ZAMEK CIESZYN
43-400 Cieszyn, ul. Zamkowa 3 a b c
NIP 5482634242, REGON 241812689
nr tel/fax: +48 33 851 08 21
www.zamekcieszyn.pl

Zarządzenie Nr 5/2018

Dyrektora Zamku Cieszyn

z dnia 25.05.2018

w sprawie wdrożenia „Polityki Bezpieczeństwa Informacji Zamku Cieszyn" i „Instrukcji Zarządzania Systemem Informatycznym Zamku Cieszyn"

Na podstawie art. 32 ust. 1 Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1)

§ 1

Wdrażam „Politykę Bezpieczeństwa Informacji Zamku Cieszyn" oraz „Instrukcję Zarządzania Systemem Informatycznym Zamku Cieszyn", które stanowią środki organizacyjne, o których mowa w art. 32 ust. 1 ogólnego rozporządzenia o ochronie danych.

§ 2

Dokumenty, o których mowa w § 1 stanowią załączniki do zarządzenia.

§ 3

Zobowiązuję wszystkich pracowników Zamku Cieszyn do zapoznania się z treścią dokumentów wymienionych w § 1 w zakresie niezbędnym do prawidłowego i bezpiecznego przetwarzania danych, w terminie do dnia 15.06.2018

§ 4

Zarządzenie wchodzi w życie z dniem podpisania.

§ 5

Traci moc Zarządzenie 3a/2015 Dyrektora Zamku Cieszyn z dnia 30.06.15 r.

ZAMEK CIESZYN
dyrektor
Ewa Gołębiowska

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

POLITYKA BEZPIECZEŃSTWA INFORMACJI ZAMKU CIESZYN

§ 1
Wstęp

1. Przyjęcie Polityki bezpieczeństwa informacji w Zamku Cieszyn, ma na celu ustanowienie jasnych zasad bezpieczeństwa informacji. Dyrektor Zamku Cieszyn deklaruje świadomość potrzeby ochrony danych osobowych i innych tajemnic ustawowo chronionych. Celem Polityki bezpieczeństwa informacji jest zapewnienie poufności, integralności i dostępności danych.
2. Polityka bezpieczeństwa informacji jest zbiorem zasad obowiązujących przy przetwarzaniu danych osobowych w Zamku Cieszyn.
3. Zasady określone w Polityce bezpieczeństwa informacji należy stosować również przy ochronie innych tajemnic ustawowo chronionych, o ile przepisy prawa nie zobowiązują do stosowania wyższego poziomu ochrony.
4. Celem Polityki bezpieczeństwa informacji jest zapewnienie odpowiednich standardów ochrony danych osobowych, w tym zapewnienia poufności, integralności i dostępności danych osobowych.
5. Szczegółowe zasady przetwarzania danych osobowych w systemie informatycznym Zamku Cieszyn zostały określone w Instrukcji Zarządzania Systemem Informatycznym.
6. Polityka bezpieczeństwa informacji jest dokumentem wchodzącym w zakres środków, o których mowa w art. 24 ust. 1 i art. 32 ust. 1 Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1).
7. Do środków, o których mowa ust. 6 należą również inne polityki ochrony danych, wytyczne wdrożone w Zamku Cieszyn lub skierowane do administratora danych przez Urząd Marszałkowski lub inny podmiot publiczny celem realizacji.
8. Podstawą prawną do opracowania dokumentu jest:
    1. Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1), zwanego dalej rozporządzeniem 2016/679.
    2. Ustawa o ochronie danych osobowych.
9. Podstawowe pojęcia:
    1. **Rozporządzenie 2016/679** - Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1).
    2. **UODO** – Ustawa o ochronie danych osobowych.
    3. **AD** – Administrator w rozumieniu art. 4 pkt 7 rozporządzenia 2016/679, Zamek Cieszyn reprezentowany przez Dyrektora;
    4. **Zamek Cieszyn** – samorządowa instytucja kultury działająca zgodnie ze Statutem;
    5. **Osoba upoważniona** – Osoba upoważniona przez AD do przetwarzania danych osobowych w Zamku Cieszyn;
    6. **Inspektor ochrony danych** – pracownik lub osoba wykonująca zadania na podstawie umowy, wymienione w art. 39 rozporządzenia 2016/679.
    7. **Wyznaczony pracownik** – Pracownik zatrudniony na stanowisku ds. kadrowych i kancelaryjnych Zamku Cieszyn wyznaczony do realizacji niektórych zadań z zakresu

ochrony danych osobowych;
8. **PBI** – Polityka bezpieczeństwa informacji Zamku Cieszyn;
9. **POD** – Polityka ochrony danych;
10. **IZSI** – Instrukcja Zarządzania Systemem Informatycznym Zamku Cieszyn.

§ 2
Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe

1. Dane osobowe w Zamku Cieszyn przetwarzane są w następującym budynku:

   Zamek Cieszyn, ul. Zamkowa 3 a,b,c, 43-400 Cieszyn

2. Szczegółowy wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe stanowi załącznik nr 1 do PBI.

§ 3
Rejestr czynności przetwarzania i rejestr kategorii czynności przetwarzania

1. Wyznaczony pracownik prowadzi rejestr czynności przetwarzania i rejestr kategorii czynności przetwarzania zgodnie z zakresem określonym w rozporządzeniu 2016/679.
2. Zakresy danych umieszczanych w prowadzonych rejestrach mogą wykraczać poza zakresy określone w rozporządzeniu 2016/679.
3. W przypadku realizacji nowej czynności przetwarzania pracownik sprawujący nadzór nad czynnością przetwarzania zobowiązany jest do przekazania wyznaczonemu pracownikowi wszystkie niezbędne informacje dotyczące nowej czynności przed rozpoczęciem przetwarzania danych.
4. Pracownik sprawujący bezpośredni nadzór nad czynnością przetwarzania wpisaną do rejestru zobowiązany jest niezwłocznie powiadomić o zaistnieniu zdarzenia, skutkującego nieaktualnością wpisu w rejestrze czynności przetwarzania danych.
5. Rejestr kategorii czynności przetwarzania prowadzonych przez Zamek Cieszyn wypełnia się na podstawie danych otrzymanych od podmiotu powierzającego przetwarzanie (jeżeli dotyczy).

§ 4
Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

1. Ochronę fizyczną Zamku Cieszyn stanowią:
   1) system alarmowy;
   2) system monitoringu wizyjnego w wybranych pomieszczeniach;
   3) zamki, kłódki, kraty itp.;
   4) szafy drewniane, metalowe i szuflady zamykane na klucz.
2. Obowiązki pracownika rozpoczynającego i kończącego pracę:
   1) Rozpoczynając pracę pracownik powinien pobrać klucze zgodnie z zasadami określonymi w Instrukcji postępowania z kluczami oraz zabezpieczenia pomieszczeń Zamku Cieszyn.
   2) Pomieszczenia służbowe winny być zamknięte każdorazowo pod nieobecność osób w nich pracujących.
   3) Pracownik powinien zachowywać zasadę "czystego biurka" i "czystego monitora".
   4) Pracownik opuszczający na dłużej stanowisko pracy powinien wylogować się

z aplikacji lub zablokować dostęp do systemu.
5) Po zakończeniu pracy pracownik powinien wyłączyć zgodnie z przepisami wszystkie urządzenia, które nie wymagają stałego zasilania.
6) Stanowisko pracy powinno być uporządkowane, a w szczególności zamknięte powinny być pieczątki, druki ścisłego zarachowania, podpisy elektroniczne, zewnętrzne nośniki informacji, wydruki komputerowe zawierające dane osobowe lub inne informacje chronione itp.
7) Po zamknięciu pomieszczenia klucze powinny zostać zdane.
8) Zabronione jest pozostawianie kluczy w drzwiach, na parapetach itp.

3. Bezpieczne użytkowanie komputerów przenośnych:
1) Komputery przenośne powinny być zabezpieczone podczas transportu, użytkowania oraz przechowywania w ogólnie przyjęty sposób np. torba na laptop, zabezpieczenie przed kradzieżą, niepozostawianie bez nadzoru w samochodzie itp.
2) Przetwarzanie danych osobowych może odbywać się tylko w uzasadnionych przypadkach, przy zachowaniu zabezpieczeń przyjętych dla komputerów przenośnych - szyfrowanie, na których przetwarzane są dane osobowe oraz w sposób uniemożliwiający dostęp do danych osobom postronnym.
3) Wynoszenie komputerów przenośnych poza siedzibę Zamku Cieszyn dopuszczalne jest tylko w uzasadnionych przypadkach, za zgodą Dyrektora Zamku.
4) Za bezpieczeństwo komputera przenośnego oraz danych na nim przetwarzanych odpowiedzialny jest bezpośrednio pracownik, któremu powierzono ww. mienie.

4. Środki organizacyjne związane z ochroną danych osobowych
1) AD powołał Inspektora ochrony danych.
2) W celu właściwej ochrony danych osobowych Zamek Cieszyn ma wyznaczonego pracownika zatrudnionego na stanowisku ds. kadrowych i kancelaryjnych, który bezpośrednio sprawuje pieczę nad aktualnością dokumentacji z zakresu ochrony danych osobowych, w szczególności rejestru czynności i rejestru kategorii czynności oraz upoważnień do przetwarzania danych.

5. Nadzór nad sprawnym, bezpiecznym i ciągłym funkcjonowanie systemu informatycznego Zamku Cieszyn realizowany jest przez pracownika zatrudnionego na stanowisku informatyka.

6. Na stanowiskach komputerowych, gdzie przetwarza się dane osobowe, zobowiązują zabezpieczenia w postaci loginów i haseł do systemu operacyjnego oraz do programów dziedzinowych przetwarzających dane osobowe.

7. Upoważnienia do przetwarzania danych.
1) Każda z osób przetwarzających dane osobowe posiada imienne upoważnienie do przetwarzania danych osobowych i jest bezpośrednio odpowiedzialna za bezpieczeństwo przetwarzanych przez siebie danych. Wzór upoważnienia stanowi załącznik nr 2 do PBI.
2) Osoba upoważniona zobowiązana jest do podpisania oświadczenia, które stanowi załącznik nr 3 do PBI.
3) AD określa do jakich zasobów powinna być osoba upoważniona.
4) Wyznaczony pracownik przygotowuje upoważnienie do podpisu AD.
5) W przypadku pracowników Zamku Cieszyn, wydane upoważnienia włącza się do akt osobowych pracownika.
6) Ewidencję osób upoważnionych do przetwarzania danych prowadzi wyznaczony pracownik, która stanowi załącznik 4 do PBI.
7) Wygaśnięcie ważności upoważnienia lub odwołanie upoważnienia skutkuje natychmiastowym zaprzestaniem przetwarzania danych (np. zablokowaniem dostępu do systemu) i odnotowaniem tego faktu w ewidencji osób upoważnionych do

przetwarzania danych osobowych.

8) Każda z osób upoważnionych do przetwarzania danych przed przystąpieniem do pracy przechodzi podstawowe szkolenie prowadzone przez Inspektora ochrony danych lub wyznaczonego pracownika z zakresu rozporządzenia 2016/679, UODO, POD, PBI i IZSI oraz ogólnych zasad bezpieczeństwa informacji, co potwierdzane jest na liście obecności stanowiącej załącznik 5 do PBI.
9) Osoby, które zostały upoważnione do przetwarzania danych, są zobowiązane zachować w tajemnicy te dane oraz sposoby ich zabezpieczenia.
10) Wszyscy pracownicy Zamku Cieszyn, stażyści, praktykanci, wolontariusze oraz kontrahenci realizujący zadania w budynku Zamku Cieszyn zobowiązani są do zwracania uwagi na sytuacje, które mogą zagrozić bezpieczeństwu danych osobowych.

§ 5
Powierzenie przetwarzania danych osobowych

1. Powierzenie przetwarzania danych osobowych może odbywać się tylko w uzasadnionych przypadkach oraz zgodnie z art. 28 rozporządzenia 2016/679.
2. W przypadku powierzenia przetwarzania danych zapisy dotyczące bezpieczeństwa danych mogą stanowić część umowy zasadniczej dotyczącej określonego przedmiotu umowy lub stanowić odrębną umowę.
3. Umowy powierzenia są ewidencjonowane przez wyznaczonego pracownika.
4. Umowy powierzenia mogą być ewidencjonowane w ramach prowadzonej ewidencji wszystkich umów Zamku Cieszyn.

§ 6
Umowy serwisowe

Umowy serwisowe na sprzęt komputerowy, oprogramowanie i inne urządzenia służące do przetwarzania danych powinny zawierać formalne zapisy z zakresu bezpieczeństwa informacji tzw. klauzulę o zachowaniu poufności.

§ 7
Incydenty związane z naruszeniem poufności, integralności i dostępności danych osobowych

1. Naruszenie systemu ochrony danych osobowych (incydent) może być stwierdzone na podstawie: stanu urządzeń zabezpieczających, zawartości zbiorów danych osobowych, sposobu działania oprogramowania i sieci informatycznej itp.
2. O każdym incydencie należy powiadomić Dyrektora Zamku Cieszyn lub Kierownika Działu Administracyjno-Gospodarczego oraz Inspektora ochrony danych.
3. Naruszenie systemu ochrony danych osobowych należy ewidencjonować w rejestrze zgłoszeń incydentów, który stanowi załącznik nr 6 do PBI.
4. W przypadku stwierdzenia naruszenia ochrony danych osobowych należy: zabezpieczyć pomieszczenie, zablokować dostęp do systemu informatycznego dla użytkowników oraz osób nieupoważnionych.
5. Inspektor ochrony danych podejmuje działania wyjaśniające mające na celu ustalenie przyczyn i okoliczności naruszenia bezpieczeństwa danych osobowych, osób winnych naruszenia bezpieczeństwa danych oraz skutków naruszenia.
6. Naruszenie ochrony danych osobowych zgłasza się organowi nadzorczemu, zgodnie z zakresem o którym mowa w art. 33 rozporządzenia 2016/679, chyba że jest mało

prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw i wolności osób fizycznych

7. Za nieprzestrzeganie zapisów Polityki bezpieczeństwa informacji i Instrukcji zarządzania systemem informatycznym wobec pracownika mogą zostać wyciągnięte konsekwencje zgodnie z Kodeksem pracy. Wobec osób trzecich i firm na zasadzie odrębnych przepisów.

§ 7
Audyty

1. Inspektor ochrony danych zobowiązany jest przynajmniej raz na rok przeprowadzić audyt planowy.
2. W przypadku wystąpienia incydentu bezpieczeństwa przeprowadza się audyt doraźny.
3. Szczegółowe zasady przeprowadzania audytu określa procedura stanowiąca załącznik nr 7 do PBI.

§ 8
Przegląd dokumentacji

1. Inspektor ochrony danych dokonuje przynajmniej raz w roku przeglądu PBI oraz IZSI.
2. Przegląd PB oraz IZSI odbywa się również w przypadku poważnego naruszenia bezpieczeństwa informacji, zmian regulacji prawnych.
3. Przeprowadzenie przeglądu odnotowuje się w załączniku nr 8 do PBI.

ZAMEK CIESZYN
dyrektor
Ewa Gołębiowska

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

Załącznik nr 7
do Polityki bezpieczeństwa informacji
w Zamku Cieszyn

Procedura audytu
realizowanego przez Inspektora ochrony danych

§ 1

1. Audyty, o których mowa w art. 39 ust. 1 lit. b rozporządzenia 2016/679 przeprowadzane przez Inspektora ochrony danych dokonywane są dla Dyrektora Zamku Cieszyn.
2. Audyty, o których mowa w ust. 1 są przeprowadzane w trybie:
   1) audytu planowego - według planu audytu, o którym mowa w ust. 3;
   2) audytu doraźnego - w przypadku nieprzewidzianym w planie audytu, w sytuacji powzięcia przez Inspektora ochrony danych wiadomości o incydencie - naruszeniu ochrony danych osobowych lub uzasadnionego podejrzenia wystąpienia takiego naruszenia;
3. Plan audytu określa przedmiot, zakres oraz termin przeprowadzenia audytów planowych oraz sposób i zakres ich dokumentowania.
4. Inspektor ochrony danych w planie audytu uwzględnia, w szczególności czynności przetwarzania i systemy informatyczne służące do przetwarzania danych osobowych oraz konieczność weryfikacji zgodności przetwarzania danych osobowych:
   1) z zasadami, o których mowa w art. 12-22 rozporządzenia 2016/679;
   2) z zasadami dotyczącymi bezpieczeństwa przetwarzania danych osobowych, o których mowa w art. 32 rozporządzenia 2016/679, innych przepisów regulujących przetwarzanie danych osobowych oraz Polityką bezpieczeństwa informacji Zamku Cieszyn i innymi regulacjami wewnętrznymi.
5. Plan audytu jest przygotowywany przez Inspektora ochrony danych na okres nie krótszy niż kwartał i nie dłuższy niż rok.
6. Plan audytu jest przedstawiany Dyrektorowi Zamku Cieszyn nie później niż na dwa tygodnie przed dniem rozpoczęcia okresu objętego planem.
7. Plan audytu obejmuje co najmniej jeden audyt.
8. Czynności przetwarzania oraz systemy informatyczne służące do przetwarzania lub zabezpieczania danych osobowych powinny być objęte audytem co najmniej raz na pięć lat.
9. Audyt doraźny jest przeprowadzany niezwłocznie po powzięciu wiadomości przez Inspektora ochrony danych o naruszeniu ochrony danych osobowych lub uzasadnionym podejrzeniu takiego naruszenia.
10. Inspektor ochrony danych zawiadamia Dyrektora Zamku Cieszyn o rozpoczęciu audytu doraźnego, przed podjęciem pierwszej czynności w toku audytu.

§ 2

1. Inspektor ochrony danych dokumentuje czynności przeprowadzone w toku audytu, w zakresie niezbędnym do oceny zgodności przetwarzania danych osobowych z rozporządzeniem 2016/679 oraz innymi przepisami regulującymi przetwarzanie danych osobowych.
2. Dokumentowanie czynności w toku audytu może polegać, w szczególności na utrwaleniu danych z systemu informatycznego służącego do przetwarzania lub zabezpieczania danych, urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych osobowych, odebraniu wyjaśnień od osoby, której czynności objęto audytem itp.
3. W systemie informatycznym służącym do przetwarzania danych osobowych czynności Inspektora ochrony danych mogą być wykonywane przy udziale osób upoważnionych do przetwarzania danych, w szczególności osoby zarządzającej tym systemem.

§ 3

Q

1. Pracownik odpowiedzialny za przetwarzanie danych osobowych, bierze udział w audycie lub umożliwia Inspektorowi ochrony danych przeprowadzenie czynności w toku audytu.
2. Inspektor ochrony danych informuje pracownika o zakresie planowanych czynności audytowych.

§ 4

1. Po zakończeniu audytu Inspektor ochrony danych osobowych przygotowuje raport z audytu.
2. Raport z audytu jest sporządzany w postaci elektronicznej albo w postaci papierowej.
3. Inspektor ochrony danych przekazuje Dyrektorowi Zamku Cieszyn raport z audytu:
   1) z audytu planowego- nie później niż w terminie 30 dni od zakończenia audytu;
   2) z audytu doraźnego - niezwłocznie po zakończeniu audytu.
4. Przykładowy wzór raportu z audytu stanowi załącznik do procedury.

ZAMEK CIESZYN
dyrektor
Ewa Gołębiowska

&

Załącznik do Procedury audytu
realizowanego przez Inspektora ochrony danych

WZÓR

Raport z audytu

1. **Temat audytu:**

2. **Rodzaj audytu: planowy/doraźny[1]**

3. **Inspektor ochrony danych:**

4. **Okres przeprowadzenia audytu:**

5. **Szczegółowy zakres przeprowadzonego audytu oraz osoby biorące udział w audycie:**

6. **Opis stanu faktycznego w tym naruszeń przepisów prawa:**

7. **Działania naprawcze oraz rekomendacje podnoszące standard ochrony danych osobowych:**

8. **Uwagi:**

.....
Inspektor ochrony danych

[1]Niepotrzebne skreślić

Załącznik nr 8
do Polityki Bezpieczeństwa Informacji
Zamku Cieszyn

Przegląd dokumentacji Polityki bezpieczeństwa informacji oraz Instrukcji zarządzania systemem informatycznym

L.p.	Przyczyna przeglądu (np. okresowy przegląd/zmiana przepisów prawa/incydent)	Data przeglądu	Uwagi (np. bez uwag, konieczność aktualizacji dokumentacji – należy wskazać zakres koniecznych zmian)	Imię i nazwisko osoby przeglądającej	Podpis
1					
2					
3					
4					
5					
6					
7					
8					
9					

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

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM ZAMKU CIESZYN

§ 1
Wstęp

1. Instrukcja Zarządzania Systemem Informatycznym (IZSI) jest dokumentem, który szczegółowo określa zasady pracy w systemie informatycznym Zamku Cieszyn.
2. Przez system informatyczny Zamku Cieszyn należy rozumieć samodzielne stanowiska komputerowe z dostępem do sieci Internet, stanowiska komputerowe bez dostępu do sieci Internet oraz komputery przenośne i inne urządzenia mobilne.
3. Zamek Cieszyn dysponuje centralnie zarządzanym systemem informatycznym.
4. Nadzór nad sprawnym, bezpiecznym i ciągłym funkcjonowaniem systemu informatycznego Zamku Cieszyn realizowany jest przez pracownika zatrudnionego na stanowisku Informatyka.
5. Z IZSI zobowiązani są zapoznać się wszyscy użytkownicy systemu informatycznego Zamku Cieszyn.

§ 2
Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności

1. Administrator (AD) lub wyznaczony przez AD Kierownik Działu Administracyjno-Gospodarczego określa do jakich zasobów powinna osoba być upoważniona w systemie informatyczny.
2. Osobą uprawnioną do nadawania uprawnień w systemie informatycznym jest Informatyk.
3. Na podstawie wydanego upoważnienia Informatyk nadaje uprawnienia.
4. Upoważnienie przekazuje się użytkownikowi systemu informatycznego.
5. Przekazanie loginu i hasła może nastąpić dopiero po otrzymaniu przez użytkownika systemu informatycznego przetwarzającego dane osobowe upoważnienia do przetwarzania danych osobowych.
6. Wygaśnięcie ważności upoważnienia lub odwołanie upoważnienia skutkuje natychmiastowym zaprzestaniem przetwarzania danych, zablokowaniem konta w systemie i odnotowaniem tego faktu przez wyznaczonego pracownika w ewidencji osób upoważnionych do przetwarzania danych osobowych.

§ 3
Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem

1. Do logowania się w systemie używa się identyfikatora (loginu) i hasła.
2. Uwierzytelnienie w systemie następuje po podaniu własnego identyfikatora i hasła.
3. Unikalny identyfikator, przypisany tylko danemu użytkownikowi, nadawany jest przez Informatyka.
4. Po założeniu identyfikatora, ustawiane jest hasło, które w bezpieczny sposób jest przekazywane użytkownikowi przez Informatyka.
5. Użytkownik, jeśli jest taka możliwość techniczna, zobowiązany jest zmienić hasło przy pierwszym dostępie do systemu.
6. Hasło jest własnością użytkownika, które nie może przekazać innym użytkownikom.
7. Hasło musi się składać z co najmniej 8 znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne.
8. Zmiana hasła następuje nie rzadziej niż co 30 dni.
9. Hasło musi być przechowywane w bezpieczny sposób.

§ 4
Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników

1. Monitory stanowisk komputerowych, gdzie przetwarzane są dane osobowe należy ustawić tak, aby uniemożliwić wgląd do nich osobą postronnym.
2. Przed rozpoczęciem pracy użytkownik zwraca uwagę, czy nie zaszły okoliczności wskazujące na naruszenie ochrony danych osobowych.
3. Włącza komputer i inne urządzenia peryferyjne.
4. Uwierzytelnia się w systemie sieci informatycznej za pomocą indywidualnego identyfikatora i hasła.
5. Uwierzytelnia się w systemie aplikacyjnym.
6. Pracownik opuszczający na dłużej stanowisko pracy powinien wylogować się z aplikacji i systemu lub zablokować dostęp do systemu np. nacisnąć kombinację klawiszy Windows +L
7. Użytkownik kończy pracę w systemie zgodnie z wymogami danej aplikacji i systemu np. wybór funkcji "koniec", "wyloguj", "zamknij".
8. Ekrany monitorów winny być automatycznie wyłączane po upływie 10 min. nieaktywności użytkownika
9. Po zakończeniu pracy pracownik powinien wyłączyć zgodnie z przepisami wszystkie urządzenia, które nie wymagają ciągłego zasilania.

§ 5
Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania

1. Za tworzenie i przechowywanie kopii zapasowych odpowiedzialny jest:
   a) Informatyk;
   b) Za tworzenie kopii bezpieczeństwa na stanowiskach komputerowych (komputery przenośne), nie podłączonych do systemu informatycznego pracownik użytkujący dany komputer zgodnie z ustaleniami z informatykiem.
2. Częstotliwość wykonywania kopii bezpieczeństwa uzależniona jest od ilości zmian wprowadzonych do systemu i uzgodniona jest z Dyrektorem Zamku Cieszyn.
3. Kopie bezpieczeństwa danych przetwarzanych w systemie informatycznym tworzy się co tydzień.
4. Okres przechowywania kopii 6 miesięcy.
5. Kopie bezpieczeństwa tworzy się na zewnętrznych nośnikach np. zewnętrzny dysk twardy, pendrive, CD, DVD.
6. Kopie bezpieczeństwa przechowuje się w szafie, w sekretariacie.

§ 6
Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe

1. Na zewnętrznych nośnikach informacji zapis danych osobowych w tym zbiorów danych osobowych może nastąpić tylko w uzasadnionych przypadkach.
2. Elektroniczne zewnętrzne nośniki informacji przechowuje się w miejscach bezpiecznych

– przechowywania danych osobowych.

3. Wynoszenie poza Zamek Cieszyn zewnętrznych nośników informacji zawierających dane osobowe może nastąpić tylko, kiedy jest to podyktowane przepisem prawa lub wyraził na to zgodę AD, a dane zostały zabezpieczone poprzez np. szyfrowanie.
4. Dane przechowywane na zewnętrznych nośnikach informacji przechowywane są tylko w czasie niezbędnym do spełnienia celu, w jakim zostały zapisane.
5. Sposób usuwania danych osobowych z elektronicznych nośników informacji powinien być bezpieczny, uniemożliwiający odtworzenie.

§ 7
Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego i utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej

1. System informatyczny zabezpieczony jest poprzez zainstalowane oprogramowanie antywirusowe, firewall.
2. Zabronione jest instalowanie oprogramowania, które nie zostało dopuszczone do użytku w Zamku Cieszyn.
3. Oprogramowanie jest na bieżąco aktualizowane.
4. Każdy zewnętrzny nośnik, z którego informacja będzie wprowadzana do komputera musi uprzednio zostać sprawdzony programem antywirusowym.
5. Na wybranych stacjach komputerowych (stanowiska pracy z systemem kadrowo-płacowym) zainstalowane jest urządzenie podtrzymujące napięcie UPS.

§ 8
Szyfrowanie danych

1. W celu redukcji ryzyk naruszenia praw i wolności osób fizycznych, których dane dotyczą Dyrektor Zamku Cieszyn zobowiązuje do szyfrowania danych chronionych przetwarzanych lub przesyłanych poza siedzibę Zamku Cieszyn.
2. Szyfrowanie danych w Zamku Cieszyn stosuje się w szczególności w następujących przypadkach:
   a) szyfrowanie zewnętrznych nośników informacji, dysków twardych lub danej partycji urządzeń mobilnych przetwarzających informacje chronione poza siedzibą Zamku Cieszyn;
   b) szyfrowanie informacji chronionych przesyłanych do podmiotów zewnętrznych.
3. O ile przepisy prawa nie stanowią inaczej, przesyłanie informacji chronionych pomiędzy podmiotami publicznymi następuje za pośrednictwem ePuap.
4. Szyfrowanie informacji odbywa się z wykorzystaniem dedykowanego oprogramowania lub funkcjonalności systemu.
5. Podczas szyfrowania wymagane jest podanie hasła.
6. Użytkownik szyfrujący dane jest zobowiązany do zastosowania hasła zgodnie z wymaganiami zawartymi w IZSI.

§ 9
Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych

1. Przegląd i konserwacja sprzętu informatycznego w Zamku Cieszyn realizowany jest przez Informatyka lub w uzasadnionych przypadkach zewnętrznego usługodawcę.

2. Bezpośredni nadzór nad przeglądami i konserwacją przez zewnętrznego usługodawcę sprawuje Kierownik Działu Administracyjno-Gospodarczego lub Informatyk.
3. Naprawa urządzeń, dysków lub innych nośników informacji zawierających dane osobowe poza siedzibą Zamku Cieszyn dopuszczalna jest kiedy nośnik pozbawi się informacji chronionych, jeżeli takiej możliwości nie ma umowa na realizację usługi bazuje na odpowiednich zapisach poufności i powierzenia.
4. Urządzenia, dyski lub inne nośniki informacji zawierające dane osobowe, a przeznaczone do likwidacji, należy zniszczyć w sposób uniemożliwiający odtworzenie.

ZAMEK CIESZYN
dyrektor
Ewa Gołąbiowska

Załącznik nr 1 do Polityki Bezpieczeństwa Informacji Zamku Cieszyn			
Budynek: Zamek Cieszyn, ul. Zamkowa 3 a,b, c 43-400 Cieszyn			
L.p.	**Nr pomieszczenia**	**Opis**	**Uwagi**
1	Budynek A parter	Informatyk	
2	Budynek A parter	Stanowisko ds. komunikacji	
3	Budynek A parter	Dział Wzornictwa	
4	Budynek A parter	Dział Przedsiębiorczości	
5	Budynek A parter	Gabinet Zastępcy Dyrektora	
6	Budynek B II piętro	Składnica akt	
7	Budynek C parter	Kierownik Działu Turystyki	
8	Budynek C I piętro	Gabinet Dyrektora	
9	Budynek C I piętro	Kierownik Działu Administracyjno-Gospodarczego	
10	Budynek C I piętro	Sekretariat/Kadry	
11	Budynek C I piętro	Dział Finansowo-Księgowy	

Załącznik nr 2
do Polityki Bezpieczeństwa Informacji Zamku Cieszyn

Cieszyn,.....

UPOWAŻNIENIE

Na podstawie art. 29 i 32 ust. 4 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenia o ochronie danych) (Dz. Urz. UE L 119 z 4.05.2016, str. 1) upoważniam Panią/Pana:

Imię i nazwisko – Stanowisko – Dział

do przetwarzania danych, w zakresie wykonywanych obowiązków służbowych, tradycyjnie (papierowo) oraz z użyciem systemu informatycznego Zamku Cieszyn, w tym
w następującym zakresie:

Niniejsze upoważnienie jest ważne do dnia...../odwołania lub zakończenia stosunku pracy/stażu/praktyki i nie może być przenoszone na inne osoby.

Osoba upoważniona do przetwarzania danych osobowych objętych zakresem, o którym mowa wyżej, jest zobowiązana do zachowania ich w tajemnicy, również po ustaniu zatrudnienia/zakończeniu stażu/praktyki oraz zachowania w tajemnicy informacji o ich zabezpieczeniu. Jednocześnie oświadcza, że zapoznała się z przepisami o ochronie danych osobowych.

.....
(podpis osoby upoważniającej)

Otrzymują:
1. Adresat
2. Informatyk
3. Kadry

Załącznik nr 3
do Polityki Bezpieczeństwa Informacji
Zamku Cieszyn

Nr.....

OŚWIADCZENIE OSOBY UPOWAŻNIONEJ

Zobowiązuję się do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, do których mam lub będę miał (a) dostęp w związku z wykonywaniem obowiązków służbowych na rzecz Zamku Cieszyn

Zobowiązuję się przestrzegać regulaminów, instrukcji i procedur obowiązujących w Zamku Cieszyn dotyczących bezpieczeństwa informacji w tym ochrony danych osobowych.

Oświadczam, że zostałem(am) zapoznany(a) z, Rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1), Ustawą o ochronie danych osobowych, Polityką ochrony danych oraz Polityką bezpieczeństwa informacji Zamku Cieszyn w zakresie koniecznym do realizacji obowiązków służbowych.

Cieszyn,.....

.....
(podpis osoby składającej oświadczenie)

Załącznik nr 4

do Polityki bezpieczeństwa informacji Zamku Cieszyn

Ewidencji osób upoważnionych do przetwarzania danych osobowych

Tabela							
Lp.	**Imię i nazwisko**	**Dział - Stanowisko**	**Nr upoważnienia**	**Data nadania upoważnienia**	**Data ustania upoważnienia**	**Zakres upoważnienia**	**Identyfikator w danym systemie informatycznym (login)[1]**
1							
2							
3							
4							

[1] Jeżeli dotyczy

5							
6							
7							
8							
9							
10							
11							
12							

13							
14							
15							
16							
17							
18							
19							

20							
21							
22							
23							
24							
25							
26							

Załącznik nr 5
do Polityki Bezpieczeństwa Informacji
Zamku Cieszyn

SZKOLENIE WEWNĘTRZNE Z ZAKRESU OCHRONY DANYCH OSOBOWYCH

L.p.	*Imię i nazwisko uczestnika*	*Stanowisko*	*Data szkolenia*	*Podpis*	*Podpis przeprowadzającego szkolenie*
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					
16					
17					

L.p.	*Imię i nazwisko uczestnika*	*Stanowisko*	*Data szkolenia*	*Podpis*	*Podpis przeprowadzającego szkolenie*
18					
19					
20					
21					
22					
23					
24					
25					
26					
27					
28					
29					
30					

P

Załącznik nr 6 do Polityki bezpieczeństwa informacji Zamku Cieszyn

Rejestr zgłoszeń incydentów

L.p.	Imię i nazwisko zgłaszającego	Data zgłoszenia	Godzina zgłoszenia	opis sytuacji	Informacja o zabezpieczonych dowodach naruszenia	Propozycja co do dalszego trybu postępowania	Uwagi
1							
2							
3							
4							
5							
6							