanie).

Telepraca

W celu ochrony informacji pobieranych, przetwarzanych i przechowywanych
w miejscach wykonywania telepracy przez pracowników wprowadza się następującą politykę oraz wspierające ją zabezpieczenia:

1. Dostęp zdalny do sieci lokalnej możliwy jest jedynie wybranym użytkownikomi zestawiany jest na zasadzie tunelu szyfrowanego VPN.
2. Do logowania wykorzystywana jest para użytkownik/hasło oraz certyfikat.
3. Dostępy bez zestawienia tunelu VPN możliwe są jedynie ze wskazanych zewnętrznych adresów IP.
4. Nie zależnie od zestawionego tunelu VPN istnieje konieczność dodatkowego logowania na wszystkie serwery/urządzenia czy usługi.
5. Wszystkie działania na serwerach opartych o platformę Windows rejestrowane są przez system DLP.
6. Aktywność użytkowników na systemach innych niż Microsoft logowana jest przez ich mechanizmy wewnętrzne.
7. Dane przetwarzane w miejscach telepracy (np. dostęp zdalny biura rachunkowego) są w modelu terminalowym zgodnie z nadanymi uprawnieniami. Całość aktywności monitorowana jest z wykorzystaniem oprogramowania DLP.
8. Komunikacja pomiędzy klientem a siecią Jednostki jest szyfrowana.

7 BEZPIECZEŃSTWO ZASOBÓW LUDZKICH

7.1 Przed zatrudnieniem

Role i zakresy, odpowiedzialności i obowiązki w zakresie bezpieczeństwa informacji, które mają zastosowanie w obszarze zatrudniania ustanowione zostały w Regulaminie Organizacyjnym.

Postępowanie sprawdzające

Każdy kandydat na pracownika podlega postępowaniu sprawdzającemu, uwzględniającemu między innymi jego kompetencje merytoryczne, umiejętności oraz kwalifikacje etyczne, ze szczególnym uwzględnieniem takich cech jak uczciwość, odpowiedzialność, przewidywalność zachowań etc.

Warunki zatrudnienia

Każdy pracownik przy zawieraniu umowy o pracę podpisuje umowę o poufności w celu stworzenia warunków dla wymiany pozyskanych informacji w ramach stosunku pracy podczas przygotowań oraz wykonywania działań na rzecz Jednostki.

Ryzyko ze strony osób, które potencjalnie mogą w łatwiejszy sposób uzyskać dostęp do informacji (np. osoby sprzątające pomieszczenia), jest minimalizowane przez zobowiązywanie ich do zachowania tajemnicy na podstawie odrębnych pisemnych oświadczeń.

7.2 Podczas zatrudnienia

Odpowiedzialność kierownictwa

Do skutecznego zarządzania bezpieczeństwem informacji zaangażowane jest kierownictwo Jednostki, co zostało uregulowane w Regulaminie organizacyjnym. Kierownictwo wymaga od pracowników, wykonawców oraz

259

użytkowników reprezentujących stronę trzecią stosowania zasad bezpieczeństwa zgodnie z wprowadzonymi w organizacji politykami, standardami i procedurami.

Uświadamianie, kształcenie i szkolenie z zakresu bezpieczeństwa informacji

Postanowienia ogólne

Wszyscy pracownicy jednostki oraz, gdzie jest to wskazane, wykonawcy i użytkownicy reprezentujący stronę trzecią, są szkoleni w zakresie bezpieczeństwa informacji, oraz regularnie informowani i zapoznawania o uaktualnieniach polityk i procedur obowiązujących w organizacji.

Podczas zatrudnienia kierownictwo Jednostki egzekwuje realizację wymagań polityki bezpieczeństwa informacji oraz uświadamiania pracowników o zagrożeniach powstających na skutek niewłaściwego postępowania w przedmiotowym obszarze.

Każdy pracownik jest zobowiązany do stosowania przepisów prawa oraz procedur obowiązujących jednostce. Pracownicy wykonują swoje obowiązki zgodnie z zakresem czynności i odpowiedzialności oraz są zobowiązani zgodnie z Kodeksem pracy dbać o dobro zakładu pracy, chronić jego mienie oraz zachować w tajemnicy informacje, których ujawnienie mogłoby narazić pracodawcę na szkodę.

Skrzynki pocztowe służbowe podlegają wyłącznie służbowemu przeznaczeniu i co za tym idzie o możliwości monitorowania ich treści, o czym Jednostka, jako pracodawca, informuje pracowników.

W Jednostce zainstalowane jest oprogramowanie monitorujące aktywność użytkowników systemu informatycznego /kontrola jakościowa i ilościowa pracy/, o czym Jednostka, jako pracodawca, informuje pracowników.

260

Szkolenia wewnętrzne

Administrator Bezpieczeństwa Informacji organizuje szkolenia wewnętrzne uwzględniając następujące wytyczne:

a) szkoli się każdą osobę, która ma uzyskać dostęp do informacji;
b) szkolenia wewnętrzne wszystkich osób upoważnionych do przetwarzania danych przeprowadzane są w przypadku każdej zmiany zasad lub procedur ich ochrony;
c) przeprowadza się szkolenia dla osób innych niż upoważnione do przetwarzania danych, jeśli pełnione przez nie funkcje wiążą się z zabezpieczeniem informacji.

Tematyka szkoleń obejmuje następujące zagadnienia:

1. Ochronę danych osobowych według wymogów wynikających z Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz. U. 2014 r. poz.1182 oraz aktów wykonawaych do ustawy.
2. Bezpieczeństwo systemów informatycznych wg. Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2012 r. poz.526) oraz normy PN-ISO/IEC 27001:2014.

Postępowanie dyscyplinarne

Sposób postępowania dyscyplinarnego wobec pracowników, którzy naruszyli bezpieczeństwo informacji obowiązujące w organizacji, stosuje się zgodnie z ustawą - Kodeks pracy i Regulaminem Pracy.

Postępowanie dyscyplinarne nie będzie rozpoczęte bez uprzedniej weryfikacji potwierdzającej, że nastąpiło naruszenie bezpieczeństwa informacji.

261

7.3 Zakończenie zatrudnienia lub zmiana zakresu obowiązków

Po zakończeniu zatrudnienia lub zmianie zakresu obowiązków zostają skutecznie usuwane wszystkie uprawnienia, poprzez:

a) przekazanie informacji o zakończeniu zatrudnienia do osób przełożonych, którzy są odpowiedzialni za sprawdzenie swoich systemów i usunięcie z nich uprawnień danej osoby (pracownika);
b) zapewnienie zwrotu aktywów, z których dany pracownik korzystał – komputer, samochód, telefon itp.).
c) W sytuacji zmiany zakresu obowiązków następuje nadanie nowych praw.
d) **Osobą odpowiedzialną za rozliczenie pracownika jest bezpośredni przełożony.**

8 ZARZĄDZANIE AKTYWAMI

8.1 Odpowiedzialność za aktywa

Odpowiedzialność za aktywa jest elementem polityki zarządzania bezpieczeństwem informacji. Osobami odpowiedzialnymi za aktywa wyszczególnione w ramach SZBI są osoby fizyczne lub prawne.

Inwentaryzacja aktywów

Za bezpieczeństwo aktywów odpowiedzialność ponosi osoba wskazana w Rejestrze Aktywów.

W Jednostce wszystkie aktywa są jasno zidentyfikowane oraz jest sporządzona i utrzymywana aktualna analiza ryzyka. Za prowadzenie i aktualizowanie Rejestru odpowiedzialny Administrator Bezpieczeństwa Informacji.

Własność aktywów

W celu osiągnięcia i utrzymania odpowiedniego poziomu ochrony aktywów organizacji wszystkie aktywa mają wyznaczonego właściciela. Właścicielom aktywów przydzielono odpowiedzialność za utrzymanie odpowiednich zabezpieczeń, które obowiązują na podstawie obowiązujących w jednostce dokumentów SZBI.

Akceptowalne użycie aktywów

Pracownicy i współpracownicy posiadają dostęp do aktywów zgodnie z ich uprawnieniami, zakresem obowiązków, odpowiedzialności i własności. Aktywa mogą być wynoszone z Jednostki za zgodą Burmistrzapod warunkiem ich właściwego zabezpieczenia, zgodnego z odpowiadającą w tym zakresie polityką szczegółową.

263

Zwrot aktywów

Zasady dotyczące przekazania i zwrotu aktywów będących w posiadaniu pracowników zostały określone w rozdziale 7. 3 Zakończenie zatrudnienia lub zmiana zakresu obowiązków.

8.2 Klasyfikacja informacji

Klasyfikowanie informacji

Podstawowym elementem klasyfikacji są następujące grupy informacji:

a) informacje zwykłe
b) informacje chronione (dotyczą one takich danych, jak: dane osobowe, w tym dane wrażliwe; tajemnice handlowe, tajemnicę przedsiębiorstwa oraz wszystkie inne dane, których poufność określają przepisy szczególne).

W grupach informacji zebrane zostały dokumenty logicznie ze sobą powiązaneo podobnych wymaganiach związanych z bezpieczeństwem. Do określenia poziomu bezpieczeństwa danej grupy informacji przyjęto wskaźniki definiujące poufność, integralność oraz dostępność danej grupy informacji, wymagane w Jednostki.

Przez poufność rozumiemy zapewnienie, iż dostęp do informacji mają tylko i wyłącznie osoby uprawnione. Przez integralność rozumiemy zapewnienie, iż informacje nie zostały zmienione lub zniszczone w nieautoryzowany sposób (niezgodny z wewnętrznymi regulacjami Jednostki). Przez dostępność rozumiemy zapewnienie, iż informacje będą udostępniane z zasobów o różnym poziomie bezpieczeństwa z uwagi na miejsce i sposób przechowywania. Ze względu na charakter pracy Jednostki i jego funkcjonowanie do określenia wskaźników bezpieczeństwa największy nacisk położono na wszystkie wymienione parametry. Informacje sklasyfikowano do grup informacji: zwykłych oraz chronionych, z wyłączeniem informacji niejawnych.

Oznaczanie informacji

Oznaczenie informacji zostało zawarte w Procedurze nr P.8.2.2.

Postępowanie z aktywami

Oznaczenie informacji zostało zawarte w Procedurze nr P.8.2.3.

8.3 Postępowanie z nośnikami

Nośniki są przechowywane w sposób uniemożliwiający dostęp do nich osób nieupoważnionych, jak również zabezpieczający je przed zagrożeniami środowiskowymi (np. zalanie, pożar-sejf ogniotrwały). Nośniki zawierające informacje sklasyfikowane jako wewnętrzne i chronione, które opuszczają obszar bezpieczny, zabezpieczone są z wykorzystaniem metod kryptograficznych.

Zarządzanie nośnikami wymiennymi

Zarządzanie nośnikami wymiennymi zostało opisane w procedurze nr P.8.3.1.

Wycofywanie nośników

Wycofywanie nośników informacji zostało opisane w procedurze nr P.8.3.2

Przekazywanie nośników

W sytuacji przekazywania nośników z danymi poza obszar Jednostki należy stosować następujące zasady bezpieczeństwa:

a) adresat powinien zostać powiadomiony o przesyłce;
b) nadawca powinien sporządzić kopię przesyłanych danych;
c) dane przed wysłaniem powinny zostać zaszyfrowane, a hasło podane adresatowi inną drogą;
d) stosować bezpieczne koperty depozytowe;
e) przesyłkę należy przesyłać kurierem;
f) adresat powinien powiadomić nadawcę o otrzymaniu przesyłki.

265

ROZPOWSZECHNIENIE I ZARZĄDZANIE DOKUMENTEM POLITYKI

Prawo dostępu do Polityki Bezpieczeństwa Informacji posiadają przede wszystkim pracownicy Jednostki oraz osoby i instytucje mające dostęp do informacji podlegającej ochroniea także strony umów i porozumień.

Niniejsza polityka podlega regularnym przeglądom przez Administratora Bezpieczeństwa Informacji, podczas okresowych przeglądów Systemu (**załącznik nr 6 stanowi Rejestr przeglądu i aktualizacji polityki Bezpieczeństwa Informacji)**. W zależności od potrzeb mogą zostać przeprowadzone dodatkowe przeglądy po stwierdzeniu istotnego naruszenia bezpieczeństwa, pojawieniu się zasadniczych zmian w Jednostce, jego strukturze lub jego otoczeniu (nowe zagrożenia, technologie). Celem przeglądów polityki jest zapewnienie jej stosowalności w stosunku do realizowanych zadań oraz możliwości obsługi interesantów w każdych warunkach niezależnie od okoliczności i zmian w Jednostce.

9 KONTROLA DOSTĘPU

9.1 Wymagania biznesowe wobec kontroli dostępu

Jednostka stawia sobie jako główny cel realizację ustawowych zadań i świadczenie usług publicznych na wysokim poziomie bezpieczeństwa.Aby realizować ten cel wprowadzone są następujące zasady.

Polityka kontroli dostępu

Zostaje ustanowiona i udokumentowana Polityka kontroli dostępu. Osobami odpowiedzialnymi za przestrzeganie zasad wynikających z niniejszego rozdziału są Administrator Bezpieczeństwa Informacji oraz Administrator Systemu Informatycznego w zakresach wynikających z przydzielonych im obowiązków.

Dostęp do informacji przechowywanych i przetwarzanych w zakresie ograniczonym do danych osobowych jest zgodny z obowiązującymi przepisami prawa powszechnego oraz wymaganiami bezpieczeństwa, przyjętymi w normach PN-ISO/IEC 27001:2014.

Polityka kontroli polega w szczególności na:

a) wydzieleniu obszarów przeznaczonych do przechowywania oraz przetwarzania poszczególnych zbiorów danych i zapewnieniu odpowiednich barier fizycznych przeciwdziałających nieuprawnionemu dostępowi zgodnie z postanowieniami Rozdziału 11;
b) zarządzaniu uprawnieniami (9.2.3) poszczególnych użytkowników w sposób zapewniający dostęp wyłącznie do danych wymaganych do wykonywania obowiązków służbowych, jeśli dane te podlegają ochronie z jakiejkolwiek przyczyny;
c) stosowaniu bezpiecznych systemów przetwarzania informacji;
d) nadzorowaniu działalności stron trzecich, mogących wpłynąć na bezpieczeństwo informacji;

267

e) bieżącym informowaniu pracowników o istotnych zmianach, które ich dotyczą w zakresie regulacji dotyczących przechowywania, przetwarzania i udostępniania informacji;

f) adekwatność i skuteczność stosowanych w Jednostce środków kontroli dostępu do informacji podlega bieżącej weryfikacji, zmian dokumentacji i metod postępowania wynikających z ewolucji uregulowań prawnych oraz systemów przetwarzania danych, a także reagowania na zagrożenia ujawnione przez inne strony. Niezależnie od tych środków weryfikacji polityka kontroli dostępu podlega co roku przeglądowi przez Zespół ds. Bezpieczeństwa Informacji i jest zatwierdzana przez Kierownictwo Jednostki.

Dostęp do sieci i usług sieciowych

System teleinformatyczny połączony jest z publiczną siecią telekomunikacyjną. Komunikacja na styku sieci lokalnej i Internetu zabezpieczona jest poprzez zaporę sieciową. Użytkownicy mają dostęp do zasobów zgodnie z ich upoważnieniami i z zakresem obowiązków.

Załącznik nr 13-Polityka szczegółowa dotycząca korzystania z Internetu.

9.2 Zarządzanie dostępem użytkowników

Użytkownicy systemu teleinformatycznego mają dostęp do zasobów Jednostki zgodniez profilem dostępowym użytkownika na podstawie przydzielonych mu uprawnień.

Rejestrowanie i wyrejestrowanie użytkowników i przydzielanie praw dostępu

Proces rejestrowania użytkowników wygląda następująco:

a) osoba dokonująca rejestracji otrzymuje informacje co do systemów informatycznych i poziomów uprawnień dla danego użytkownika;

268

b) dokonuje założenia konta i/lub modyfikacji uprawnień;
c) dokonuje weryfikacji uprawnień;
d) przekazuje hasło/hasła dostępu wymuszając jego zmianę przy kolejnym logowaniu.

Wyrejestrowanieużytkownika polega na cofnięciu jego uprawnień lub blokady konta.

W szczególnych przypadkach konta użytkowników wyrejestrowanych będą usuwane z systemu po upływie trzech lat od dnia wyrejestrowania.

Przydzielanie praw dostępu następuje automatycznie na podstawie roli przypisanej danemu użytkownikowi w chwili zakładania mu konta użytkownika.

Przydzielanie dostępu użytkownikom

Administrator Systemu Informatycznego jest odpowiedzialny za nadawanie i odbieranie uprawnień do systemów i usług wszystkim użytkownikom.

Procedura nadawania i odbierania praw dostępu przebiega w następujący sposób:

1) Administrator Systemu Informatycznego nadaje oraz modyfikuje uprawnienia.
2) Przydzielanie praw dostępu następuje na podstawie zakresu obowiązków przypisanych danemu użytkownikowi oraz upoważnienia do przetwarzania danych osobowych w chwili zakładania mu konta użytkownika.
3) Dodatkowe uprawnienia mogą zostać przyznane użytkownikowi w przypadku zaistnienia takiej potrzeby wynikającej ze zmian zakresu obowiązków.
4) Ostatnim etapem jest weryfikacja poprawności przydzielonych uprawnień, której dokonuje Administrator Systemu Informatycznego.

269

Zarządzanie prawami uprzywilejowanego dostępu

1. Nadawanie praw uprzywilejowanego dostępu ograniczone jest wyłącznie do osób, którym takowe są niezbędne.
2. Hasła dostępu generowane są w sposób automatyczny i cechują się wysoką złożonością.

Zarządzanie poufnymi informacjami uwierzytelniającymi użytkowników

Identyfikator składa się z imienia oraz nazwiska rozdzielonych znakiem interpunkcyjnym kropki. W identyfikatorze pomija się polskie znaki diakrytyczne. W przypadku dublowania się identyfikatorów zostanie on rozszerzony o symbol wydziału.

W przypadku zbieżności nadawanego identyfikatora z identyfikatorem wcześniej zarejestrowanego użytkownika Administrator Systemu Informatycznego, za zgodą Administratora Bezpieczeństwa Informacji, nadaje inny identyfikator, odstępując od zasady określonej wyżej.

Hasło powinno składać się z unikalnego zestawu **co najmniej ośmiu znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne.**Hasło nie może być identyczne z identyfikatorem użytkownika ani jego imieniem lub nazwiskiem.

Użytkownicy systemu informatycznego zobowiązani są do zmiany hasła nie rzadziej niż co 30 dni i nie częściej niż co 1 dzień. Administrator Bezpieczeństwa Informacji może w uzasadnionych sytuacjach, polecić dokonanie zmiany hasła przez użytkownika.

Przegląd praw dostępu użytkowników

Administrator Systemu Informatycznego weryfikuje uprawnienia dostępu użytkowników do informacji zawartych w systemach informatycznych Jednostki. Powyższego przeglądu dokonuje się w sytuacji naruszenia bezpieczeństwa informacji spowodowanym nieautoryzowanym logowaniem, w sytuacji zmian

270

personalnych lub stwierdzenia innego rodzaju incydentu.(**Załącznik nr 7 stanowi Wzór protokołu z kontroli uprawnień**).

Odbieranie lub dostosowanie dostępu

Odbieranie lub dostosowanie dostępu następuje w sytuacji ustania stosunku pracy, zakończenia umowy/porozumienia/projektu oraz podczas innych sytuacji, w których jest to wymagane. Dokonywane jest na polecenie Burmistrzaprzez Administratora Systemu Informatycznego.

Wyrejestrowywanie uprawnień

1. Wyrejestrowania użytkownika z systemu informatycznego dokonuje Administrator Systemu Informatycznego.
2. Wyrejestrowanie, o którym mowa w pkt. 1, może mieć charakter czasowy lub trwały.
3. Wyrejestrowanie następuje poprzez:
   - zablokowanie konta użytkownika do czasu ustania przyczyny uzasadniającej blokadę (wyrejestrowanie czasowe),
   - usunięcie danych użytkownika z bazy użytkowników systemu (wyrejestrowanie trwałe).
4. Powodem do wszczęcia procedury czasowego wyrejestrowania użytkownika z systemu informatycznego może być:
   - nieobecności w pracy trwającej dłużej niż 21 dni kalendarzowych,
   - zawieszenia w pełnieniu obowiązków służbowych,
   - wypowiedzenie umowy o pracy,
   - wszczęcie postępowania dyscyplinarnego względem osoby upoważnionej do przetwarzania danych osobowych.
5. Przyczyną trwałego wyrejestrowania użytkownika z systemu informatycznego jest rozwiązanie lub wygaśnięcie stosunku pracy lub innego stosunku prawnego, w ramach którego zatrudniony był użytkownik.

271

9.3 Odpowiedzialność użytkowników

W momencie zakładania użytkownika w systemie informatycznym generowane jest jednorazowe hasło. Użytkownik zobligowany jest do jego zmiany przy pierwszym logowaniu. **Wszyscy użytkownicy mają unikalne identyfikatory do swojego wyłącznego i osobistego użytku.**

Stosowanie poufnych informacji uwierzytelniających

Zabrania się użytkownikom systemu udostępniania swojego identyfikatora i hasła innym osobom oraz korzystania przez osoby upoważnione do przetwarzania danych osobowychz identyfikatora lub hasła innego użytkownika.

9.4 Kontrola i ograniczenie dostępu do systemów i aplikacji

Systemy informatyczne i aplikacje posiadają mechanizmy autoryzacyjne. System informatyczny zabezpieczony jest poprzez wdrożone oprogramowanie DLP. Logi systemowe, aplikacyjne i z oprogramowania DLP podlegają przeglądom przez Administratora Systemu Informatycznego i Administratora Bezpieczeństwa Informacji w zakresie wynikającym z ich kompetencji.

Procedury bezpiecznego logowania

Procedura bezpiecznego logowania została opisana w procedurze nr P.9.4.2.

System zarządzania hasłami

Administrator systemu nie ma wiedzy na temat haseł innych pracowników przez co zapewniona jest rozliczalność. Użytkownicy systemu informatycznego zobowiązani są do okresowej zmiany haseł. Częstotliwość zmiany haseł – raz na 30 dni, złożoność co najmniej 8 znaków, co najmniej 3 z 4 grup znaków (małe litery, duże litery, cyfry, znaki specjalne).

Hasła administracyjne są spisane oraz udokumentowany jest sposób dostępu administracyjnego do systemów informatycznych i urządzeń Jednostki. Powyższe hasła przechowywane są w sposób bezpieczny, uniemożliwiające dostęp osobom nieuprawnionym.

Użycie uprzywilejowanych programów narzędziowych

Jednostka w ramach swojej głównejdziałalności oraz działań wewnętrznych nie wykorzystuje uprzywilejowanych programów narzędziowych.

Kontrola dostępu do kodów źródłowych programów

Kod źródłowy strony internetowej jednostki i wewnętrznego rejestru zamówień archiwizowany jest zgodnie z polityką wykonywania kopii zapasowych. Dostęp do niego ma wyłącznie Administrator Systemu Informatycznego.

Załącznik nr 3 –Sposób przepływu danych pomiędzy systemami informatycznymi przetwarzającymi dane osobowe.

2t3

10 KRYPTOGRAFIA

10.1 Zabezpieczenia kryptograficzne

Polityka stosowania zabezpieczeń kryptograficznych

Technologia kryptograficzna używana jest w 4 aspektach:

1. Zabezpieczanie danych znajdujących się na komputerach przenośnych, autoryzacja z wykorzystaniem użytkownika i hasła lub klucza kryptograficznego.
2. Zabezpieczanie połączeń zdalnych do infrastruktury Jednostki z wykorzystaniem kanałów cyfrowanych VPN.
3. Bezpieczne logowania poprzez sieć Internet do usług administrowanych przez firmy trzecie-dostęp https i protokół SSL, poczta elektroniczna.

Należy stosować następujące sposoby kryptograficznej ochrony danych:

1. Orzy przesyłaniu danych za pomocą poczty elektronicznej stosuje się protokoły szyfrowane – wykorzystując szyfrowanie połączenia (TLS lub SSL).
2. Przy przesyłaniu danych pracowników, niezbędnych do wykonania przelewów wynagrodzeń, używa się bezpiecznych stron szyfrowanych protokołem SSL oznaczonych jako https:// i podpisanych certyfikatem.

Zarządzanie kluczami

Klucze kryptograficzne zmieniane są w momencie zauważenia incydentu związanego
z naruszeniem bezpieczeństwa stosowanych urządzeń kryptograficznych.

Zmienia się je także w sytuacji gdy zachodzą podejrzenia, że mogły dostać się w ręce osób nieupoważnionych (np. w sytuacji wygaśnięcia stosunku pracy, gdy zwalniany pracownik miał do nich dostęp).

11 BEZPIECZEŃSTWO FIZYCZNE I ŚRODOWISKOWE

11.1 Obszary bezpieczne, fizyczne wejście, biura, pomieszczenia i obiekty

Fizyczna granica obszaru bezpiecznego

Za obszar bezpieczny uznaje się budynki i pomieszczenia wyszczególnione **w załączniku nr 2 –Wykaz budynków i pomieszczeń.**

Fizyczne zabezpieczenia wejść

Pomieszczenia składające się na obszar bezpieczny zabezpieczone są drzwiami zamykanymi na klucz.

Zabezpieczenie biur, pomieszczeń i obiektów

Zabezpieczenia budynku, biur, pomieszczeń i obiektów opisane zostało w załączniku nr 2.

Zabezpieczenie serwerowni

Załącznik nr 2-Wykaz budynków i pomieszczeń.

Ochrona przed zagrożeniami zewnętrznymi i środowiskowymi

W przypadku nastąpienia katastrofy naturalnej, wrogiego ataku lub wypadku pracownicy Jednostki oraz wszystkie osoby przebywające na terenie obszaru bezpiecznego są zobowiązane przestrzegać następujących zasad:

1. W przypadku wystąpienia zagrożenia powodującego konieczność przeprowadzenia ewakuacji osób lub mienia z pomieszczeń, w których przetwarzane są dane osobowe, mają zastosowanie przepisy niniejszego rozdziału oraz innych przepisów szczegółowych.
2. O zagrożeniu, jego skali i podjętych krokach zaradczych osoba kierująca ewakuacją zobowiązana jest powiadomić bezpośredniegoprzełożonego. W razie niemożności skontaktowania się z nim zawiadamia innych członków Zespołu ds. Bezpieczeństwa informacji i ciągłości działania. Numery telefonów do tych osób powinny być znane pracownikom.
3. Osoby biorące udział w akcji ratunkowej mają prawo wejść do pomieszczeń,w których przetwarzane są dane informacje.
4. W przypadku ogłoszenia alarmu ewakuacyjnego użytkownicy przebywający w pomieszczeniach, obowiązani są do przerwania pracy i w miarę możliwości przed opuszczeniem tych pomieszczeń do:

a) zamknięcia systemu informatycznego;

b) zabezpieczenia danych gromadzonych w kartotekach.

5. W czasie trwania akcji ratunkowej i po jej zakończeniu obecni użytkownicy powinni, w miarę możliwości, zabezpieczyć dane przed nieuprawnionym do nich dostępem. Obowiązek ten ciąży w równym stopniu na wszystkich pracownikach obecnych przy akcji ratunkowej.

Praca w obszarach bezpiecznych

Zasady pracy w obszarach bezpiecznych zostały opisane w procedurze nr P.11.1.5.

Obszary dostaw i załadunku

Osoby trzecie nie mają co do zasady dostępu do infrastruktury jednostki oraz sprzętu komputerowego.

Dla osób trzecich chcących skorzystać z dostępu do sieci Internet lub dla komputerów serwisowych wydzielona jest odrębna podsieć oddzielona od sieci Jednostki.

Podmioty/jednostki podległe mające swoją siedzibę w budynku Jednostki i wykorzystujące fizycznie jej infrastrukturę sieciową, mają wydzielone sieci w sposób uniemożliwiający dostęp do sieci lokalnej.

11.2 Sprzęt

Lokalizacja i ochrona sprzętu

Sprzęt umieszczonyjest w zabezpieczonych pomieszczeniach Jednostki. Sprzęt przenośny podlega ochronie zgodnie z niniejszym dokumentem.

Systemy wspomagające zabezpieczania/awarie zasilania

Serwery i urządzenia sieciowe zabezpieczone są przed awariami zasilania poprzez zastosowanie urządzenia UPS. W przypadku awarii zasilania w

277

serwerowni rozpoczyna się procedura automatycznego wyłączania systemów informatycznych. Automatyczne wyłączenie serwerów następuje po przekroczeniu ustalonego poziomu naładowania baterii w urządzeniu UPS. Ponowne włączenie serwerów następuje automatycznie po naładowaniu baterii zasilaczy awaryjnych, możliwe jest też włączenie ręczne, poprzez naciśnięcie przycisku na poszczególnych fizycznych urządzeniach.

Stacje robocze zabezpieczone są przed awariami zasilania poprzez stosowanie jego podtrzymywanie z wykorzystaniem urządzeń UPS. Pojemność UPS-ów wystarcza na ręczne zamknięcie stacji roboczej i należy to do obowiązków pracującego na nim użytkownika (po niezwłocznym uprzednim zapisaniu wszystkich dokumentów i zamknięciu wszystkich używanych aplikacji).

Powyższa procedura ręcznego wyłączenia komputera powinna się zakończyć w czasie dwóch minut.

Bezpieczeństwo okablowania

Okablowanie sieciowe zostało zaprojektowane w ten sposób, że dostęp do linii teletransmisyjnych jest możliwy tylko z pomieszczeń zamykanych na klucz. Ponadto okablowanie znajduje się w tunelach ochronnych.

Bezpieczne zbywanie lub przekazywanie do ponownego użycia

W celu wykluczenia przypadkowego przekazania danych osobom nieuprawnionym, sprawdzane są wszystkie nośniki informacji w celu stwierdzenia, czy nie posiadają one danych Jednostki lub przetwarzanych w związku z funkcjonowaniem Jednostki. Dane wrażliwe lub licencjonowane programy są trwale usuwane lub nadpisane w sposób bezpieczny.

Pozostawianie sprzętu użytkownika bez opieki

Wszyscy użytkownicy zobowiązani są do zabezpieczenia sprzętu przed opuszczeniem stanowiska pracy w zależności od miejsca, w którym znajduje się

sprzęt np. poprzez zablokowanie ekranu lub zamknięcie pomieszczenia na klucz w przypadku, gdy z pomieszczenia wychodzi ostatnia osoba.

Załącznik nr 11 Polityka szczegółowa dotycząca bezpiecznego użytkowania sprzętu IT.

Dobre praktyki dotyczące bezpieczeństwa informacji: Polityka „czystego biurka" i polityka „czystego ekranu"

1. Informacje w wersji tradycyjnej (papierowej) są przechowywane po zakończeniu pracy w zamykanych na klucz meblach biurowych, a tam gdzie jest to możliwew szafach metalowych. Klucze od szaf są zabezpieczone przed dostępem do nich osób nieupoważnionych do przetwarzania danych osobowych.
2. Przed osobami postronnymi należy chronić ekrany komputerów (ustawienie monitora powinno uniemożliwiać pogląd), wydruki leżące na biurkach orazw otwartych szafach.
3. Monitory komputerów wyposażone są wautomatyczną blokadę systemu aktywującą się po20 minutach od przerwania pracy. Wznowienie dostępu do systemu następuje dopiero po wprowadzeniu odpowiedniego hasła.
4. W przypadku opuszczenia stanowiska pracy użytkownik obowiązany jest aktywizować wygaszacz ekranu lub w inny sposób zablokować stację roboczą.

279

12 BEZPIECZNA EKSPLOATACJA

Bezpieczna eksploatacja maszyn, urządzeń, budynków i środków transportu obejmuje działania techniczne, administracyjne i kierownicze, których celem jest utrzymywanie ichw stanie gotowości do pełnienia wymaganej funkcji (lub przywracanie do takiego stanu) oraz ich ochrona przed uszkodzeniem lub zniszczeniem. Czynności związane z bezpieczną eksploatacją, to m.in.:

a) kontrola (przegląd);
b) sprawdzanie (testowanie);
c) pomiary;
d) wymiana sprzętu;
e) wymiana części;
f) regulacja;
g) naprawa;
h) wykrywanie usterek i nieprawidłowości;
i) serwisowanie.

12.1 Procedury eksploatacyjne, odpowiedzialność i dokumentowanie procedur

W Jednostce stosowana jest prawidłowa i bezpieczna eksploatacja środków przetwarzania informacji. Odpowiedzialność za bezpieczną eksploatację ww. urządzeń ponoszą osoby za nie odpowiedzialne oraz osoby z nich korzystające. Procedury i instrukcje eksploatacyjne są: udokumentowane, utrzymywane i dostępne dla wszystkich użytkowników, którzy ich potrzebują.

Dokumentowanie procedur eksploatacyjnych

Dokumentowanie toku prac eksploatacyjnych znajduje się w procedurze P.12.1.1

Zarządzanie zmianami

Zmiany w środkach przetwarzania informacji i systemach są na bieżąco kontrolowanei nadzorowane przez ASI.

Tworzenie i dostosowywanie procedur do wymogów normy **PN – ISO/ IEC 27001 : 2014** należy do obowiązków Pełnomocnika ds. ZBI.

Zarządzanie pojemnością

1. Stosowane przez Jednostkę systemy informatyczne oraz rozwiązania sprzętowe są skalowalne.
2. System DLP monitoruje: logi systemowe, przestrzeń dyskową oraz wydajność sprzętu komputerowego.

Oddzielanie środowisk rozwojowych, testowych i produkcyjnych

1. Testowanie oprogramowania odbywa się na wydzielonych maszynach wirtualnych lub fizycznych komputerach lub serwerach.
2. Testowane rozwiązania nie mają wpływu na działanie systemów produkcyjnych.
3. Środowiska rozwojowe, testowe i produkcyjne są rozdzielone.

12.2 Ochrona przed szkodliwym oprogramowaniem

1. W organizacji wykorzystywane jest oprogramowanie antywirusowe, którego celem jest zabezpieczenie przed szkodliwym oprogramowaniem.
2. Użytkownicy pracują na kontach z uprawnieniami adekwatnymi do potrzeb wynikających z danego stanowiska pracy, co ogranicza możliwość instalowania oprogramowania i dostęp do plików systemowych etc.

12.3 Kopie zapasowe

Administrator Systemu Informatycznego jest odpowiedzialny za wykonywania kopii zapasowych.

Zakres danych objętych kopią zapasową, harmonogram ich wykonywania, testowanie oraz miejsce przechowywania określa załącznik nr 8 do niniejszej polityki.

Likwidacja nośników zawierających kopie

1. Nośniki zawierające nieaktualne kopie danych, będące poza wykazem cyklicznych kopii, likwiduje się czyniąc o tym stosowny zapis w dzienniku kopii zabezpieczających. W przypadku nośników jednorazowych, takich jak płyty CD-R, DVD-R, likwidacja polega na ich fizycznym zniszczeniu w taki sposób, by nie można było odczytać ich zawartości (np. w dedykowanej ku temu niszczarce). Nośniki wielorazowego użytku, takie jak dyski twarde, dyskietki, płyty CD-RW, DVD-RW, etc. można wykorzystać ponownie do celów przechowywania kopii bezpieczeństwa po uprzednim usunięciu ich zawartości za pomocą wymazywania z co najmniej trzykrotnym nadpisaniem.
2. Nośniki wielorazowego użytku nienadające się do ponownego użycia zniszczone są fizycznie za pomocą certyfikowanych rozwiązań, a ich zniszczenie odnotowywane jest w dzienniku kopii zabezpieczających i protokole kasowania danych/nośników.

Przechowywanie elektronicznych nośników informacji zawierających dane osobowe

1. Zakazuje się przetwarzania danych osobowych na zewnętrznych nośnikach magnetycznych, optycznych i innych oraz ich przesyłania pocztą elektroniczną bez uprzedniego zaszyfrowania.

2. Na nośnikach, o których mowa w pkt 1, dopuszczalne jest przekazywanie zbiorów danych jedynie po uprzednim zaszyfrowaniu danych i udostępnieniu hasła innym kanałem.
3. W przypadku posługiwania się nośnikami danych pochodzącymi od podmiotu zewnętrznego użytkownik jest zobowiązany do uprzedniego sprawdzenia go programem antywirusowym.
4. Nośniki magnetyczne raz użyte do przetwarzania danych osobowych nie mogą być wykorzystywane do innych celów mimo usunięcia danych i podlegają ochroniew trybie niniejszej instrukcji.

12.4 Rejestrowanie zdarzeń i monitorowanie oraz rejestrowanie działań administratorów i operatorów

Rejestrowanie zdarzeń

1. W Jednostce rejestruje się udane i nieudane logowania do systemu czy też wszystkie próby zmiany ustawień zabezpieczeń na komputerach. Wszystkie te zdarzenia są rejestrowane w Dzienniku Zdarzeń.
2. Dzienniki zdarzeń są systematycznie monitorowane.
3. Logi rejestrujące zdarzenia są chronione przed manipulacją i nieuprawnionym dostępem.
4. Rejestrowanie działań administratorów i operatorów w systemach informatycznych realizowane jest poprzez system DLP, logi systemowe oraz logi systemów dziedzinowych.
5. System informatyczny tworzy logi na następujących poziomach:
    a. poziom DLP (stacje robocze+ serwery Windows);
    b. poziom systemów operacyjnych.
6. Logi ze wszystkich poziomów zabezpieczone są w zakresie integralności, dostępności i poufności.
7. Logi są archiwizowane zgodnie z polityką szczegółową wykonywania kopii zapasowych.

8. Logi są regularnie przeglądane pod kątem bezpieczeństwa informacji.
9. Harmonogram przeglądania logów:
    a) system DLP –raz/tydzień;
    b) logi systemu Windows - raz/tydzień;
    c) inne –w zależności od potrzeb i sytuacji.
10. Rejestrowanie działań administratorów i operatorów w systemach informatycznych realizowane jest przez:
    a) system DLP;
    b) logi systemowe;

Synchronizacja zegarów

1. Synchronizacja zegarów:
    a) synchronizacja czasu serwerów oraz stacji roboczych realizowany jest poprzez:serwery/protokół NTP z autoryzowanego i bezpiecznego serwera czasu;
    b) stacje robocze-synchronizacja czasu z serwerem domeny Active Directory.

12.5 Nadzór i instalacja oprogramowania produkcyjnego

Integralność systemów produkcyjnych zapewniona jest poprzez:

a) gradację uprawnień użytkowników;
b) nadzór nad instalowanym oprogramowaniem;
c) regularne i wykonywane za pomocą różnych metod (często duplikowane) kopie zapasowe systemu informatycznego.

Instalacja oprogramowania w systemach produkcyjnych

Instalacja oprogramowania w systemach produkcyjnych znajduje się w procedurze nr P.12.5.1

12.6 Zarządzanie podatnościami technicznymi

System informatyczny jest stale monitorowany pod kątem podatności technicznych. Odbywa się to poprzez:

a) monitorowanie informacji o ujawnionych podatnościach na portalach branżowych dotyczących bezpieczeństwa informacji;
b) okresowe wykonywanie testów podatności z wykorzystaniem profesjonalnego dedykowanego do tego celu oprogramowania;

Po ujawnieniu podatności, systemy informatyczne są aktualizowane (zgodnie z rangą podatności) lub ryzyko wykorzystania zidentyfikowanej podatności jest analizowane, szacowane i zarządzanie nim odbywa się zgodnie z dokumentami SZBI.

Ograniczenia w instalowaniu oprogramowania

1. Instalowanie oprogramowania przez użytkowników jest możliwe jedynie w obrębie przyznanych im uprawnień. To powoduje, że takowe uprawnienia mają jedynie administratorzy serwerów lub stacji roboczych, którzy są świadomi zakresu i rodzaju licencji na oprogramowanie w Jednostce.
2. Każdorazowa instalacja oprogramowania jest rejestrowana przez system DLP,a zainstalowane oprogramowanie na systemach operacyjnych Windows jest regularnie monitorowane oraz analizowane pod kątem licencjonowania, konieczności użytkowania i bezpieczeństwa.
3. Administrator Systemu Informatycznego dba o aktualność i bezpieczeństwo zainstalowanego oprogramowania.Aktualizacje instalowane są najpierw na kilku komputerach w wydzielonej grupie testowej, po sprawdzeniu poprawności działania zatwierdzana jest instalacja dla pozostałych komputerów.

285

Załącznik nr 12 Polityka szczegółowa dotycząca korzystania z oprogramowania.

12.7 Audyty systemów informacyjnych

1. System informatyczny jest regularnie analizowany pod kątem bezpieczeństwa.
2. Testowanie bezpieczeństwa i audytowanie odbywa się z zachowaniem wszelkich norm bezpieczeństwa.
3. Audyty wewnętrzne odbywają się w okresie, w którym dostępność systemów informatycznych nie jest krytyczna (np. w przeddzień okresów wolnych od pracy).

13 BEZPIECZEŃSTWO KOMUNIKACJI

13.1 Zarządzanie bezpieczeństwem sieci

1. Administrator Systemu Informatycznego sprawuje nadzór nad bezpieczeństwem sieci.
2. Umowy zawierane ze stronami trzecimi dotyczące dostępu, przetwarzania, przekazywania lub zarządzania informacjami organizacji lub środkami przetwarzania informacji lub dodanie produktów lub usług do środków przetwarzania informacji są przeglądane pod kątem przyjętych w organizacji wymagań bezpieczeństwa.
3. System informatyczny zabezpieczony jest Firewall'em.
4. Komunikacja pomiędzy siecią lokalną a segmentem serwerowym zabezpieczona jest z wykorzystaniem mechanizmów IPS/IDS.
5. Logi z powyższej komunikacji przechowywane są na serwerze.
6. Sieć Jednostki podzielona jest na podsieci pod względem funkcjonalnym
   i bezpieczeństwa:

   a) sieć lokalna (stacje robocze i serwery),-segment stacji roboczych;
   b) podsieci wydzielone dla jednostek –segment serwera.

13.2 Przesyłanie informacji

1. Komunikacja wewnątrz Jednostki odbywa się poprzez zasoby współdzielone z ograniczonym dostępem oraz pocztę elektroniczną.
2. Przesyłanie danych osobowych z użyciem e-maila poza organizację może odbywać się tylko po uprzednim zaszyfrowaniu danych.
3. W przypadku przesyłania informacji wrażliwych wewnątrz Jednostki, bądź też wszelkich informacji poza organizację, należy wykorzystywać mechanizmy kryptograficzne (hasłowanie wysyłanych plików, podpis elektroniczny).

4. W przypadku zabezpieczenia plików hasłem, obowiązuje minimum 8 znaków; na hasło składają się: dużei małe litery, cyfry lub znaki specjalne, samo hasło należy przesłać odrębnym e-mailem lub inną metodą, np. telefonicznie lub SMS-em.
5. Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu e-mail odbiorcy wiadomości.
6. Zaleca się, aby użytkownik podczas przesyłania danych osobowych e-mailemzaznaczył opcjęprośby o potwierdzenie otrzymania i zapoznania się z informacją przez adresata.
7. Nie należy otwierać załączników (plików) w e-mailach nadesłanych przez nieznanego nadawcę lub podejrzanych załączników nadanych przez znanego nadawcę.
8. Użytkownicy powinni okresowo kasować niepotrzebne e-maile.
9. Podczas wysyłania e-maili do wielu adresatów jednocześnie należy użyć metody „Ukryte do wiadomości-UDW".
10. E-mail jest przeznaczony wyłącznie do wykonywania obowiązków służbowych.
11. Użytkownicy mają prawo korzystać z e-maili dla celów prywatnych wyłącznie okazjonalnie i praktyka ta powinna być ograniczona do niezbędnego minimum.
12. Korzystanie z e-maila dla celów prywatnych nie może wpływać na jakość i ilość świadczonej przez użytkownika pracy oraz na prawidłowe i rzetelne wykonywanie przez niego obowiązków służbowych.
13. Przy korzystaniu z e-maila, użytkownicy mają obowiązek przestrzegać uprawnień osób trzecich, wynikających z praw autorskich i praw pokrewnych.
14. Użytkownicy nie mają prawa korzystać z e-maila w celu rozpowszechniania treścio charakterze obraźliwym, niemoralnym lub niestosownym wobec powszechnie obowiązujących zasad postępowania.

15. Wiadomości elektroniczne nie są używane do przesyłania informacji podlegających ochronie. W razie konieczności zabezpieczenia takiej wiadomości stosuje się techniki kryptograficzne.
16. Zasady korzystania z poczty elektronicznej niewymieniane w punktach poprzedzających zostały sprecyzowane w **Polityce szczegółowej, stanowiącej załącznik nr 9.**

289

14 POZYSKIWANIE, ROZWÓJ I UTRZYMANIE SYSTEMÓW

14.1 Wymagania bezpieczeństwa systemów informacyjnych

Najbardziej krytycznymi etapami cyklu życia systemu informatycznego są projektowaniei wdrożenie. Zatem wymagania bezpieczeństwa powinny być zdefiniowane na etapie formułowania wymagań systemu informatycznego i powinny być spójne z przyjętym modelem biznesowym. W celu identyfikowania wymagań dotyczących bezpieczeństwa informacji Zespół ds. Bezpieczeństwa będzie dokonywał analizy systemu zgodnie z poniższymi punktami.

Analiza i specyfikacja wymagań bezpieczeństwa informacji

Zespół ds. Bezpieczeństwa będzie identyfikować wymagania dotyczące bezpieczeństwa informacji w nowych systemach lub przy rozbudowie istniejących systemów.

W identyfikowaniu wymagań brana jest pod uwagę:

a) zgodność z polityką i przepisami,
b) modelowanie zagrożeń,
c) przeglądy incydentów (gdy mowa o rozbudowie systemu).

Identyfikacja wymagań związanych z bezpieczeństwem informacji realizowana będzie na wczesnych etapach projektów systemów informacyjnych. Wymagania te będą uwzględniały:

a) zastosowanie odpowiednich wymagań dotyczących uwierzytelniania użytkowników,
b) procesy przydzielania dostępu i autoryzacji dla użytkowników biznesowych (standardowych), uprzywilejowanych i technicznych,
c) wymagania co do ochrony zaangażowanych aktywów w zakresie dostępności, poufności i integralności,

d) wymagania wynikające z procesów biznesowych (np. rejestrowanie działań użytkowników),

e) wymagania narzucane przez inne zabezpieczenia, np. przez system DLP.

Zabezpieczanie usług aplikacyjnych w sieciach publicznych

Informacje przesyłane w sieciach publicznych, związane z usługami świadczonymi przez aplikacje, chronione są przed nieuczciwymi działaniami, sporami dotyczącymi umów oraz nieuprawionym ujawnieniem i zmianami za pomocą:

a) procesówautoryzacjizaimplementowanych w aplikacjach,

b) weryfikacji stron komunikacji,

c) wymagania ochrony wszelkich informacji poufnych,

d) stosowanie szyfrowanych kanałów transmisji.

Ochrona transakcji usług aplikacyjnych

Transakcje dokonywane w ramach usług świadczonych przez aplikacje są chronione, by zapobiec nieuprawionym zmianom, ujawnieniu, powieleniu czy odtworzeniu, a także błędomw trasowaniu czy przerwaniu transmisji. Realizowane jest to poprzez:

a) stosowanie podpisów elektronicznych,

b) zapewnienie, że:
   - poufne informacje uwierzytelniające są ważne i zweryfikowane;
   - transakcja pozostaje poufna;
   - prywatność wszystkich stron jest zapewniona;

c) komunikacja jest szyfrowana,

d) protokoły używane do komunikacji są bezpieczne.

e) szczegóły transakcji znajdują się na nośniku znajdującym się poza siecią Internet (np. na stacji roboczej w Jednostce),

f) jeśli wykorzystywane są certyfikaty lub podpisy wydawane przez stronę trzecią, to bezpieczeństwo jest zintegrowane i włączone w cały proces zarządzania certyfikatami lub podpisami.

14.2 Bezpieczeństwo w procesach rozwoju i wsparcia

Polityka bezpieczeństwa prac rozwojowych

1. Bezpieczeństwo informacji jest procesem na stałe obecnym w Jednostce. Dotyczy ono zarówno systemów obecnie eksploatowanych jak i planowanych do wdrożenia.
2. Bezpieczeństwo informacji dotyczy także aspektów sprzętowych/planowanej rozbudowy, uzupełniania bazy sprzętowej itp.
3. Bezpieczeństwo informacji jest uwzględnione na każdym z etapów wykorzystywania systemów informatycznych. Zarówno dane testowe, produkcyjne, jak i zmigrowane do nowego systemu (w przypadku zakończenia eksploatacji danego systemu) podlegają pełnej ochronie zapewniającej ich poufność i integralność.
4. Ochrona polega między innymi na:
   a) rozdzieleniu systemów rozwojowych od produkcyjnych,
   b) mechanizmów autoryzacji analogicznych do stosowanych w systemach produkcyjnych,
   c) przechowywanie danych systemów rozwojowych w bezpiecznych strefach.
5. Systemy rozwojowe są formalnie wersjonowane.
6. Kontrola zmian realizowana jest poprzez:
   a) logi systemowe,
   b) kopie zapasowe systemów rozwojowych inicjowanych ręcznie wg potrzeb.
7. Prace rozwojowe nad oprogramowaniem oraz systemami prowadzone są

292

w warunkach laboratoryjnych - w rozłącznym z produkcyjnym środowiskiem.

8. Systemy i oprogramowanie wdrażane jest w systemie produkcyjnym dopiero po przejściu testów jakościowych, funkcjonalnych i bezpieczeństwa.
9. Po wdrożeniu zmian w platformach produkcyjnych (aktualizacja oprogramowania, wdrożenie nowego systemu informatycznego) badany jest jego wpływ na całość funkcjonujących urządzeń i aplikacji oraz poprawności jej biznesowych funkcjonalności.
10. Przed wdrożeniem na platformę produkcyjną oprogramowania/system informatyczny jest wnikliwie testowany w systemach rozwojowych i testowych.
11. Konieczność modyfikacji oprogramowania determinowana jest przez:
    a) wymaganą aktualizację-np. opublikowanie podatności,
    b) zmiany funkcjonalne i technologiczne oraz sprzętowe,
    c) dodatkowe funkcjonalności biznesowe.
12. Powyższe modyfikacje w pakietach oprogramowania wykonywane są z rozwagą ograniczają się do wymaganych zmian, które to są ściśle kontrolowane.

Zasady projektowania bezpiecznych systemów

1. Środowiska rozwojowe chronione są analogicznie do systemów produkcyjnych.
2. Organizacja nadzoruje i monitoruje prace rozwojowe nad systemami zleconymi podmiotom zewnętrznym. Realizowane jest to poprzez:
    a) odpowiednie zapisy w umowach dotyczące bezpieczeństwa informacji,
    b) narzucenie standardu zabezpieczeń zgodnie ze standardami Urzędu,
    c) prawo do audytu.

3. Bezpieczeństwo jest testowane na etapie tworzenia systemu, po każdej jego istotnej zmianie lub zakończonej pracy nad modułem/większą funkcjonalnością.
4. Dla potrzeb odbioru systemów informatycznych lub ich modyfikacji planowane są programy testów akceptujących oraz kryteria z nimi związane.
5. Stosowne zapisy znajdują się w umowach w przypadku prac zleconych na zewnątrz.
6. Dane testowe chronione są zgodnie z ogólnie przyjętą polityką Jednostki. Są one starannie dobierane, tak aby zawierały sytuacje szczególne i krytyczne.

14.3 Dane testowe

1. Dane testowe są starannie wybierane, chronione i nadzorowane.
2. Wybierane są takie dane, aby zawierały jedynie informacje ogólne, nie pozwalające na identyfikację osób lub nie zawierające innych poufnych danych.
3. Jeśli jednak stosowane są dane rzeczywiste, to:
   d) w testowych aplikacjach stosuje się takie same procedury kontroli dostępu, jak do systemów produkcyjnych,
   e) po zakończeniu testów dane rzeczywiste są niezwłocznie usuwane ze środowiska testowego,
   f) wszelkie czynności kopiowania i użycia w testach danych rzeczywistych są odnotowywane/rejestrowane.

15 RELACJE Z DOSTAWCAMI

15.1 Bezpieczeństwo w porozumieniach z dostawcami

Opiera się na poniższych zasadach:

1. Usługi w obszarach kluczowych dla funkcjonowania Jednostce, zawierają
   w umowach klauzule o poufności, jak również postanowienia gwarantujące integralność oraz dostępność danych.
2. Zapisy w umowach z dostawcami dotyczą bezpieczeństwa informacji, terminów dostaw, czasu SLA, sposobów reklamacji orz ewentualnych kar umownych. Umowy opracowywane są w oparciu o analizę ryzyka w zakresie realizowanych usług.
3. Realizacja umów jest monitorowana w zakresie bezpieczeństwa informacji. Kluczowe umowy oraz te obarczone wysokim ryzykiem zawierają zapisy o prawie do audytu. Audyt wykonywany jest w razie niewłaściwej realizacji umowy.
4. W umowach, które swoim zakresem obejmują powierzenia przetwarzania lub udostępnienie danych osobowych stosuje się odpowiednie klauzule zabezpieczające.
5. Zapisy dotyczące relacji z dostawcami zawarte w tejże polityce są na bieżąco analizowane i dostosowywane do istniejących warunków.

295

16 ZARZĄDZANIE INCYDENTAMI ORAZ UDOSKONALENIAMI

16.1 Odpowiedzialność i procedury

W celu zapewnienia spójnego i skutecznego zarządzania incydentami związanymiz bezpieczeństwem informacji zostają wprowadzone Procedury Zarządzania Incydentami (Procedury ZI). Administrator Bezpieczeństwa Informacji jest odpowiedzialny za planowanie, przygotowywanie, wdrażanie i poprawianie tych procedur. Zespół ds. Bezpieczeństwa nadzoruje koordynację działań w przypadku wystąpienia incydentu naruszającego System Bezpieczeństwa Informacji.

16.2 Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji

1. Wszelkie zdarzenia związane z naruszeniem bezpieczeństwa informacji lub ujawnieniem podatności należy zgłaszać do członków Zespołu ds. Bezpieczeństwa Informacji i Ciągłości Działania; w przypadku niemożliwości kontaktu z nimi – do bezpośredniego przełożonego.
2. Każdy z pracowników i kontrahentów Jednostki zobowiązany jest do możliwie najszybszego zgłaszania zdarzeń związanych z bezpieczeństwem informacji.
3. W szczególności w sytuacji gdy zauważy:
   a) nieskuteczne zabezpieczenie;
   b) naruszenie oczekiwanej integralności, poufności lub dostępności informacji;
   c) błędy ludzkie wpływające na bezpieczeństwo informacji, zarówno własne jaki współpracowników;
   d) zachowania niezgodne z polityką lub zaleceniami;
   e) naruszenia ustaleń związanych z bezpieczeństwem fizycznym;

f) nienadzorowane zmiany systemu;
g) niepoprawne działania systemu lub sprzętu;
h) naruszenia dostępu;
i) awarie lub inne nienormalne zachowania systemu mogące wskazywać na atak lub rzeczywiste naruszenie bezpieczeństwa.

4. Zgłoszenia incydentu następuje przez poinformowanie o nim Administratora Systemu Informatycznego w formie pisemnej notatki, z opisem zdarzenia które nastąpiło lub w formie ustnej.
5. Każde zgłoszenie incydentu zapisywane jest do **Dziennika Zdarzeń, który stanowi załącznik nr 10.**
6. Oceny incydentu dokonuje Administrator Systemu Informatycznego i odnotowuje ją do DziennikaZdarzeń.
7. W sytuacji wystąpienia incydentu zagrażającemu bezpieczeństwu informacji Administrator Systemu Informatycznego informuje o tym Administratora Bezpieczeństwa Informacji.

Zgłaszanie słabości związanych z bezpieczeństwem informacji

1. Każdy pracownik zobowiązany jest do odnotowywania i zgłaszania wszelkich zaobserwowanych lub podejrzewanych słabości związanych z bezpieczeństwem informacji w systemach lub usługach.
2. Powyższa czynności powinna być wykonana możliwie najszybciej do punktu kontaktowego.
3. Niniejsze procedury odnoszą się także do kooperantów i kontrahentów.

Zabrania się próbować dowieść istnienia podejrzewanej słabości. Testowanie podatności może być zinterpretowane jako niewłaściwe korzystanie z systemu i spowodować szkody w systemie informatycznym lub usłudze. Pociągnąć za sobą może to konsekwencje prawne wobec osoby wykonującej takie testy.

297

Ocena i podejmowanie decyzji w sprawie zdarzeń związanych z bezpieczeństwem informacji

1. Każde zdarzenie związane z bezpieczeństwem informacji podlega ocenie pod kątem kwalifikacji go jako incydentu naruszenia bezpieczeństwa informacji. Powyższa ocena oparta jest na wiedzy i doświadczeniu Zespołu ds. Bezpieczeństwa Informacjii Ciągłości Działania.
2. W przypadkach szczególnych dopuszczalne jest wykorzystywanie ekspertów zewnętrznych, za zgodą kierownictwa Jednostki.

Reagowanie na incydenty związane z bezpieczeństwem informacji zostało oznaczonew procedurze nr P. 16.1.5

Wyciąganie wniosków z incydentów związanych z bezpieczeństwem informacji

1. Incydenty bezpieczeństwa informacji są rejestrowane i dokumentowane przez Administratora Bezpieczeństwa Informacji. Określane są ich przyczyny, prawdopodobieństwo ponownego wystąpienia, ich skutki oraz koszty.
2. Każdorazowo po wpisaniu nowego incydentu do Dziennika ZdarzeńAdministrator Bezpieczeństwa Informacji analizuje poprzednie incydenty celem wykrycia ewentualnych powiązań pomiędzy nimi i podjęcia dodatkowych działań mających na celu minimalizację ryzyka jego ponownego wystąpienia.
3. Dodatkowo, incydenty mogą być wykorzystywane podczas szkoleń pracowniczych jako przykłady tego co może się wydarzyć, jak unikać ich w przyszłości i jak reagować na nie, w momencie gdy już się wydarzą. Podczas wykorzystywania powyższych informacji należy wykazać się daleko idącą ostrożnością w aspekcie zachowania poufności; zaleca się anonimiazację danych.

Gromadzenie materiału dowodowego zostało oznaczone w procedurze nr A.16.1.7

299

17 Aspekty bezpieczeństwa informacji w zarządzaniu ciągłością działania

17.1 Ciągłość w bezpieczeństwie informacji

Jednostka zarządza bezpieczeństwem informacji na każdym etapie jego funkcjonowania.

Planowanie ciągłości bezpieczeństwa informacji

1. W niekorzystnych sytuacjach wymagania w zakresie bezpieczeństwa informacji pozostają takie same jak w te w normalnych warunkach eksploatacyjnych.
2. W lokalizacjach zastępczych stosujemy mechanizmy szyfrowania uniemożliwiające dostęp do danych nawet w przypadku posiadania dostępu fizycznego do sprzętu.
3. Dane pomiędzy lokalizacjami przenoszone są w postaci zaszyfrowanej.

Wdrożenie ciągłości bezpieczeństwa informacji zostało oznaczone w procedurze nr P.17.1.2

Plan działania w przypadku awarii sprzętowej

1. Przeniesienia funkcjonalności na dostępne urządzenia (np. na serwer zapasowy), aw przypadku niemożności – zastosować sprzęt zastępczy lub alternatywną konfigurację.
2. Odtworzenie danych z kopii zapasowych, a w przypadku niemożności (niemożliwości) ich odtworzenia –odtworzenie z kopii zapasowych danych znajdujących się winnej lokalizacji, niż pierwotne dane źródłowe.

Weryfikacja, przegląd i ocena ciągłości bezpieczeństwa informacji.

1. Weryfikacja poprawności wykonywania kopii zapasowych sprawdzana jest poprzez okresową (cotygodniową) weryfikację logów oprogramowania wykonującego kopie.
2. Przy pierwszej kopii wykonanej danym narzędziem należy wykonać próbę odzyskiwania danych.
3. Powyższe próby wykonuje się każdorazowo jeżeli jest podejrzenie, że kopii mogą wykonywać się niepoprawnie lub mogą być problemy z ich odtworzeniem.

Nadmiarowość

1. Serwery posiadają redundancję podzespołów najczęściej ulegających awarii, tj. dysków twardych i zasilaczy.
2. Urządzenia nie posiadające redundancji są proste do zastąpienia za pomocą innych urządzeń znajdujących się w ciągłej sprzedaży (maksymalny czas oczekiwania na urządzenie zastępcze nie przekracza 24h).
3. Nośniki danych – dyski twarde w serwach oraz NAS są łączone w macierze RAID. Macierze te budowane są w taki sposób aby awaria jednego dysku nie prowadziła do utraty danych.

18 ZGODNOŚĆ

18.1 Zgodność z przepisami prawa

Postanowienia ogólne

Pracownicy Jednostki oraz kontrahenci muszą przestrzegać wszelkich zasad wynikających z Polityki Bezpieczeństwa Informacji, przepisów prawa powszechnego oraz norm międzynarodowych. Korzystanie z Systemów Informatycznych Jednostki nie daje pracownikom ani kontrahentom jakichkolwiek praw własności intelektualnej do Systemów Jednostki ani do dostępnych w nim treści.

4. Informacji pochodzących z Systemu Informatycznego Jednostki nie wolno wykorzystywać, chyba że ich właściciel udzieli na to pozwolenia lub jest to w inny sposób dozwolone przez prawo.
5. Niniejsze warunki nie powodują przyznania pracownikom Jednostki ani jego kontrahentom prawa do wykorzystania jakichkolwiek marek lub logotypów znajdujących się w jego zasobach Systemu Informatycznego.
6. Nie wolno usuwać, zasłaniać ani zmieniać żadnych informacji prawnych znajdujących się na materiałach Jednostki lub materiałach w związku z nimi.
7. Wszystkie licencje na oprogramowanie są własnością Jednostki.

Przeglądy zgodnościzasobów

Przeglądy zgodności zasobów Jednostki znajdują się w procedurze nr P. 18.1.2

Postępowanie w przypadku wykrycia niezgodności

Jeżeli w wyniku przeglądu zgodności zostaną wykryte jakiekolwiek niezgodności, to zaleca się, aby Zespół ds. Bezpieczeństwa:

302

1. ustalił przyczyny niezgodności;
2. ocenił potrzebę działać zapewniających zgodność;
3. wprowadził odpowiednie działania korygujące.

Kroki poczynione przy postępowaniu naprawczym rejestrowane są w Raporcie Naprawczym.

Niezależny przegląd bezpieczeństwa informacji

Realizacja działań związanych ze sprawdzeniem obszaru w zakresie bezpieczeństwa informacji jest poddawana okresowo w zależności od potrzeb jednostki.

Zgodność z politykami bezpieczeństwa i standardami

Kierownictwo na bieżąco dokonuje przeglądu zgodności przetwarzania informacjiw Jednostce z Polityką Bezpieczeństwa Informacji i innymi regulacjami w podległym obszarze.

Sprawdzanie zgodności technicznej

Systemy informacyjne Jednostki są regularnie sprawdzane pod kątem zgodności z normami wdrażania zabezpieczeń.

19 Wykaz załączników

Załącznik nr 1-Rejestr aktywów-wykaz i struktura zbiorów danych,

Załącznik nr 2-Wykaz budynków i pomieszczeń,

Załącznik nr 3 –Sposób przepływu danych pomiędzy systemami informatycznymi przetwarzającymi dane osobowe,

Załącznik nr 4-Oświadczenie o znajomości Polityki bezpieczeństwa informacji,

Załącznik nr 5- Oświadczenie o zachowaniu poufności

Załącznik nr 6-Przegląd i aktualizacja Polityki bezpieczeństwa informacji,

Załącznik nr 7-Wzór protokołu z kontroli uprawnień,

Załącznik nr 8-Polityka szczegółowa kopii zapasowych,

Załącznik nr 9 Polityka szczegółowa korzystania z poczty elektronicznej,

Załącznik nr 10- Dziennik zdarzeń,

Załącznik nr 11-Polityka szczegółowa dotycząca bezpiecznego użytkowania sprzętu IT,

Załącznik nr 12- Polityka szczegółowa dotycząca korzystania z oprogramowania,

Załącznik nr 13 Polityka szczegółowa dotycząca korzystania z Internetu,

Załącznik nr 14- Upoważnienia,

Załącznik nr 15-Potwierdzenie nadania uprawnień,

Załącznik nr 16 –Ewidencja osób upoważnionych,

Załącznik nr 17- Struktura rejestru zbiorów prowadzonego przez Administratora Bezpieczeństwa Informacji.

Załącznik nr 1 do Polityki bezpieczeństwa informacji	*Tytuł* **Rejestr aktywów – wykaz i struktura zbiorów danych**	

1.

Nazwa zbioru:	**Dzienni korespondencji przychodzącej i wychodzącej**
Status zbioru:	Administrator Danych Osobowych powołał Administratora Bezpieczeństwa Informacji, w związku z tym ma zastosowanie art. 43 ust. 1a.
Forma przetwarzania danych:	Korespondencja przychodząca –forma elektroniczna za pomocą eObiegu i papierowa. Natomiast korespondencja wychodząca –forma papierowa
Struktura zbioru danych:	Imię, nazwisko, nazwa, adres korespondencyjny.
Podstawa prawna:	Ustawa z dnia 8 marca 1990 r. o samorządzie gminnym (Dz.U.2015.1515 j.t.) Ustawa w z dnia 18 stycznia 2011 roku w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych (Dz. U. 2011 nr 14 poz. 67 ze zmianami).

2.

Nazwa zbioru:	**Rejestr wniosków o udzielenie informacji publicznej**
Status zbioru:	Zbiór zwolniony z rejestracji na podstawie art. 43 ust.1 pkt 12.
Forma przetwarzania danych:	Papierowa
Struktura zbioru danych:	Imię, nazwisko, nazwa, adres korespondencyjny, adres e-mail.
Podstawa prawna:	Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. 2014. 782 ze zm).

3.

Nazwa zbioru:	**Kadry i Płace**
Status zbioru:	Zbiór jest zwolniony z rejestracji na podstawie art. 43. ust.1 pkt 4.
Forma przetwarzania danych:	Papierowa i elektroniczna za pomocą programu „PłaceOptivum" Vulcan, Płatnika-aplikacja udostępniona przez ZUS, pakietu MS Office.
Struktura zbioru danych:	imię i nazwisko, nazwisko rodowe, imiona rodziców, data i miejsce urodzenia, adres zamieszkania, korespondencyjny, numer ewidencyjny PESEL, Numer Identyfikacji Podatkowej, dokumentacja kandydata do pracy, miejsce pracy, zawód, wykształcenie, seria i numer dowodu osobistego, numer telefonu, nr konta bankowego.
Podstawa prawna:	Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy (Dz. U. z 2014 r. poz. 1502, 1662 z późn. zm.)
Przepływ danych:	Eksport danych z programu „PłaceOptivum" do home banking i Płatnika. Eksport danych w postaci elektronicznej do ZUS, transmisja zabezpieczona metodami kryptograficznymi.

4.

Nazwa zbioru:	**Stażyści**
Status zbioru:	Zbiór jest zwolniony z rejestracji na podstawie art. 43. ust.1 pkt 4.
Forma przetwarzania danych:	Papierowa.
Struktura zbioru danych:	imię i nazwisko, data urodzenia, adres zamieszkania, adres korespondencyjny, numer ewidencyjny PESEL, miejsce odbywania stażu oraz zajmowane stanowisko, okres odbywania stażu.
Podstawa prawna:	Ustawa z dnia 20 kwietnia 2004 r. o promocji zatrudnienia i instytucjach rynku pracy (Dz. U. z 2015 r., 149 ze. zm.)

5.

Nazwa zbioru:	**Rada Miejska** **Obejmuje:** **1)** oświadczenia majątkowe radnych, **2)** dane teleadresowe radnych,
Status zbioru:	Administrator Danych Osobowych powołał Administratora Bezpieczeństwa Informacji, w związku z tym ma zastosowanie art. 43 ust.1a.
Forma przetwarzania danych:	Papierowa oraz elektroniczna (publikacja na Biuletynie Informacji Publicznej).
Struktura zbioru danych:	Ad. 1 – imię, nazwisko, nazwisko rodowe, miejsce zatrudnienia, stanowisko lub funkcja, stan majątkowy, informacje o wynagrodzeniu, informacje o zajmowanym stanowisku kierowniczym w podmiotach prawa gospodarczego, adres zamieszkania; Ad. 2 – imię, nazwisko, adres zamieszkania, telefon kontaktowy.
Podstawa prawna:	Ustawa z dnia 8 marca 1990 r. o samorządzie gminnym (Dz.U.2015.1515 j.t.)

6.

Nazwa zbioru:	**Gospodarka odpadami komunalnymi** **Obejmuje:** • Deklaracje i decyzje o wysokości opłaty za gospodarowanie odpadami komunalnymi • Postępowanie egzekucyjne w sprawie opłaty za gospodarowanie odpadami komunalnymi • Postępowania wymiarowe • Księgowość podatkowa opłaty za gospodarowanie odpadami komunalnymi (zwroty, przeksięgowania, odroczenia) • Umorzenia opłaty za gospodarowanie odpadami komunalnyminależności publicznoprawne.
Status zbioru:	Administrator Danych Osobowych powołał Administratora Bezpieczeństwa Informacji, w związku z tym ma zastosowanie art. 43 ust. 1a.
Forma przetwarzania danych:	Papierowa oraz elektroniczna za pomocą programu „Sortownik" Anko System Sp. z o.o.

Struktura zbioru danych:	właściciel nieruchomości, nazwa pełna, nazwisko, nazwa skrócona, imię, NIP, REGON, PESEL, data urodzenia, imię ojca, imię matki, numer telefonu, adres e-mail, adres siedziby/zamieszkania, dane nieruchomości, na której powstają odpady komunalne, informacja o wysokości opłaty za gospodarowanie odpadami komunalnymi, kwota zadłużenia, numer umowy z firmą wywozową, data wpisu do RDR, nr rejestrowy, rodzaj odbieranych odpadów komunalnych Nr zezwolenia, przedmiot i obszar działalności objętej zezwoleniem, termin podjęcia działalności, wymagania w zakresie jakości usług objętych zezwoleniem, niezbędne zabiegi z zakresu ochrony środowiska i ochrony sanitarnej wymagane po zakończeniu działalności objętej zezwoleniem, inne wymagania szczególne wynikające z odrębnych przepisów, w tym wymagania dotyczące standardu sanitarnego wykonywania usług, ochrony środowiska i obowiązku prowadzenia odpowiedniej dokumentacji działalności, objętej zezwoleniem, określenie stacji zlewnej, okres obowiązywania zezwolenia.
Podstawa prawna:	Ustawa z dnia 13 września 1996 r. o utrzymaniu czystości i porządku w gminach (tekst jednolity – Dz. U. z 2013 r., poz. 1399 z późn. zm.); Ustawa z dnia 29 sierpnia 1997 r. Ordynacja podatkowa (tekst jednolity – Dz. U. z 2015 r., poz. 613 z późn. zm.); Ustawa z dnia 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji (tekst jednolity – Dz. U. z 2014 r., poz. 1619 z późn. zm.).

7.

Nazwa zbioru:	**Ochrona środowiska** **Obejmuje:** 1) ewidencję wyrobów zawierających azbest; 2) rejestr decyzji środowiskowych, 3) zezwolenia na wycinkę drzew i krzewów
Status zbioru:	Administrator Danych Osobowych powołał Administratora Bezpieczeństwa Informacji, w związku z tym ma zastosowanie art. 43 ust. 1a.
Forma przetwarzania danych:	Elektroniczna za pomocą pakietu biurowego Office oraz papierowa.
Struktura zbioru danych:	imię i nazwisko, adres zamieszkania, nr ew. działki i położenie, obręb działki, tytuł władania nieruchomością, powierzchnia płyt azbestowych.
Podstawa prawna:	Ustawa z dnia 16 kwietnia 2004 r. o ochronie przyrody (Dz.U.2015.1651 j.t.),

	Ustawa z dnia 19 czerwca 1997 r. o zakazie stosowania wyrobów zawierających azbest (Dz. U. z 2004 r. Nr 3, poz. 20 z późn. zm.), Ustawa z dnia 3 października 2008 roku o udostępnianiu informacji o środowisku i jego ochronie, udziale społeczeństwa w ochronie środowiska oraz o ocenach oddziaływania na środowisko (Dz.U. 2013,poz. 1235).

8.

Nazwa zbioru:	**Decyzje drogowe** **Obejmuje:** • decyzje na zajęcie pasa drogowego oraz na wykonywanie transportu drogowego (w formie zezwolenia), • zezwolenia na lokalizację zjazdu.
Status zbioru:	Administrator Danych Osobowych powołał Administratora Bezpieczeństwa Informacji, w związku z tym ma zastosowanie art. 43 ust. 1a.
Forma przetwarzania danych:	Elektroniczna za pomocą pakietu biurowego Office oraz papierowa.
Struktura zbioru danych:	imię i nazwisko, adres zamieszkania, nr ew. działki i położenie, nazwa firmy, adres zamieszkania adresata decyzji i innych stron postępowania, numer decyzji, data wydania decyzji, organ wydający decyzję, oznaczenie stron postępowania.
Podstawa prawna:	Ustawa z dnia 21 marca 1985 r. o drogach publicznych (Dz. U. Nr 2015, poz. 460 j.t.)

9.

Nazwa zbioru:	**Zamówienia publiczne**
Status zbioru:	Administrator Danych Osobowych powołał Administratora Bezpieczeństwa Informacji, w związku z tym ma zastosowanie art. 43 ust. 1a.
Forma przetwarzania danych:	Elektroniczna za pomocą pakietu biurowego Office oraz papierowa.
Struktura zbioru danych:	imię i nazwisko, adres, Numer Identyfikacji Podatkowej, Nr REGON, numer konta bankowego, podwykonawcy, telefon

	kontaktowy.
Podstawa prawna:	Ustawa z dnia 29 stycznia 2004 r. prawo zamówień publicznych (Dz. U. z 2013 r., 907 ze zm.)

10.

Nazwa zbioru:	**Obrona cywilna-** **Ewidencja osób wyznaczonych do pełnienia służby w formacjach obrony cywilnej,** **Akcja kurierska,** **Rejestr świadczeń na rzecz obrony**
Status zbioru:	Administrator Danych Osobowych powołał Administratora Bezpieczeństwa Informacji, w związku z tym ma zastosowanie art. 43 ust. 1a.
Forma przetwarzania danych:	Elektroniczna za pomocą pakietu biurowego Office oraz papierowa.
Struktura zbioru danych:	imię i nazwisko, adres zameldowania, adres zamieszkania, data i miejsce urodzenia miejsce pracy, numer telefonu, imiona rodziców, PESEL,
Podstawa prawna:	Ustawa z dnia 21 listopada 1967 r. o powszechnym obowiązku obrony Rzeczypospolitej Polskiej (Dz. U. z 2015 r., 827 ze zm.)

11.

Nazwa zbioru:	**Ochrona przeciwpożarowa**
Status zbioru:	Administrator Danych Osobowych powołał Administratora Bezpieczeństwa Informacji, w związku z tym ma zastosowanie art. 43 ust. 1a.
Forma przetwarzania danych:	Papierowa
Struktura zbioru danych:	imię i nazwisko, adres zamieszkania, data i miejsce urodzenia miejsce pracy, numer telefonu, imiona rodziców, PESEL, brak przeciwwskazań do pełnienia funkcji
Podstawa prawna:	Ustawa z dnia 24 sierpnia 1991 r. o ochronie przeciwpożarowej (Dz. U. z 2009 r. Nr 178, poz. 1380 z późn. zm.)

12.

Nazwa zbioru:	**Rejestr osób podlegających rejestracji i kwalifikacji wojskowej**
Status zbioru:	Administrator Danych Osobowych powołał Administratora Bezpieczeństwa Informacji, w związku z tym ma zastosowanie art. 43 ust. 1a.
Forma przetwarzania danych:	Elektroniczna za pomocą pakietu biurowego Office oraz papierowa.
Struktura zbioru danych:	imię i nazwisko, nazwisko rodowe, imiona i nazwiska rodowe rodziców, PESEL, data i miejsce urodzenia, stan cywilny, adres i data zameldowania na pobyt stały, adres i data zameldowania na pobyt czasowy, numer i seria wojskowego dokumentu osobistego
Podstawa prawna:	Ustawa z dnia 21 listopada 1967 r. o powszechnym obowiązku obrony Rzeczypospolitej Polskiej (Dz. U. z 2015 r., 827 ze zm.)

13.

Nazwa zbioru:	**Kontrahenci** • Faktury, • Przelewy,
Status zbioru:	Zbiór jest zwolniony z rejestracji na podstawie art. 43. ust.1 pkt 8.
Forma przetwarzania danych:	Papierowa i elektroniczna za pomocą home banking, Budżet Win „RECORD".
Struktura zbioru danych:	imię i nazwisko, nazwa, adres, siedziba, Numer Identyfikacji Podatkowej, Nr REGON, PESEL, nr konta bankowego, numer umowy (sygnatura), nazwa wykonawcy lub dostawcy / adres, przedmiot umowy, wartość umowy brutto, data zawarcia umowy, osoba odpowiedzialna za realizację umowy, okres realizacji / gwarancja

14.

Nazwa zbioru:	**Rejestr wniosków o wpis do CEiDG**
Status zbioru:	Procesor
Forma przetwarzania danych:	Papierowa oraz elektroniczna za pomocą systemu CEiDG.
Struktura zbioru danych:	Wniosek o wpis do centralnej ewidencji i informacji o działalności gospodarczej zawiera następujące dane: Dane wnioskodawcy: Płeć, rodzaj dokumentu tożsamości, serię i numer dokumentu tożsamości, PESEL, NIP, REGON, nazwisko, nazwisko rodowe, imię pierwsze, imię drugie, imię ojca, imię matki, miejsce urodzenia, data urodzenia posiadane obywatelstwo, pouczenie/oświadczenie, określenie czy jest się cudzoziemcem oraz dane dokumentu potwierdzającego status cudzoziemca, adres miejsca zamieszkania wnioskodawcy: województwo, powiat, gmina, miejscowość, ulica, nr nieruchomości/domu, nr lokalu, kod pocztowy, poczta, określenie firmy przedsiębiorcy, którego wniosek dotyczy, przewidywana liczba pracujących/zatrudnionych, rodzaj działalności gospodarczej nazwa skrócona, data rozpoczęcia działalności, dane do kontaktu: nr telefonu, faksu, adres poczty elektronicznej, strona www, główne miejsce wykonywania działalności gospodarczej jeżeli jest inne niż adres wnioskodawcy, dodatkowe miejsce wykonywania działalności: numer REGON, nazwa jednostki lokalnej, adres dodatkowego miejsca wykonywania działalności gospodarczej (podanie danych adresowych jak wyżej), data powstania obowiązku opłacania składek do ZUS, dane dla potrzeb KRUS, informacja o zawieszeniu/wznowieniu/zaprzestaniu wykonywania działalności gospodarczej, informacja dotycząca naczelników urzędów skarbowych, oświadczenie o formie opłacania podatku dochodowego od osób fizycznych, forma wpłaty zaliczki, rodzaj prowadzonej dokumentacji rachunkowej, dane podmiotu prowadzącego dokumentację rachunkowa wnioskodawcy (firma, NIP), adres miejsca przechowywania dokumentacji rachunkowej wnioskodawcy, wskazanie czy prowadzę: zakład pracy chronionej, zagraniczne przedsiębiorstwo drobnej wytwórczości, działalność w formie spółki/spółek cywilnych, jestem wspólnikiem spółki, informacje

	o małżeńskiej wspólności majątkowej, dane identyfikacyjne rachunków bankowych wnioskodawcy: kraj siedziby banku, pełna nazwa banku, posiadacz rachunku, nr rachunku, osobisty rachunek bankowy (dane jak poprzednio wskazane), pełnomocnictwo do prowadzenia spraw, dane pełnomocnika: wskazanie czy pełnomocnik jest osobą prawną, nazwa firmy pełnomocnika, imię i nazwisko, PESEL/KRS, data urodzenia, NIP, obywatelstwo, adres pełnomocnika (dane jak poprzednio wskazywane), zakres pełnomocnictwa
Podstawa prawna:	Ustawa z dnia 2 lipca 2004 r. Przepisy wprowadzające ustawę o swobodzie działalności gospodarczej (Dz.U. 2004 nr 173 poz. 1808), Ustawa z dnia 2 lipca 2004 roku o swobodzie działalności gospodarczej (t.j.: Dz.U. 2015, poz 584 ze zm.) Ustawa z dnia 25 grudnia 2014 r. o zmianie ustawy o swobodzie działalności gospodarczej (Dz. U. z 2014, poz. 1885).

15.

Nazwa zbioru:	**Zezwolenia na sprzedaż napojów alkoholowych**
Status zbioru:	Administrator Danych Osobowych powołał Administratora Bezpieczeństwa Informacji, w związku z tym ma zastosowanie art. 43 ust. 1a.
Forma przetwarzania danych:	Elektroniczna za pomocą pakietu biurowego MS Office oraz papierowa.
Struktura zbioru danych:	imię i nazwisko, nazwa, adres zamieszkania (siedziba firmy), Numer Identyfikacji Podatkowej (NIP), numer telefonu, seria i numer dowodu osobistego, miejsce pracy, rodzaj zezwolenia, przedmiot działalności gospodarczej, numer w rejestrze przedsiębiorców, adres punktu sprzedaży/adres punktu składowania napojów alkoholowych, dane pełnomocników (imię, nazwisko, adres zamieszkania), adres zamieszkania (lub siedziby).
Podstawa prawna:	Ustawa z dnia 26 października 1982 r. o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi. (Dz.U.2015.1286 j.t) Ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz.U. z 2013 poz 267 tekst jednolity ze zm.).

16.

Nazwa zbioru:	**Podatki i opłaty lokalne** Zbiór służy do prowadzenia wymiaru podatków lokalnych i księgowości zobowiązań podatkowych, ewidencji dłużników, na wniosek podatnika Urząd wydaje zaświadczenia o prowadzeniu gospodarstwa rolnego, o posiadaniu kwalifikacji rolniczych, zaświadczenia dotyczące wliczania okresów zatrudnienia w gospodarstwie rolnym do pracowniczego stażu pracy.
Status zbioru:	Administrator Danych Osobowych powołał Administratora Bezpieczeństwa Informacji, w związku z tym ma zastosowanie art. 43 ust. 1a.
Forma przetwarzania danych:	Papierowa i elektroniczna za pomocą programu: „Opłaty od środków transportowych", „obsługa kasy", „tytuły wykonawcze"- Biuro Projektowo-Wdrożeniowe BPW Level s.c.
Struktura zbioru danych:	imię i nazwisko, data urodzenia, adres, numer i seria dowodu osobistego, imiona rodziców, informacja o wysokości i rodzaju podatku, adres nieruchomości, numer nieruchomości, numer księgi wieczystej, NIP, nr konta bankowego, PESEL, kwota zadłużenia lub dane dot. należności pieniężnych, dane dot. zaistnienia zdarzenia z którym ustawa podatkowa wiąże powstanie zobowiązania podatkowego, marka pojazdu, typ, model, liczba osi, rok produkcji pojazdu, dane dotyczące własności/współwłasności pojazdu, tytuł prawny do nieruchomości, tytuły wykonawcze, wysokość zaległości, wysokość odsetek, ilość zakupionego paliwa, kwota zwrotu podatku, limit zwrotu podatku

Podstawa prawna:	Ustawa z dnia 29 sierpnia 1997 r. Ordynacja podatkowa (Dz. U. z 2015 r., poz. 613 z późn. zm.) Ustawa z dnia 12 stycznia 1991 r. o podatkach i opłatach lokalnych (Dz. U. z 2014 r., poz. 849 z późn. zm.) Ustawa z dnia 30 października 2002 r. o podatku leśnym (Dz. U. Nr 2013, poz. 465 z późn. zm.), Ustawa z dnia 15 listopada 1984 r. o podatku rolnym (Dz. U. z 2013 r., poz. 1381 z późn. zm.) Ustawa z dnia 10 marca 2006 r. o zwrocie podatku akcyzowego zawartego w cenie oleju napędowego wykorzystywanego do produkcji rolnej (Dz.U.2015.1340 j.t.), Ustawa z dnia 26 lipca 1991 r. o podatku dochodowym od osób fizycznych (t.j. Dz.U. z 2012 r., poz. 361 ze zm.), Ustawa z dnia 15 lutego 1992 r. o podatku dochodowym od osób prawnych (t.j. Dz.U. z 2014 r., poz. 851 ze zm.), Ustawa z dnia 17.06.1966 r. o postępowaniu egzekucyjnym w administracji Dz. U. z 2015 r., poz. 87).

17.

Nazwa zbioru:	**Rolnictwo**
Status zbioru:	Administrator Danych Osobowych powołał Administratora Bezpieczeństwa Informacji, w związku z tym ma zastosowanie art. 43 ust. 1a.
Forma przetwarzania danych:	Elektroniczna za pomocą pakietu biurowego Office oraz papierowa
Struktura zbioru danych:	imię, nazwisko, adres zamieszkania, numer polisy ubezpieczeniowej, dane dot. nieruchomości.
Podstawa prawna:	Ustawa z dnia 20 lipca 1990 r. o wliczaniu okresów pracy w indywidualnym gospodarstwie rolnym do pracowniczego stażu pracy (Dz.U. 1990 nr 54, poz. 310). Rozporządzenie Rady Ministrów z dnia 27 stycznia 2015r. w sprawie szczegółowego zakresu i sposobu realizacji niektórych zadań ARMIR, Dz. U. 2015.187

18.

Nazwa zbioru:	**Zagospodarowanie przestrzenne** **Obejmuje:** • numeracja porządkowa nieruchomości; • rejestr miejscowych planów zagospodarowania przestrzennego (wypisy, wyrysy); • lokalizacja inwestycji celu publicznego; • zaświadczenie o przeznaczeniu terenu w planie zagospodarowania przestrzennego; • wydanych decyzji o warunkach zabudowy i zagospodarowaniu terenu • opinie geologiczne; • akty notarialne; • kopie decyzji o pozwoleniu na budowę.
Status zbioru:	Administrator Danych Osobowych powołał Administratora Bezpieczeństwa Informacji, w związku z tym ma zastosowanie art. 43 ust. 1a.
Forma przetwarzania danych:	Elektroniczna za pomocą pakietu biurowego MS Office oraz papierowa.
Struktura zbioru danych:	imię i nazwisko, adres zamieszkania, nr ew. działki i położenie, imiona rodziców.
Podstawa prawna:	Ustawa z dnia 27 marca 2003 r. o planowaniu i zagospodarowaniu przestrzennym (tj. Dz. U. z 2015 r., 199 ze zm.) Ustawa z dnia 17 maja 1989 r. prawo geodezyjne i kartograficzne (Dz. U. z 2015 r., 520 ze zm.).

19.

Nazwa zbioru:	**Ewidencja najemców i właścicieli lokali – gospodarowanie zasobem mieszkaniowym**
Status zbioru:	Administrator Danych Osobowych powołał Administratora Bezpieczeństwa Informacji, w związku z tym ma zastosowanie art. 43 ust. 1a.
Forma przetwarzania danych:	Papierowa i elektroniczna za pomocą programu „Czynsz" Biuro Projektowo-Wdrożeniowe BPW Level s.c.

Struktura zbioru danych:	imię i nazwisko, data urodzenia, adres zamieszkania, adres zamieszkania, seria i numer dowodu osobistego, PESEL, numer telefonu, wysokość i źródło dochodu, warunki zamieszkiwania kwalifikujące do ich poprawy, tytuł prawny do lokalu, ilość członków rodziny, inne informacje zawarte we wniosku osób ubiegających się o lokal socjalny lub zamianę lokalu, powierzchnia lokalu socjalnego lub użytkowego.
Podstawa prawna:	Ustawa z dnia 21 czerwca 2001 r. o ochronie praw lokatorów, mieszkaniowym zasobie gminy i o zmianie Kodeksu Cywilnego (Dz. U. 2014 r., poz. 150).

20.

Nazwa zbioru:	**Gospodarka nieruchomościami** **Obejmuje:** • czynsze dzierżawne i opłaty za użytkowanie wieczyste; • przekształcenie prawa użytkowania wieczystego w prawo własności nieruchomości; • sprzedaż gruntów; • scalanie i podział i nieruchomości; • nabywanie i wykup nieruchomości na mienie gminy; • podziały nieruchomości; • rozgraniczanie nieruchomości.
Status zbioru:	Administrator Danych Osobowych powołał Administratora Bezpieczeństwa Informacji, w związku z tym ma zastosowanie art. 43 ust. 1a.
Forma przetwarzania danych:	Elektroniczna za pomocą pakietu biurowego Office oraz papierowa.
Struktura zbioru danych:	imię i nazwisko, imiona rodziców, data i miejsce urodzenia, PESEL, numer i seria dowodu osobistego, adres zamieszkania, nr ew. działki i położenie, inne informacje dotyczące nieruchomości – powierzchnia, wartość, przeznaczenie, wysokość naliczonych opłat z tytułu dzierżawy, wieczystego użytkowania, terminy płatności), okres dzierżawy, numer księgi wieczystej, numer dokumentu będącego podstawą prawa własności.
Podstawa prawna:	Ustawa z dnia 21 sierpnia 1997r. o gospodarce nieruchomości (Dz.U.2015.1774 j.t.); Ustawa z dnia 29 lipca 2005r. o przekształceniu prawa użytkowania wieczystego w prawo własności nieruchomości (Dz. U. 2012. 83 ze zm.); Ustawa z dnia 18 lipca 2001r. Prawo wodne (Dz.U.2015.469 j.t.).

21.

Nazwa zbioru:	**Rejestr dowodów osobistych** Zawiera dane dotyczące osób, które ubiegają się o wydanie dowodu osobistego na podstawie wniosku, są także informacje dotyczące dowodów unieważnionych.
Status zbioru:	Procesor
Forma przetwarzania danych:	Elektroniczna za pomocą systemu Źródło oraz papierowa.
Struktura zbioru danych:	numer PESEL, nazwisko i imię (imiona), nazwisko rodowe, imię ojca, imię i nazwisko rodowe matki, data i miejsce urodzenia, płeć, wzrost, kolor oczu, adres miejsca zamieszkania na pobyt stały/pobyt czasowy trwający ponad 3 m-c, seria i numer poprzedniego dowodu, wystawca dowodu, wizerunek twarzy, podpis wnioskodawcy.
Podstawa prawna:	Ustawa o dowodach osobistych z dnia 6 sierpnia 2010 r. (Dz.U. z 2010 r. Nr 167, poz. 1131 z późn. zm.), Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U.2013.1422 j.t.), Ustawa z dnia 24 września 2010 r. o ewidencji ludności (Dz.U.2015.388 j.t.).

22.

Nazwa zbioru:	**Rejestr mieszkańców**
Status zbioru:	Administrator Danych Osobowych powołał Administratora Bezpieczeństwa Informacji, w związku z tym ma zastosowanie art. 43 ust. 1a.
Forma przetwarzania danych:	Elektroniczna za pomocą systemu Źródło, programuSEWLWIN, RWWIN (Sygnity) oraz papierowa.
Struktura zbioru danych:	nazwisko i imię (imiona), nazwisko rodowe, imiona i nazwiska rodowe rodziców, data urodzenia, miejsce urodzenia, kraj urodzenia, stan cywilny, numer aktu urodzenia i oznaczenie urzędu stanu cywilnego, w którym ten akt został sporządzony, płeć, numer PESEL, obywatelstwo albo status bezpaństwowca, imię i nazwisko rodowe oraz numer PESEL

	małżonka, jeżeli został mu nadany, data zawarcia związku małżeńskiego, numer aktu małżeństwa i oznaczenie urzędu stanu cywilnego, w którym ten akt został sporządzony, data rozwiązania związku małżeńskiego, sygnatura akt i oznaczenie sądu, który rozwiązał małżeństwo, sygnatura akt oznaczenie sądu, który ustalił nieistnienie małżeństwa, sygnatura akt oznaczenie sądu, który unieważnił małżeństwo, data zgonu małżonka albo data znalezienia jego zwłok, numer jego aktu zgonu i oznaczenie urzędu stanu cywilnego, w którym ten akt został sporządzony, adres i data zameldowania na pobyt stały; kraj miejsca zamieszkania, kraj poprzedniego miejsca zamieszkania, data wymeldowania z miejsca pobytu stałego, adres i data zameldowania na pobyt czasowy oraz data upływu deklarowanego terminu pobytu, data wymeldowania z miejsca pobytu czasowego, data wyjazdu poza granice Rzeczypospolitej Polskiej trwającego dłużej niż 6 miesięcy i wskazanie kraju wyjazdu, data powrotu z wyjazdu poza granice Rzeczypospolitej Polskiej trwającego dłużej niż 6 miesięcy, seria, numer i data ważności ostatniego wydanego dowodu osobistego obywatela polskiego oraz oznaczenie organu wydającego dokument, seria, numer i data ważności ostatniego wydanego paszportu obywatela polskiego, data zgonu albo data znalezienia zwłok, numer aktu zgonu i oznaczenie urzędu stanu cywilnego, w którym ten akt został sporządzony.
Podstawa prawna:	Ustawa z dnia 24 września 2010 r. o ewidencji ludności (Dz.U.2015.388 j.t.).
Przepływ danych:	Zbiór służy do przetwarzania danych w ramach Rejestru wyborców –osób uprawnionych do głosowania (ta sama baza danych). Subskrypcja danych z systemu Źródło do SELWIN.

23.

Nazwa zbioru:	**Rejestr zamieszkałych cudzoziemców**
Status zbioru:	Administrator Danych Osobowych powołał Administratora Bezpieczeństwa Informacji, w związku z tym ma zastosowanie art. 43 ust. 1a.
Forma przetwarzania danych:	Elektroniczna za pomocą systemu Źródło, programuElektroniczna za pomocą systemu Źródło, programuSEWLWIN, (Sygnity) oraz papierowa.
Struktura zbioru danych:	nazwisko i imię (imiona), data urodzenia, kraj urodzenia, płeć, numer PESEL, obywatelstwo albo status bezpaństwowca, adres i data zameldowania na pobyt stały, kraj miejsca zamieszkania, kraj

	poprzedniego miejsca zamieszkania, data wymeldowania z miejsca pobytu stałego, seria, numer i data ważności dokumentu podróży cudzoziemca, a w przypadku cudzoziemców, o których mowa w art. 7 ust. 1 pkt 3 lit. a i b, ważnego dokumentu podróży lub innego ważnego dokumentu potwierdzającego tożsamość i obywatelstwo; Pozostałe dane o ile są dostępne, mianowicie: imiona i nazwiska rodowe rodziców, miejsce urodzenia, stan cywilny, numer aktu urodzenia i oznaczenie urzędu stanu cywilnego, w którym ten akt został sporządzony, imię i nazwisko rodowe oraz numer PESEL małżonka, jeżeli został mu nadany, data zawarcia związku małżeńskiego, numer aktu małżeństwa i oznaczenie urzędu stanu cywilnego, w którym ten akt został sporządzony, data rozwiązania, związku małżeńskiego, sygnatura akt i oznaczenie sądu, który rozwiązał małżeństwo, sygnatura akt i oznaczenie sądu, który ustalił nieistnienie małżeństwa, sygnatura akt i oznaczenie sądu, który unieważnił małżeństwo, data zgonu małżonka albo data znalezienia jego zwłok, numer jego aktu zgonu i oznaczenie urzędu stanu cywilnego, w którym ten akt został sporządzony, adres i data zameldowania na pobyt czasowy oraz data upływu deklarowanego terminu pobytu, data wymeldowania z miejsca pobytu czasowego, data wyjazdu poza granice Rzeczypospolitej Polskiej trwającego dłużej niż 6miesięcy i wskazanie kraju wyjazdu, data powrotu z wyjazdu poza granice Rzeczypospolitej Polskiej trwającego dłużej niż 6 miesięcy, data upływu deklarowanego przez cudzoziemca terminu pobytu, data zgonu albo data znalezienia zwłok, numer aktu zgonu i oznaczenie, urzędu stanu cywilnego, w którym ten akt został sporządzony.
Podstawa prawna:	Ustawa z dnia 24 września 2010 r. o ewidencji ludności (Dz.U.2015.388 j.t.).
Przepływ danych:	Subskrypcja danych z systemu Źródło do SELWIN.

24.

Nazwa zbioru:	**Akta Stanu Cywilnego** **Obejmuje:** • Księgi Stanu Cywilnego, • Dokonywanie wzmianek dodatkowych w aktach stanu cywilnego, • Wydawanie z rejestru stanu cywilnego odpisów i zaświadczeń, • Unieważnienia, sprostowania, ustalania treści, odtwarzania i uzupełniania aktów stanu cywilnego,

	• Przyjmowanie oświadczeń z zakresu Urzędu Stanu Cywilnego, • Dokonywanie aktualizacji danych w rejestrze PESEL.
Status zbioru:	Zbiór podlega zgłoszeniu do rejestracji GIODO z uwagi na art. 27 ust. 1.
Forma przetwarzania danych:	Elektroniczna za pomocą systemu Źródło, programuPB_USC, EKSPORT USC (Technika IT.)oraz papierowa.
Struktura zbioru danych:	Nazwiska i imiona, imiona rodziców, data urodzenia, adres zamieszkania lub pobytu, numer PESEL, seria i numer dowodu osobistego, nazwisko: panieńskie, z poprzedniego małżeństwa, rodowe, miejsce i godzina urodzenia, data i numer aktu: urodzenia, małżeństwa, zgonu, nazwisko i imię: ojca, matki, współmałżonka, płeć, stan cywilny, data i miejsce zawarcia małżeństwa, nazwisko i imię, adres osoby zgłaszającej zgon, numer aktu zgonu żony, męża, imię i nazwisko rodowe małżonka, nazwisko rodowe matki i ojca kobiety, mężczyzny, data unieważnienia aktu małżeństwa, urodzenia, zgonu, imię nadane z urzędu, data i numer orzeczenia sądu ustalającego ojcostwo, zaprzeczającego ojcostwo, przysposabiającego dziecko, imię i nazwisko przysposabiającej dziecko, zmiana nazwiska dziecka, rejestracja w polskich księgach stanu.
Podstawa prawna:	Ustawa z dnia 28 listopada 2014 r. Prawo o aktach stanu cywilnego (Dz.U.2014.1741).
Przepływ danych:	Subskrypcja danych z systemu Źródło do PB_USC.

25.

Nazwa zbioru:	**Gminna Komisja Rozwiązywania Problemów Alkoholowych**
Status zbioru:	Zbiór podlega zgłoszeniu do rejestracji GIODO z uwagi na art. 27 ust. 1.
Forma przetwarzania danych:	Elektroniczna za pomocą pakietu biurowego MS Office oraz papierowa
Struktura zbioru danych:	imię i nazwisko, adres zamieszkania, status rodzinny, źródło i wysokość dochodów, wykształcenie, PESEL, data urodzenia, **dane wrażliwe: stan zdrowia, nałogi.**
Podstawa prawna:	Ustawa z dnia 26 października 1982 r. o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi (Dz. U. z 2015 r., 1286 ze zm.).

26.

Nazwa zbioru:	**Rejestr skazanych- nieodpłatna kontrolowana praca fizyczna na cele społeczne przydzielona przez Sąd**
Status zbioru:	Zbiór podlega zgłoszeniu do rejestracji GIODO z uwagi na art. 27 ust. 1.
Forma przetwarzania danych:	Elektroniczna za pomocą pakietu biurowego Office oraz papierowa.
Struktura zbioru danych:	imię i nazwisko, adres zamieszkania, data i miejsce urodzenia, okres wykonywania kary, orzeczenie o skazaniu.
Podstawa prawna:	Ustawa z dnia 6 czerwca 1997 r. Kodeks karny wykonawczy (Dz. U. z 1997r. Nr 90,poz. 557 ze zmianami).
Opis powiązań oraz przepływ danych:	brak

27.

Nazwa zbioru:	**Woda i ścieki** Zbiór przetwarzany jest w zakresie wystawienia faktury za dostawę wody i odprowadzanie ścieków.
Status zbioru:	Administrator Danych Osobowych powołał Administratora Bezpieczeństwa Informacji, w związku z tym ma zastosowanie art. 43 ust. 1a.
Forma przetwarzania danych:	Papierowa i elektroniczna za pomocą programu „Hydrosoft" Anko System Sp. z o.o. Przetwarzanie zbioru ma miejsce na urządzeniach przenośnych także poza obszarem przetwarzania danych. Dane wytworzone na urządzeniach przenośnych są eksportowane do lokalnego zbioru Woda i ścieki oraz z lokalnego zbioru do urządzenia przenośnego.
Struktura zbioru danych:	imię i nazwisko, adres zamieszkania, PESEL, NIP, stan i numer wodomierza, nr telefonu

Podstawa prawna:	Ustawa z dnia 7 czerwca 2001 r. o zbiorowym zaopatrzeniu w wodę i zbiorowym odprowadzaniu ścieków (Dz.U.2015.139 j.t.).

28.

Nazwa zbioru:	**Karta Dużej Rodziny**
Status zbioru:	Procesor Zbiór powierzony do przetwarzania do Miejskiego Ośrodka Pomocy Społecznej w Łaskarzewie.
Forma przetwarzania danych:	W postaci papierowej oraz dane z wniosków są wprowadzane do systemu RI KRD.
Struktura zbioru danych:	Imię, nazwisko, data urodzenia, PESEL, adres zamieszkania, adres korespondencyjny, dane członków rodziny: Imię, nazwisko, data urodzenia, PESEL, adres zamieszkania, adres korespondencyjny, termin ukończenia nauki w szkole, wskazanie kogo dotyczy dane dotyczą, wraz z określeniem jeśli występuje orzeczenie o stopniu niepełnosprawności.
Podstawa prawna:	Ustawa z dnia 5 grudnia 2014 r. o Karcie Dużej Rodziny (Dz.U.2014.1863).

29.

Nazwa zbioru:	**System Informacji Oświatowej** Zawiera informacje o kadrze nauczycielskiej zatrudnionej w placówkach oświatowych na terenie gminy.
Status zbioru:	Administrator Danych Osobowych powołał Administratora Bezpieczeństwa Informacji, w związku z tym ma zastosowanie art. 43 ust. 1a.
Forma przetwarzania danych:	Zbiór przetwarzany jest za pośrednictwem Systemu Informacji Oświatowej.
Struktura zbioru danych:	Data urodzenia, PESEL, miejsce pracy, zawód, wykształcenie, wysokość wynagrodzenia, płeć, forma i wymiar zatrudnienia, forma kształcenia i doskonalenia, stopień awansu zawodowego, przygotowanie pedagogiczne, staż pracy, wysokość dodatków

Podstawa prawna:	Ustawa z dnia 15 kwietnia 2011 r. o systemie informacji oświatowej (Dz. Dz.U.2015.45 j.t.)

30.

Nazwa zbioru:	**Awans zawodowy nauczycieli** Zawiera informacje o osobach ubiegających się o wyższy stopień awansu zawodowego w jednostkach oświatowych położonych na terenie gminy.
Status zbioru:	Administrator Danych Osobowych powołał Administratora Bezpieczeństwa Informacji, w związku z tym ma zastosowanie art. 43 ust. 1a.
Forma przetwarzania danych:	Elektroniczna za pomocą pakietu biurowego Office oraz papierowa.
Struktura zbioru danych:	Imiona, nazwisko, data urodzenia, adres zam., przebieg zatrudnienia, wykształcenie, miejsce pracy, wymiar zarudnienia.
Podstawa prawna:	Ustawa z dnia 26 stycznia 1982 r. Karta Nauczyciela (Dz. U. z 2014 r. poz. 191 i 1198 oraz z 2015 r. poz. 357 i 1268)

31.

Nazwa zbioru:	**Dofinansowanie kosztów kształcenia młodocianych pracowników**
Status zbioru:	Administrator Danych Osobowych powołał Administratora Bezpieczeństwa Informacji, w związku z tym ma zastosowanie art. 43 ust. 1a.
Forma przetwarzania danych:	Elektroniczna za pomocą pakietu biurowego Office oraz papierowa.
Struktura zbioru danych:	imię i nazwisko, adres zamieszkania, numer ewidencyjny PESEL, nr rachunku bankowego
Podstawa prawna:	Ustawa z dnia 7 września 1991 r. systemie oświaty (Dz. U. z 1991 r. Nr 95, poz. 425 z późn. zm.)

32.

Nazwa zbioru:	**Pomoc materialna dla uczniów (Stypendia)**
Status zbioru:	Zbiór podlega rejestracji do GIODO z uwagi na art. 27 ust. 1
Forma przetwarzania danych:	Papierowa oraz elektroniczna za pomocą programu „Pomoc materialna dla uczniów" Sputnik Software.
Struktura zbioru danych:	imię i nazwisko,imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania i pobytu stałego, miejsce pracy, zawód, wykształcenie, numer PESEL, dochody, stan zdrowia, orzeczenie o niepełnosprawności, sytuacja mieszkaniowa, nałogi, numer telefonu, informacja o korzystaniu z pomocy społecznej, informacja o alimentach, potwierdzeni zdarzenia losowego, nr konta bankowego, informacja o wychowaniu w rodzinie niepełnej, szkoła do której uczęszcza uczeń.
Podstawa prawna:	Ustawa z dnia 7 września 1991 r. systemie oświaty (Dz. U. z 1991 r. Nr 95, poz. 425 z późn. zm.)

33.

Nazwa zbioru:	**Płace-pracownicy Oświaty**
Status zbioru:	Administrator Danych Osobowych powołał Administratora Bezpieczeństwa Informacji, w związku z tym ma zastosowanie art. 43 ust. 1a.
Forma przetwarzania danych:	Papierowa i elektroniczna za pomocą programu „PłaceOptivum" Vulcan, Płatnika-aplikacja udostępniona przez ZUS, pakietu MS Office.
Struktura zbioru danych:	imię i nazwisko, nazwisko rodowe, imiona rodziców, data i miejsce urodzenia, adres zamieszkania, korespondencyjny, numer ewidencyjny PESEL, Numer Identyfikacji Podatkowej, dokumentacja kandydata do pracy, miejsce pracy, zawód, wykształcenie, seria i numer dowodu osobistego, numer telefonu, nr konta bankowego.
Podstawa prawna:	Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy (Dz. U. z 2014 r. poz. 1502, 1662 z późn. zm.)
Przepływ danych:	Eksport danych z programu „Płace" do home banking i Płatnika. Eksport danych w postaci elektronicznej do ZUS, transmisja zabezpieczona metodami kryptograficznymi.

34.

Nazwa zbioru:	**Archiwum**
Status zbioru:	Zbiór jest zwolniony z rejestracji na podstawie art. 43. ust.1 pkt 12.
Forma przetwarzania danych:	Papierowa
Struktura zbioru danych:	Wszystkie dane występujące w zbiorach opisanych w niniejszym wykazie.
Podstawa prawna:	Ustawa z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz.U.2011, poz. 123, nr 698).

Załącznik nr 2 do Polityki bezpieczeństwa informacji	*Tytuł* **Wykaz budynków i pomieszczeń**	

Urząd Miasta Łaskarzew ul. Duży Rynek 32, 08-450 Łaskarzew.

Pomieszczenia tworzące obszar przetwarzania danych osobowych:

Parter:

Nr	Nazwa
3	Referat finansowy, kasa, podatki
4	Referat zarządzania oświatą
5	Urząd Stanu Cywilnego
6	Sala ślubów

I piętro:

Nr	Nazwa
7	Sekretariat
8	Burmistrz Miasta Łaskarzew
9	Sekretarz Miasta Łaskarzew
10	Referat finansowo- budżetowy, Skarbnik

II piętro:

Nr	Nazwa
11	Ewidencja ludności, obsługa Rady Miasta
12 i 13	Referat inwestycji, budownictwa, gospodarki nieruchomościami, ochrony środowiska i rolnictwa, zamówienia publiczne
17	Referat organizacyjny, promocja miasta, informatyzacja
18	Referat organizacyjny, ewidencja działalności gospodarczej, zarządzanie kryzysowe i obrona cywilna

Serwerownia:

Znajduje się na drugim piętrze budynku, wejście do Serwerowni zabezpieczone jest poprzez drzwi antywłamaniowe. Serwerownia wyposażona jest w klimatyzację oraz alarm klimatyzacja, alarm wyzwalany czujnikiem otwarcia drzwi. Urządzenia sieciowe podłączone pod UPS.

Załącznik nr 3 do Polityki bezpieczeństwa informacji	*Tytuł* **Sposób przepływu danych pomiędzy systemami informatycznymi przetwarzającymi dane osobowe**	

Systemy informatyczne przetwarzające dane osobowe oraz przepływ danych pomiędzy programami informatycznymi przetwarzającymi dane osobowe zostały wyszczególnione w załączniku nr 1.

Załącznik nr 4 do Polityki bezpieczeństwa informacji	*Tytuł* **Oświadczenie o znajomości Polityki bezpieczeństwa informacji**	

OŚWIADCZENIE

Oświadczam, iż zostałam/zostałem zaznajomiona/zaznajomiony z przepisami dotyczącymi ochrony danych osobowych, w szczególności ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (tekst jednolity: Dz. U. 2014 r. poz.1182), wydanych na jej podstawie aktów wykonawczych oraz wdrożonej **Polityce bezpieczeństwa informacji wraz załącznikami.**

Ponad to oświadczam, iż zostałam/zostałem zaznajomiona/zaznajomiony z faktem, iż systemy informatyczne, do których mam dostęp na komputerach służbowych i na których wykonuję obowiązki pracownicze, są monitorowane, w zakresie ilościowego i jakościowego wykorzystania tych systemów.

Oświadczam, że monitoring obejmuje również sposób wykorzystania służbowej poczty elektronicznej. Zobowiązuję się do wykorzystywania jej jedynie w celu realizacji zadań pracowniczych, wynikających ze stosunku pracy.

(podpis osoby składającej oświadczenie)

Załącznik nr 5 do Polityki bezpieczeństwa informacji	*Tytuł* **Oświadczenie o zachowaniu poufności**	

OŚWIADCZENIE

Ja niżej podpisana/podpisany..... zobowiązuję się do zachowania w tajemnicy danych osobowych, do których mam lub będę miała/miał* dostęp w związku z wykonywaniem przeze mnie zadań służbowych i obowiązków pracowniczych, zarówno w trakcie obowiązującego stosunku pracy, jaki bezterminowo po ustaniu zatrudnienia.

Oświadczam, że przyjmuję do wiadomości, iż postępowanie sprzeczne z powyższymi zobowiązaniami może zostać uznane za ciężkie naruszenie podstawowych obowiązków pracowniczych, w rozumieniu art. 52 § 1 Kodeksu Pracy, oraz że może spowodować inne sankcje przewidziane przepisami prawa.

.....

(podpis składającego oświadczenie)

* - niepotrzebne skreślić

331

Załącznik nr 6 do Polityki bezpieczeństwa informacji	*Tytuł* **Przegląd i aktualizacja Polityki bezpieczeństwa informacji**	

L.p.	Data aktualizacji	Rodzaj wprowadzonej zmiany
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		

Załącznik nr 7 do Polityki bezpieczeństwa informacji	*Tytuł* **Wzór protokołu z kontroli uprawnień**	

L.p.	**Data dokonania kontroli uprawnień**	**Użytkownik, którego kontrola dotyczy**
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		
11.		
12.		
13.		
14.		
15.		
16.		
17.		
18.		
19.		
20.		

1. W obszarze przetwarzania danych osobowych wykonuje się kopie:
   1) przetwarzanych zbiorów danych osobowych, w postaci:
   a) plików komputerowych,
   b) baz danych działających na lokalnych komputerach lub serwerze głównym,
   c) aplikacji służących do ich przetwarzania.
   2) Innych materiałów w postaci elektronicznej nie zawierające danych osobowych.
2. Osobą odpowiedzialną za wykonywanie kopii zapasowych jest Administrator Systemu Informatycznego.

Tabela wykonywanych kopii:

Zakres danych objętych kopią zapasową	Bazy danych wszystkich systemów dziedzinowych – bazy znajdujące się lokalnie na stacjach roboczych kopiowane są na serwer
Harmonogram kopii zapasowych	Poniedziałek-Piątek, FerroBackup, kopie pełne, na dysk serwera kopii zapasowych i replikowane na taśmę streamera
Przechowywanie nośników zawierających kopie zapasowe	Taśmy z kopiami magazynowane są w sejfie w kasie.

Załącznik nr 9 do Polityki bezpieczeństwa informacji	*Tytuł* **Polityka szczegółowa dotycząca korzystania z poczty elektronicznej**	

Zasady korzystania z poczty elektronicznej

1. Przesyłanie danych osobowych z użyciem maila poza organizację może odbywać się tylko przez osoby do tego upoważnione.

2. W przypadku przesyłania informacji wrażliwych wewnątrz organizacji, bądź wszelkich danych osobowych poza organizację należy wykorzystywać mechanizmy kryptograficzne (hasłowanie wysyłanych plików, podpis elektroniczny).

3. W przypadku zabezpieczenia plików hasłem, obowiązuje minimum 8 znaków: duże i małe litery, cyfry lub znaki specjalne a hasło należy przesłać odrębnym mailem lub inną metodą, np. telefonicznie lub SMS-em.

4. Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu.

5. Zaleca się, aby użytkownik podczas przesyłania danych osobowych mailem zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata.

6. Nie należy otwierać załączników (plików) w mailach nadesłanych przez nieznanego nadawcę lub podejrzanych załączników nadanych przez znanego nadawcę.

7. Użytkownicy nie powinni rozsyłać za pośrednictwem maila informacji o zagrożeniach dla systemu informatycznego, „łańcuszków szczęścia", itp.

8. Użytkownicy nie powinni rozsyłać maili zawierających załączniki o dużym rozmiarze.

9. Użytkownicy powinni okresowo kasować niepotrzebne maile.

10. Podczas wysyłania maili do wielu adresatów jednocześnie należy użyć metody „Ukryte do wiadomości-UDW".

11. Mail jest przeznaczony wyłącznie do wykonywania obowiązków służbowych.

12. Użytkownicy mają prawo korzystać z maili dla celów prywatnych wyłącznie okazjonalnie i powinno być to ograniczone do niezbędnego minimum.

13. Korzystanie z maila dla celów prywatnych nie może wpływać na jakość i ilość świadczonej przez użytkownika pracy oraz na prawidłowe i rzetelne wykonywanie przez niego obowiązków służbowych.

14. Przy korzystaniu z maila, użytkownicy mają obowiązek przestrzegać prawa własności i prawa autorskiego.

15. Użytkownicy nie mają prawa korzystać z maila w celu rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec powszechnie obowiązujących zasad postępowania.

16. Użytkownik bez zgody Administratora Danych Osobowych nie ma prawa wysyłać wiadomości zawierających dane osobowe dotyczące pracowników, klientów, dostawców lub kontrahentów za pośrednictwem Internetu, w tym przy użyciu prywatnej elektronicznej skrzynki pocztowej.

Załącznik nr 10 do Polityki bezpieczeństwa informacji	*Tytuł* **Dziennik zdarzeń/incydentów**	

Data wystąpienia incydentu	**Rodzaj incydentu**	**Osoba, która przyczyniła się do wystąpienia incydentu**	**Podjęte działania**	**Osoba podejmująca działanie**	**Stopień zagrożenia**

Załącznik nr 11 do Polityki bezpieczeństwa informacji	*Tytuł* **Polityka szczegółowa dotycząca bezpiecznego użytkowania sprzętu IT**	

Zasada bezpiecznego użytkowania sprzętu IT

Sprzęt IT służący do przetwarzania zbioru danych osobowych składa się z komputerów stacjonarnych, laptopów, serwerów, drukarek.

Użytkownik zobowiązany jest korzystać ze sprzętu IT w sposób zgodny z jego przeznaczeniem i chronić go przed jakimkolwiek zniszczeniem lub uszkodzeniem.

Użytkownik zobowiązany jest do zabezpieczenia sprzętu IT przed dostępem osób nieupoważnionych a w szczególności zawartości ekranów monitorów.

Użytkownik ma obowiązek natychmiast zgłosić utratę lub zniszczenie powierzonego sprzętu IT.

Samowolne otwieranie (demontaż) sprzętu IT, instalowanie dodatkowych urządzeń (np. twardych dysków, pamięci) lub podłączenie jakichkolwiek niezatwierdzonych urządzeń do systemu informatycznego jest zabronione.

Pracownicy nie mogą korzystać z prywatnego sprzętu IT (np. laptopów, nośników typu pendrive) do wykonywania zadań służbowych.

Załącznik nr 12 do Polityki bezpieczeństwa informacji	*Tytuł* **Polityka szczegółowa dotycząca korzystania z oprogramowania**	

Zasady korzystania z oprogramowania

1. Użytkownik zobowiązuje się do korzystania wyłącznie z oprogramowania dopuszczonego do stosowania w jednostce.
2. Użytkownik nie ma prawa kopiować oprogramowania zainstalowanego na sprzęcie IT przez Pracodawcę na swoje własne potrzeby ani na potrzeby osób trzecich.
3. Instalowanie jakiegokolwiek oprogramowania na sprzęcie IT może być dokonane wyłącznie przez osobę upoważnioną.
4. Użytkownicy nie mają prawa do instalowania ani używania oprogramowania innego, niż przekazane lub udostępnione im przez Administratora Danych Osobowych. Zakaz dotyczy między innymi instalacji oprogramowania z zakupionych dyskietek, płyt CD, programów ściąganych ze stron internetowych, a także odpowiadania na samoczynnie pojawiające się reklamy internetowe.
5. Użytkownicy nie mają prawa do zmiany parametrów systemu, które mogą być zmienione tylko przez osobę upoważnioną.
6. W przypadku naruszenia któregokolwiek z powyższych postanowień Administrator Systemu Informatycznego ma prawo niezwłocznie i bez uprzedzenia usunąć nielegalne lub niewłaściwie zainstalowane oprogramowanie.

Załącznik nr 13 do Polityki bezpieczeństwa informacji	*Tytuł* **Polityka szczegółowa dotycząca korzystania z Internetu**	

Zasady korzystania z Internetu

1. Zabrania się zgrywania na dysk twardy komputera oraz uruchamiania jakichkolwiek programów nielegalnych oraz plików pobranych z niewiadomego źródła. Pliki takie powinny być ściągane tylko za każdorazową zgodą Administratora Bezpieczeństwa Informacji i tylko w uzasadnionych przypadkach.
2. Użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie instalowane z Internetu bez zgody osób upoważnionych.
3. Zabrania się wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, hackerskim, pornograficznym lub innym zakazanym przez prawo (na większości stron tego typu jest zainstalowane szkodliwe oprogramowanie, infekujące w sposób automatyczny system operacyjny komputera szkodliwym oprogramowania).
4. Nie należy w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania hasła.
5. W przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, należy zwracać uwagę na pojawienie się odpowiedniej ikonki (kłódki) oraz adresu www rozpoczynającego się frazą „https:"
6. Należy zachować szczególną ostrożność w przypadku żądania lub prośby podania kodów, PIN-ów, numerów kart płatniczych przez Internet. Szczególnie tyczy się to żądania podania takich informacji przez rzekomy bank.
7. Użytkownicy mogą także korzystać z Internetu dla celów prywatnych, ale wyłącznie okazjonalnie i powinno być ono ograniczone do niezbędnego minimum.
8. Korzystanie z Internetu dla celów prywatnych nie może wpływać na jakość i ilość świadczonej przez użytkownika pracy oraz na prawidłowe i rzetelne wykonywanie przez niego obowiązków służbowych, a także na wydajność systemu informatycznego Pracodawcy.
9. Przy korzystaniu z Internetu, użytkownicy mają obowiązek przestrzegać prawa własności i prawa autorskiego.

10. W zakresie dozwolonym przepisami prawa, Administrator Danych Osobowych zastrzega sobie prawo kontrolowania sposobu korzystania przez użytkownika z Internetu pod kątem wyżej opisanych zasad.
11. Ponadto, w uzasadnionym zakresie, Pracodawca zastrzega sobie prawo do kontroli czasu spędzonego przez użytkownika w Internecie.
12. Pracodawca może również blokować dostęp do niektórych treści dostępnych przez Internet.

Załącznik nr 14 do Polityki bezpieczeństwa informacji	*Tytuł* **Upoważnienia do przetwarzania danych osobowych**	

_____, _____

(miejscowość) (data)

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Na podstawie art. 37 ustawy z dn. 29 sierpnia 1997r. o ochronie danych osobowych (tekst. jedn. 2014, poz. 1182 z późn. zm.) upoważniam pracownika:

Pana/ Panią .....

Zatrudnionego/zatrudnioną w _____ na stanowisku – _____ do przetwarzania danych osobowych w celach związanych z wykonywaniem obowiązków służbowych, w zakresie:

a) _____

b) _____

c) _____

d) _____

Upoważnienie obowiązuje na czas trwania stosunku pracy, stanowiącego podstawę do przetwarzania danych, tj. do _____

_____ _____

(pieczęć administratora danych) (miejscowość, data)

Załącznik nr 15 do Polityki bezpieczeństwa informacji	*Tytuł* **Uprawnienia w systemach dziedzinowych**	*Sygn. dok*

Imię i nazwisko pracownika:		
System dziedzinowy	**ID**	**Poziom uprawnień**
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		

Załącznik nr 16 do Polityki bezpieczeństwa informacji	*Tytuł* **Ewidencja osób upoważnionych do przetwarzania danych**	

EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

Ewidencja osób upoważnionych

Lp.	Imię i nazwisko	Stanowisko/Funkcja	Data nadania	Data ustania	Zakres upoważnienia	Identyfikator

.....

(Podpis osoby upoważnionej do prowadzenia ewidencji)

Lp.	Imię i nazwisko	Stanowisko/Funkcja	Data nadania	Data ustania	Zakres upoważnienia	Identyfikator

.....

(Podpis osoby upoważnionej do prowadzenia ewidencji)

Lp.	Imię i nazwisko	Stanowisko/Funkcja	Data nadania	Data ustania	Zakres upoważnienia	Identyfikator

.....

(Podpis osoby upoważnionej do prowadzenia ewidencji)

Lp.	Imię i nazwisko	Stanowisko/Funkcja	Data nadania	Data ustania	Zakres upoważnienia	Identyfikator

.....

(Podpis osoby upoważnionej do prowadzenia ewidencji)

Załącznik nr 17 do Polityki Bezpieczeństwa Informacji	*Tytuł* **Struktura rejestru zbiorów prowadzonego przez Administratora Bezpieczeństwa Informacji.**	

1. W stosunku do każdego zbioru danych w rejestrze znajdują się następujące informacje:
    1) Nazwa zbioru danych
    2) Oznaczenie Administratora Danych i adres jego siedziby lub miejsca zamieszkania oraz numer identyfikacyjny rejestru podmiotów gospodarki narodowej, jeżeli został mu nadany
    3) Jeżeli został wyznaczony, oznaczenie przedstawiciela Administratora Danych, o którym mowa w art. 31a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych zwanej dalej „ustawą" i adres jego siedziby lub miejsca zamieszkania
    4) W przypadku powierzenia przetwarzania danych, oznaczenie podmiotu któremu powierzono przetwarzanie danych ze zbioru na podstawie art. 31 ustawy i adres jego siedziby lub miejsca zamieszkania.
    5) Podstawa prawna upoważniająca do prowadzenia zbioru danych
    6) Cel przetwarzania danych w zbiorze.
    7) Opis kategorii osób, których dane są przetwarzane w zbiorze.
    8) Zakres danych przetwarzanych w zbiorze.
    9) Sposób zbierania danych do zbioru.
    10) Sposób udostępniania danych ze zbioru.
    11) Oznaczenie odbiorcy danych lub kategorii odbiorców, którym dane mogą być przekazywane
    12) Informacje dotyczące ewentualnego przekazywania danych do państwa trzeciego w rozumieniu art.7 pkt ustawy.
2. W stosunku do zbioru danych w rejestrze podaje się także datę dokonania wpisu informacji, o których mowa w ust. 1 oraz ich ostatniej aktualizacji.
3. W przypadku wykreślenia zbioru danych z rejestru, w rejestrze wskazuje się nazwę zbioru danych oraz datę wpisania i wykreślenia zbioru danych.
4. Informacje o których mowa w ust 1 i daty dokonania wpisu tych informacji oraz ich ostatniej aktualizacji są udostępniane w rejestrze w powszechnie zrozumiałej formie, wg. Kolejności określonej w ust. 1

Burmistrz Miasta Łaskarzew

mgr Lidia Sopel-Sereja