ZAMEK CIESZYN
43-400 Cieszyn, ul. Zamkowa 3 a b c
NIP 5482634242, REGON 241812688
nr tel/fax: +48 33 851 08 21
www.zamekcieszyn.pl

ZARZĄDZENIE NR3a/2015
Dyrektora Zamku Cieszyn z dnia 30 czerwca 2015 r.
w sprawie wprowadzenia zasad ochrony danych osobowych
oraz zasady zabezpieczania systemów komputerowych w Zamku Cieszyn

Na podstawie § 6 ust. 2 Statutu Zamku Cieszyn stanowiącego załącznik do Uchwały nr XXVII/282/12 Rady Miejskiej w Cieszynie z dnia 20 grudnia 2012 roku r. oraz art. 3 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz. U. z 2014 r., poz. 1182 z późn. zm.), zwanej dalej „ustawą", zarządzam, co następuje:

---

§ 1

Wprowadzam zasady ochrony danych osobowych oraz zasady zabezpieczania systemów komputerowych w Zamku Cieszyn, zapisane w:
- „Polityce Bezpieczeństwa danych osobowych Zamku Cieszyn" *(załącznik nr 1).*
- „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.", zwanej dalej Instrukcją *(załącznik nr 2*).

§ 2

Przekazywanie danych osobom trzecim i innym podmiotom może być dokonywane jedynie w sposób zgodny z art. 29 ustawy, tj. pisemnie na wniosku o udostępnienie danych osobowych ze zbioru, chyba, że sposób udostępniania danych osobowych regulują postanowienia innych ustaw.

§ 3

Zobowiązuję pracowników do bezwzględnego stosowania *Polityki Bezpieczeństwa oraz Instrukcji,* zastosowania środków technicznych i organizacyjnych zapewniających ochronę danych osobowych, a w szczególności zabezpieczać dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy, utratą, uszkodzeniem lub zniszczeniem, zaś w szczególności do dokonywania zmiany haseł zabezpieczających dostęp do programów komputerowych, archiwizacji danych oraz definitywnego usuwania zbędnych danych.

§ 4

1. Każdy z pracowników przetwarzający dane otrzymuje pisemne upoważnienie do przetwarzania danych.
2. Każdy pracownik upoważniony do przetwarzania danych osobowych składa pisemne zobowiązanie, że zachowa w tajemnicy dane osobowe, z którymi zapozna się trakcie pracy, również po ustaniu zatrudnienia.
3. Zamek Cieszyn prowadzi ewidencję osób upoważnionych do przetwarzania danych.

Zarządzenie wchodzi w życie z dniem podpisania.

ZAMEK CIESZYN
dyrektor
Ewa Gołębiowska

ADWOKAT
Szymon Tutka

Załącznik nr 1 do Zarządzenia
Dyrektora Zamku Cieszyn z dnia 30 czerwca 2015 r.
w sprawie wprowadzenia zasad ochrony danych osobowych
oraz zasady zabezpieczania systemów komputerowych w Zamku Cieszyn

POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH ZAMKU CIESZYN

§1
Podstawa prawna

§3 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. nr 100 z 2004 r., poz. 1024), zwanym dalej Rozporządzeniem.

§2
Definicje

Ilekroć w Polityce Bezpieczeństwa danych osobowych Zamku Cieszyn jest mowa o:

1) **Administratorze Danych** – rozumie się przez to Zamek Cieszyn reprezentowany przez Dyrektora,
2) **Instrukcji** – rozumie się przez to Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, obowiązującą w Zamku,
3) **Pracowniku** – rozumie się przez to każdego pracownika Zamku zatrudnionego przy przetwarzaniu danych osobowych,
4) **Zbiorze danych** – rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych wg określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony, czy podzielony funkcjonalnie,
5) **Przetwarzaniu danych** – rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych,
6) **Systemie informatycznym** – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
7) **Identyfikatorze użytkownika** (nazwa użytkownika) – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,
8) **Haśle** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym,
9) **Uwierzytelnianiu** – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu,
10) **Rozliczalności danych** – rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi,
11) **Integralności danych** – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
12) **Pomieszczeniach** – rozumie się przez to budynek lub pomieszczenia lub części pomieszczeń określone przez Administratora danych, tworzące obszar, w którym przetwarzane są dane osobowe z użyciem stacjonarnego sprzętu komputerowego oraz gromadzone w kartotekach.
13) **Kontrahent** – osoba współpracująca z Zamkiem Cieszyn.

§3
Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe, zwany dalej Obszarem

Obszar, w którym przetwarzane są Dane Osobowe stanowią:

1) Gabinet Dyrektora,
2) Biuro administracji,
3) Biuro głównej księgowej,
4) Biura pracowników.

§4

Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych

1. Zamek przetwarza dane osobowe wyłącznie w zakresie niezbędnym do realizacji celów statutowych i dba o to, aby dane przetwarzane były zgodnie z prawem, zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami, merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane, przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.
2. Zamek podejmować będzie wszelkie wymagane przez przepisy prawa działania w celu ochrony danych przed dostępem do nich osób nieuprawnionych w sposób przewidziany w przepisach prawa.
3. Zamek przetwarza dane osobowe w następujących Zbiorach danych osobowych:
   1) zbiory prowadzone manualnie:
      a) w stosunku do pracowników:
         - akta osobowe,
         - ewidencja czasu pracy,
         - listy płac,
         - kartoteki zarobkowa pracowników,
         - rejestr delegacji służbowych pracowników,
         - deklaracje ubezpieczeniowe pracowników,
         - oświadczenia podatkowe pracowników,
         - dowody i dokumenty księgowe,
         - rejestr wypadków pracowników
      b) w stosunku do pozostałych osób:
         - dane zgromadzone na przechowywanych umowach.

   2) zbiory danych osobowych przetwarzane w systemach informatycznych:
      a) Zbiór danych finansowo-księgowych – do przetwarzania danych w tym zbiorze stosowany jest specjalistyczny program dostępny wyłącznie na stanowisku księgowym.
      b) Kadry - Płace – do przetwarzania danych w tym zbiorze stosowany jest specjalistyczny program dostępny wyłącznie na stanowisku kadrowym i stanowiskach księgowych bądź pisma są tworzone w programach opisanych w § 5 pkt. 4.
      c) Płatnik – do przetwarzania danych w tym zbiorze stosowany jest program Płatnik dystrybuowany przez Zakład Ubezpieczeń Społecznych.
      d) Pisma – do przetwarzania danych w tym zbiorze stosowany jest program Microsoft Office i inne edytory tekstu korzystające z ochrony oprogramowania zainstalowanego na danym komputerze.

§5

Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi

1. Zbiór danych finansowo – księgowych – dane przechowywane są w plikach formatu własnego specjalistycznego oprogramowania księgowego,
2. Płace – dane przechowywane są w plikach formatu własnego dedykowanego programu kadrowo - płacowego lub edytorów tekstu opisanych w pkt. 4,
3. Płatnik – dane przechowywane są w plikach bazy danych typu MS Access,
4. Pisma – dane przechowywane są w plikach typu *.doc, *.xls, *txt, *.pdf. i innych formatach uniwersalnych edytorów tekstu i poczty elektronicznej.

§6

Sposób przepływu danych pomiędzy systemami

Dopuszczalny jest import danych generowanych w programie kadrowym i księgowym w razie ich kompatybilności oraz importowanie danych do programu Płatnik.

§7

Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

Dla zapewnienia poufności, integralności i rozliczalności przetwarzania danych Zamek stosować będzie środki techniczne i organizacyjne właściwe dla wysokiego poziomu bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym, stosownie do wymogów określonych w załączniku do rozporządzenia:

1) **zabezpieczenie Obszaru:**
   a) Obszar zabezpieczony będzie przed dostępem osób nieuprawnionych na czas nieobecności w nim osób - upoważnionych do przetwarzania danych osobowych; przebywanie osób nieuprawnionych w Obszarze będzie dopuszczalne tylko za zgodą Dyrektora i w obecności osoby upoważnionej do przetwarzania danych osobowych.
   b) Drzwi do pomieszczeń znajdujących się na terenie Obszaru zaopatrzone są w zamek kluczowy.
   c) W wypadku chwilowego opuszczenia pomieszczenia przez pracownika w ciągu dnia pracy drzwi pozostawać będą zamknięte.
   d) Ekrany monitorów stanowisk dostępu do danych osobowych będą automatycznie wyłączane po upływie 3 minut nieaktywności pracownika.
   e) W pomieszczeniach, gdzie przebywają osoby postronne, monitory stanowisk dostępu do danych będą ustawiane w sposób uniemożliwiający tym osobom wgląd w dane.
2) **mechanizmy kontroli dostępu do danych:**
   a) W systemie informatycznym stosowane będą następujące mechanizmy kontroli dostępu do danych osobowych: hasła użytkowników do systemu operacyjnego.
   b) Dostęp do danych będą miały wyłącznie osoby, których zakres obowiązków uzasadnia uzyskiwanie danych – w zakresie pozostającym w związku z wykonywanymi przez te osoby obowiązkami. Dostęp do danych może mieć miejsce jedynie po podpisaniu przez pracownika oświadczenia o zachowaniu danych w tajemnicy.
   c) O dostępie poszczególnych osób do danych będzie decydował Administrator Danych dopuszczając do korzystania z oprogramowania bądź komputera zawierającego takie dane.
   d) Jeżeli dostęp do danych przetwarzanych w systemie informatycznym będą posiadać co najmniej dwie osoby, wówczas przetwarzanie danych odbywa się za wiedzą Administratora Danych bądź za pomocą urządzeń lub programów umożliwiających identyfikację osób przetwarzających dane osobowe.
3) **zabezpieczanie systemu informacyjnego** – system informatyczny jest zabezpieczony, w szczególności przed:
   a) Działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego – poprzez oprogramowanie antywirusowe, antyszpiegowskie oraz firewall,
   b) Utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej poprzez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych. Kopie zapasowe będą przechowywane w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem i usuwaniem niezwłocznie po ustaniu ich użyteczności.
   c) Dostępem osób nieuprawnionych do przetwarzania danych w systemie informatycznym poprzez:
   - stosowanie zabezpieczeń przewidzianych w Instrukcji oraz Polityce Bezpieczeństwa; osoba użytkująca komputer przenośny zawierający dane osobowe zobowiązana będzie do

zachowania szczególnej ostrożności podczas jego transportu, przechowywania i użytkowania poza Obszarem;

- pozbawienie wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie, a w przypadku, gdy nie jest to możliwe, uszkadzanie w sposób uniemożliwiający ich odczytanie urządzeń, dysków lub innych elektronicznych nośników informacji, zawierających dane osobowe przeznaczonych do likwidacji,
- w razie uzasadnionej konieczności przekazywanie nośników danych podmiotom zewnętrznym, działającym w ramach prowadzonej działalności, zobowiązanym do zachowania w tajemnicy tych danych na podstawie odrębnej klauzuli umownej.

§8

Ewidencja osób upoważnionych do przetwarzania danych osobowych

1. Ewidencję osób upoważnionych do przetwarzania danych osobowych prowadzi Administrator Danych.(załącznik Nr 1 do Polityki Bezpieczeństwa).
2. Ewidencja osób upoważnionych do przetwarzania danych jest poufna i zawiera:
   1) nazwisko i imię osoby upoważnionej,
   2) datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych.

§9

Udostępnianie danych ze zbioru

1. Na wniosek osoby, której dane dotyczą, administrator danych jest obowiązany, w terminie 30 dni, poinformować o przysługujących jej prawach oraz udzielić, odnośnie jej danych osobowych, informacji o których mowa w ust. 2 pkt 1-5 na piśmie.
2. Każdej osobie przysługuje prawo do kontroli przetwarzania danych, które jej dotyczą, zawartych w zbiorach danych, a zwłaszcza prawo do:
   1) uzyskania wyczerpującej informacji, czy taki zbiór istnieje, oraz do ustalenia administratora danych, adresu jego siedziby i pełnej nazwy,
   2) uzyskania informacji o celu, zakresie i sposobie przetwarzania danych zawartych w takim zbiorze,
   3) uzyskania informacji, od kiedy przetwarza się w zbiorze dane jej dotyczące oraz podania w powszechnie zrozumiałej formie treści tych danych,
   4) uzyskania informacji o źródle, z którego pochodzą dane jej dotyczące,
   5) uzyskania informacji o sposobie udostępniania danych, a w szczególności informacji o odbiorcach lub kategoriach odbiorców, którym dane te są udostępnione,
   6) żądania uzupełnienia, uaktualnienia, sprostowania danych osobowych, czasowego lub stałego wstrzymania ich przetwarzania lub ich usunięcia, jeżeli są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są już zbędne do realizacji, dla którego zostały zebrane,
   7) prawie wniesienia pisemnego, umotywowanego żądania zaprzestania przetwarzania jej danych ze względu na jej szczególną sytuację, jeżeli nawet przetwarzanie jest niezbędne do wypełnienia usprawiedliwionych celów administratora danych, a przetwarzanie danych nie narusza praw i wolności osoby, której dane dotyczą,
   8) wniesienie sprzeciwu wobec przetwarzania jej danych w przypadkach, gdy przetwarzanie jest niezbędne do wypełnienia usprawiedliwionych celów administratora danych, a przetwarzanie danych nie narusza praw i wolności osoby, której dane dotyczą, gdy administrator danych zamierza je przetwarzać w celach marketingowych lub wobec przekazywania jej danych osobowych innemu administratorowi danych,
   9) wniesienia do administratora danych żądania ponownego, indywidualnego rozpatrzenia sprawy rozstrzygniętej z naruszeniem zakazu ostatecznego rozstrzygnięcia indywidualnej sprawy, gdy treść była wyłącznie wynikiem operacji na danych osobowych prowadzonych w systemie informatycznym
3. Osoba zainteresowana może skorzystać z prawa do informacji, o których mowa w ust. 1 pkt 1-5, nie częściej niż raz na 6 miesięcy.

Postanowienia końcowe

§10

Polityka jest dokumentem wewnętrznym i nie może być udostępniana osobom postronnym w żadnej formie.

§11

1. Dyrektor zobowiązany jest do zapoznania z treścią Polityki każdego użytkownika.
2. Użytkownik zobowiązany jest złożyć oświadczenie, o tym, iż został zaznajomiony z przepisami o ustawie o ochronie danych osobowych oraz wydanymi na jej podstawie aktami wykonawczymi oraz instrukcjami obowiązującymi u Administratora Danych, a także o zobowiązaniu się do ich przestrzegania (załącznik nr 2 i nr 3 do Polityki Bezpieczeństwa).
3. Oświadczenia przechowywane są w aktach osobowych pracownika.
4. W sprawach nieuregulowanych w niniejszej Polityce oraz obowiązującej Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tekst jednolity: Dz. U. z 2014 r., poz. 1182 z późn. zm.) oraz wydanych na jej podstawie aktów wykonawczych.
5. Użytkownicy zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Polityce.

ZAMEK CIESZYN
dyrektor
Ewa Gołębiowska

Załącznik nr 2 do Zarządzenia
Dyrektora Zamku Cieszyn z dnia 30 czerwca 2015 r.
w sprawie wprowadzenia zasad ochrony danych osobowych
oraz zasady zabezpieczania systemów komputerowych w Zamku Cieszyn

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

§1
Postanowienia ogólne

1. Do zapoznania się z niniejsza Instrukcją zobowiązane są osoby upoważnione do przetwarzania danych osobowych w Zamku Cieszyn.
2. Określony przez instrukcję tryb postępowania obowiązuje w przypadku:
   1) stwierdzenia naruszenia zabezpieczenia systemu informatycznego,
   2) gdy stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy wskazują na naruszenie ochrony danych osobowych.

§2
Zasady upoważnienia osób do przetwarzania danych osobowych

1. Systemy komputerowe oraz urządzenia wchodzące w ich skład, a służące do przetwarzania danych mogą być obsługiwane tylko przez osoby upoważnione.
2. Dla każdej osoby upoważnionej do przetwarzania danych osobowych Administrator Danych ustala zakres dostępu do systemu.
3. Zmiana haseł następuje nie rzadziej niż co 30 dni. Za zmianę haseł odpowiedzialny jest pracownik, któremu przyporządkowane jest stanowisko komputerowe.
4. Zasady tworzenia haseł:
   1) hasło należy budować z minimum 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne,
   2) hasło powinno być łatwe do zapamiętania, ale nie powinno to być imię, nazwisko lub słowa potocznie stosowane.
5. Zabronione jest udostępnianie innym osobom hasła. Każdy użytkownik odpowiada za swoje hasło oraz za operacje wykonane w systemie komputerowym. Udostępnienie hasła może nastąpić wyłącznie w uzasadnionych przypadkach lub na polecenie przełożonego.

§4
Procedura rozpoczęcia i zakończenia pracy w systemach komputerowych służących do przetwarzania danych osobowych

1. Osoba upoważniona do przetwarzania danych osobowych powinna rozpocząć pracę w systemie komputerowym podając swoje hasło.
2. Pracę przy przetwarzaniu danych w systemie komputerowym należy zakończyć zgodnie z wymogami danego systemu i po potwierdzeniu operacji w prawidłowy sposób wyłączyć sprzęt komputerowy.

§5
Zasady zabezpieczenia danych osobowych

I. Środki organizacyjne zabezpieczające przed utratą danych

1. W Zamku Cieszyn dane osobowe przetwarzane są na wyznaczonym Obszarze, zgodnie z wykazem znajdującym się w Polityce Bezpieczeństwa.
2. Osoby postronne mogą przebywać w pomieszczeniach, w których przetwarzane są dane osobowe tylko w obecności osób upoważnionych lub po uzyskaniu pisemnej zgody Administratora Danych.
3. Monitory stanowisk komputerowych, gdzie przetwarzane są dane osobowe należy ustawić tak, aby uniemożliwić wgląd do nich osobom postronnym. Ekrany monitorów winny być automatycznie wyłączane po upływie możliwie najkrótszego czasu nieaktywności użytkownika.

4. Naprawa urządzeń, dysków lub innych nośników informacji zawierających dane osobowe, może odbywać się tylko w obecności i pod bezpośrednim nadzorem osoby upoważnionej do ich przetwarzania lub innego wyznaczonego Pracownika.
5. W przypadku niemożności zapewnienia nadzoru, o którym mowa w pkt. 4 urządzenia, dyski i inne nośniki informacji należy albo pozbawić zapisu zawierającego dane osobowe, albo w razie uzasadnionej konieczności przekazać podmiotom zewnętrznym, działającym w ramach prowadzonej działalności, zobowiązanym do zachowania w tajemnicy tych danych na podstawie odrębnej klauzuli umownej.
6. Przeglądy i konserwację systemów komputerowych zawierających dane osobowe, a będące w użytkowaniu Zamku Cieszyn mogą być wykonywane tylko w obecności osób upoważnionych do przetwarzania danych.

II. Środki techniczne zabezpieczające przed utratą danych

1. Urządzenia i systemy informatyczne, służące do przetwarzania danych osobowych, należy zabezpieczyć przed utratą tych danych z powodu awarii zasilania lub zakłóceń w sieci zasilającej poprzez zastosowanie nośników zewnętrznych (dysków lub innych nośników jak CD, DVD, na których regularnie zapisywane są dane jako kopie bezpieczeństwa).
2. Zarządza się okresową archiwizację danych i systemów, tj. zbioru danych finansowo-księgowych, płac, Płatnika – po każdorazowym użyciu.
3. Kopie archiwizacyjne należy sporządzać na dostępnych zewnętrznych nośnikach z opisem zawierającym:
   1) datę sporządzenia,
   2) informację o zawartości
   lub na odrębnym serwerze w folderach zawierających w nazwie datę sporządzenia oraz informację o zawartości i przechowywać w miejscu niedostępnym dla osób nieupoważnionych.
4. Wydruki zawierające dane osobowe, przeznaczone do usunięcia, należy bezwzględnie zniszczyć w sposób uniemożliwiający ich odczytanie.
5. Urządzenia, dyski lub inne nośniki informacji zawierające dane osobowe, a przeznaczone do likwidacji, należy zniszczyć w sposób uniemożliwiający ich odczytanie.
6. Sprzęt komputerowy należy podłączać wyłącznie do gniazd elektrycznych przeznaczonych do jego zasilania.
7. Zabrania się podłączania innych urządzeń (np. czajników, wentylatorów, radia) do gniazd wydzielonych sieci elektrycznej zasilającej sprzęt komputerowy.

III. Ochrona danych przed wirusami komputerowymi

1. Każdy zewnętrzny nośnik, z którego informacja będzie wprowadzana do komputera musi uprzednio zostać sprawdzony programem antywirusowym.
2. Stan dysku i pamięci systemu komputerowego, wyposażonego w urządzenia do wprowadzania informacji z zewnątrz, należy co tydzień sprawdzać programem antywirusowym.
3. W przypadku zainstalowania nowych programów komputerowych służących do obsługi zbiorów danych osobowych należy je zarejestrować w rejestrze.

§6
Tryb postępowania w przypadku naruszenia ochrony danych osobowych w autonomicznych systemach komputerowych

1. Tryb postępowania obowiązuje w przypadku, gdy:
   1) stwierdzono naruszenie zabezpieczenia autonomicznego systemu informatycznego,
   2) stan urządzenia, zawartość zbioru danych, ujawnione metody pracy mogą wskazywać na naruszenie zabezpieczenia tych danych.
2. Każda osoba zatrudniona w Zamku Cieszyn, która stwierdzi lub podejrzewa naruszenie zabezpieczenia ochrony danych osobowych w systemie informatycznym, powinna niezwłocznie poinformować o tym osobę zatrudnioną przy przetwarzaniu danych osobowych lub Administratora Danych.
3. Osoba zatrudniona przy przetwarzaniu danych osobowych, która uzyskała informację lub sama stwierdziła naruszenie zabezpieczenia bazy danych osobowych w systemie informatycznym, zobowiązana jest niezwłocznie powiadomić o tym Administratora Danych.
4. Osoba zatrudniona przy przetwarzaniu danych osobowych, która uzyskała informację lub sama stwierdziła naruszenie zabezpieczenia bazy danych osobowych powinna w pierwszej kolejności:

1) zapisać wszelkie informacje związane z danym wydarzeniem, a szczególnie: dokładny czas uzyskania informacji o naruszeniu danych osobowych i czas samodzielnego wykrycia tego faktu,
2) na bieżąco wygenerować i wydrukować (jeżeli zasoby systemu na to pozwalają) wszystkie możliwe dokumenty i raporty, które mogą pomóc w ustaleniu okoliczności zdarzenia, opatrzyć je datą i podpisem.
3) przystąpić do zidentyfikowania rodzaju zaistniałego zdarzenia do określenia skali zniszczeń i metody dostępu do danych osoby niepowołanej.

5. Po wyeliminowaniu bezpośredniego zagrożenia należy przeprowadzić wstępną analizę stanu systemu w celu potwierdzenia lub wykluczenia faktu naruszenia ochrony danych osobowych.
6. Pracownik, który uzyskał informację lub sam stwierdził naruszenie zabezpieczenia bazy danych osobowych powinien sprawdzić:
   1) stan urządzeń wykorzystywanych do przetwarzania danych osobowych,
   2) zawartość zbioru danych osobowych,
   3) sposób działania programu,
   4) wykluczyć możliwość obecności wirusów komputerowych.
7. Po przywróceniu prawidłowego stanu bazy danych osobowych Pracownik przygotowuje szczegółowy raport o zdarzeniu i przekazuje go Administratorowi Danych, który uwzględnia zdarzenie w prowadzonym rejestrze incydentów, rejestr stanowi zbiór raportów z opisem ewentualnych działań podjętych w celu zapobieżenia podobnym zdarzeniom.
8. Administrator Danych podejmuje decyzję o powiadomieniu Policji o fakcie naruszenia zabezpieczenia systemu komputerowego.

§7
Zasady bezpieczeństwa dla dokumentów papierowych zawierających dane osobowe

1. Dokumenty papierowe zawierające dane osobowe należy chronić:
   1) przed kradzieżą, zniszczeniem lub niewłaściwym używaniem,
   2) przed zagrożeniami ze strony otoczenia – ogień, woda itp.
2. Obowiązuje bezwzględna zasada fizycznej ochrony dokumentów papierowych zawierających dane osobowe. Przed wyjściem z pomieszczeń, w których przechowywane są ww. dokumenty należy sprawdzić czy są one właściwie zabezpieczone.
3. Dokumenty papierowe zawierające dane osobowe przeznaczone do usunięcia lub mające charakter dokumentu roboczego należy zniszczyć w sposób uniemożliwiający odczytane informacji w ich zawartych, w miarę możliwości przy użyciu niszczarki.
4. O każdym przypadku utraty lub zniszczenia dokumentów zawierających dane osobowe należy natychmiast zgłosić Administratorowi Danych lub innej upoważnionej osobie.

§8
Zasady odpowiedzialności za postępowanie niezgodne z zapisami niniejszej instrukcji

Odstępstwa od zapisów niniejszej instrukcji będą traktowane jako ciężkie naruszenie podstawowych obowiązków pracowniczych. Dodatkowo nieprzestrzeganie zasad zawartych w instrukcji skutkuje odpowiedzialnością cywilno – prawną i karną określoną w przepisach Kodeksu cywilnego (Dz. U. z 1964 r., nr. 16 poz. 93 z późn. zm.), kodeksu karnego (Dz. U. z 1997 r., nr 88 poz. 553) oraz ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 1997 r., nr 133, poz. 833).

ZAMEK CIESZYN
dyrektor
Ewa Gołębiowska

Załącznik nr 1 do Polityki Bezpieczeństwa
Danych Osobowych Zamku Cieszyn

Ustala się następującą listę osób zatrudnionych przez Administratora danych przy gromadzeniu i przetwarzaniu danych osobowych związanych z dział. placówki:

- w zakresie gromadzenia i przetwarzania danych osobowych pracowników placówki uprawnionymi są osoby zatrudnione na następujących stanowiskach:

1. Główny księgowy
2. Specjalista ds. administracyjno – kadrowych
3. Specjalista ds. obsługi i konserwacji urządzeń

- w zakresie gromadzenia i przetwarzania danych osobowych kontrahentów Zamku:

1. osoby jak wyżej
2. Kierownik Administracyjny
3. pracownicy merytoryczni poszczególnych działów.

Załącznik nr 2 do Polityki Bezpieczeństwa
Danych Osobowych Zamku Cieszyn

Imię i nazwisko pracownika:_____

Stanowisko służbowe: _____

Oświadczenie pracownika upoważnionego do przetwarzania danych

Jako pracownik upoważniony do gromadzenia i przetwarzania danych osobowych pracowników / kontrahentów*, które są gromadzone w zakresie niezbędnym do prawidłowego funkcjonowania Zamku Cieszyn zgodnie z przepisami ustawy o ochronie danych osobowych oświadczam, co następuje:

Zapoznałam/em się z treścią wyżej wymienionej ustawy oraz z treścią Polityki Bezpieczeństwa i Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych obowiązujących w Zamku Cieszyn, szczególnie w zakresie dotyczącym zasad gromadzenia i przetwarzania danych osobowych.

Zobowiązuję się do starannego i rzetelnego wykonywania wszystkich obowiązków wynikających z obowiązujących przepisów prawa i instrukcji wewnętrznych placówki.

Zobowiązuję się do zachowania w tajemnicy przed wszystkimi nieupoważnionymi, w świetle obowiązujących przepisów prawa, osobami trzecimi wszystkich danych osobowych, które gromadzę i przetwarzam w związku z wykonywaniem powierzonych mi obowiązków.

Zobowiązuję się do nie wykorzystywania, w celach innych niż prawidłowe wykonywanie powierzonych mi obowiązków, jakichkolwiek danych osobowych, które gromadzę i przetwarzam.

Cieszyn, dnia _____

_____
(podpis – imię i nazwisko pracownika)

* niepotrzebne skreślić

Potwierdzam, w imieniu pracodawcy, własnoręczność złożonego przez pracownika na niniejszym dokumencie podpisu.

Załącznik nr 3 do Polityki Bezpieczeństwa
Danych Osobowych Zamku Cieszyn

Imię i nazwisko pracownika:_____

Stanowisko służbowe: _____

Oświadczenie informacyjne dla pracowników Zamku Cieszyn

Zgodnie z wymogami ustawy o ochronie danych osobowych informuję Pana/Panią, że Administrator danych osobowych reprezentowany przez Dyrektora zbiera i przetwarza dane osobowe Pana/Pani oraz dane osobowe pozostałych członków Pana/Pani rodziny i osób pozostających we wspólnym gospodarstwie domowym, w zakresie niezbędnym do prawidłowego wykonywania obowiązków tej placówki jako zakładu pracy i innych wynikających z przepisów prawa obowiązków, a w szczególności w zakresie kadrowo-płacowym, statystyczno-sprawozdawczym i dotyczącym ubezpieczeń społecznych i zdrowotnych.

Informuję, jednocześnie, że przysługuje Panu/Pani prawo do wglądu danych oraz uzupełnienia, uaktualnienia oraz żądania prostowania zgromadzonych danych w razie stwierdzenia, że dane te są niekompletne, nieaktualne lub nieprawdziwe.

Jednocześnie informuję, że Administrator danych osobowych tj. Zamek Cieszyn dołoży wszelkich starań, aby dane były zbierane, przetwarzane i chronione zgodnie z prawem.

Cieszyn, dnia .....

.....
(podpis i pieczęć Administratora)

Oświadczenie pracownika

Oświadczam, że zapoznałem/-am się z przekazaną mi informacją dotyczącą zasad i potrzeb gromadzenia danych moich i danych członków mojej rodziny oraz pozostających ze mną we wspólnym gospodarstwie domowym.

Oświadczam także, że wyrażam zgodę na gromadzenie i przetwarzanie przez Administratora danych, tj. Zamek Cieszyn, danych osobowych moich, członków mojej rodziny oraz osób pozostających ze mną we wspólnym gospodarstwie domowym, w zakresie niezbędnym do prawidłowego wykonywania obowiązków tej placówki jako zakładu pracy i innych wynikających z przepisów prawa obowiązków, a w szczególności w zakresie kadrowo-płacowym, statystyczno-sprawozdawczym i dotyczącym ubezpieczeń społecznych i zdrowotnych.

Oświadczam także, iż zostałem/-am pouczony należycie o przysługujących mi uprawnieniach w zakresie możliwości wglądu do gromadzonych danych oraz o możliwości ich uzupełniania oraz żądania sprostowania w razie stwierdzenia, że dane te są niekompletne, nieaktualne lub nieprawdziwe.

Cieszyn, dnia ..... r.

.....
(podpis - imię i nazwisko pracownika)