GMINNE CENTRUM KULTURY
84-312 w Cewicach, ul.Węgrzynowicza 16
tel./fax 3811 490
REGON 77052506 NIP 841-14-78-368

Zarządzenie Nr ...21...../2013
Dyrektora Gminnego Centrum Kultury w Cewicach
z dnia...6. sierpnia.....2013r.
w sprawie wprowadzenia w Gminnym Centrum Kultury w Cewicach procedur kontrolnych w zakresie ochrony i bezpieczeństwa zasobów informatycznych, w tym danych osobowych.

Na podstawie 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. z 2004 r. Nr 100, poz. 1024) oraz ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.)

Zarządzam, co następuje:

§1

Ustalam i wprowadzam do stosowania w Gminnym Centrum Kultury w Cewicach:

1. Politykę bezpieczeństwa przetwarzania danych osobowych w Gminnym Centrum Kultury w Cewicach, stanowiącą załącznik Nr 1 do niniejszego zarządzenia.
2. Instrukcję bezpieczeństwa przetwarzania danych osobowych w Gminnym Centrum Kultury w Cewicach, stanowiącą załącznik Nr 2 niniejszego zarządzenia.

§2

Zarządzenie wchodzi w życie z dniem...1 września.....2013r.

DYREKTOR
Gminnego Centrum Kultury
Dorota Bandurska

GMINNE CENTRUM KULTURY
84-312 w Cewicach, ul.Węgrzynowicza 16
tel./fax 8611 490
REGON 770925081 NIP 841-14-78-368

Załącznik Nr 1
do Zarządzenia Nr...21.../2013
Dyrektora Gminnego Centrum
Kultury w Cewicach
z dnia...6 sierpnia.....2013r.

Polityka bezpieczeństwa przetwarzania danych osobowych w Gminnym Centrum Kultury w Cewicach

Podstawa prawna:

1. *Rozporządzenie 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. z 2004 r. Nr 100, poz. 1024)*
1. *Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.)*

ROZDZIAŁ I

Postanowienia ogólne

§ 1

1. Polityka bezpieczeństwa przetwarzania danych osobowych w Gminnym Centrum Kultury w Cewicach zwana dalej „Polityką bezpieczeństwa", określa podstawowe zasady dotyczące zapewnienia bezpieczeństwa w zakresie danych osobowych przetwarzanych w zbiorach danych:

1) tradycyjnych, w szczególności kartotekach, księgach, skorowidzach, aktach osobowych, wykazach, w zbiorach ewidencyjnych;
2) w systemach informatycznych, w szczególności deklaracje ZUS, ewidencje płacowe, informacje skarbowe, ewidencje statystyczne, plany organizacyjne.

2. Ilekroć w polityce bezpieczeństwa jest mowa o:

1) **ustawie** – rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych z dnia 29 sierpnia 1997r. (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.);
2) **administrator bezpieczeństwa danych osobowych** – rozumie się Dyrektora Gminnego Centrum Kultury w Cewicach
3) **administrator systemu informatycznego** – rozumie się osobę odpowiedzialną za sprawność i funkcjonowanie systemu informatycznego, oraz stosowanie technicznych i organizacyjnych środków ochrony stosowanych w tym systemie
4) **nośniki danych osobowych** – dyskietki, płyty CD lub DVD, pamięć flash, dyski twarde, taśmy magnetyczne lub inne urządzenia/ materiały służące do przechowywania plików z danymi;

5) **osoba upoważniona (użytkownik)** – osoba posiadająca upoważnienie wydane przez administratora danych osobowych do przetwarzania danych osobowych;
6) **dane osobowe** - w rozumieniu ustawy za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
7) **przetwarzanie 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;
8) **zbiór danych** - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów;
9) **system informatyczny** - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
10) **identyfikator użytkownika (login)** - ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
11) **hasło** - ciąg znaków literowych, cyfrowych lub innych, przypisany do identyfikatora użytkownika, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;
12) **uwierzytelnianie** — rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;
13) **poufności danych** — rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom.

§ 2

1. Dyrektor Gminnego Centrum Kultury w Cewicach realizując politykę bezpieczeństwa dokłada szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności zapewnia, aby dane te były:
1) przetwarzane zgodnie z prawem;
2) zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane przetwarzaniu niezgodnemu z tymi celami;
3) merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane;
4) przechowywane w postaci uniemożliwiającej identyfikację osób, których dotyczą, przez osoby nieupoważnione.

2. Dyrektor Gminnego Centrum Kultury w Cewicach dąży do systematycznego unowocześniania stosowanych na terenie instytucji, technicznych i organizacyjnych środków ochrony tych danych w celu zabezpieczenia danych osobowych przed ich udostępnianiem osobom nieupoważnionym, przetwarzaniem z naruszeniem przepisów o ochronie danych osobowych, nieautoryzowaną zmianą, uszkodzeniem lub zniszczeniem.

ROZDZIAŁ II

Wykaz zbiorów danych osobowych w Gminnym Centrum Kultury w Cewicach

§ 3

1. Szczególnej ochronie poddane są:
   - sprzęt komputerowy użytkowany w dziale księgowości,
   - księgowy system informatyczny,
   - system informatyczny danych osobowych
   - kopie zapisów księgowych,
   - dowody księgowe,
   - dokumentacja inwentaryzacyjna,
   - sprawozdania budżetowe i finansowe
   - dokumentacja rachunkowa opisująca przyjęte przez jednostkę zasady rachunkowości

2. Dane osobowe gromadzone są w zbiorach:

1) Zbiór 1 – Kadry i płace pracowników Gminnego Centrum Kultury w Cewicach
2) Zbiór 2 – Dzienniki zajęć, listy obecności, listy uczestników zespołów i grup zajęciowych;
3) Zbiór 3 – Zgody na uczestnictwo w inicjatywach organizowanych przez instytucję.

2.1. Niniejszy zbiór ma charakter otwarty. Tabelaryczny wykaz zbiorów przedstawia załącznik nr 1 do niniejszej polityki.

§ 4

Zbiory danych osobowych wymienione w § 3 ust.1 podlegają przetwarzaniu w sposób tradycyjny oraz częściowo przy użyciu systemu informatycznego.

ROZDZIAŁ III

Wykaz budynków, pomieszczeń i stref do przetwarzania danych osobowych.

§ 5

1. Dane osobowe gromadzone i przetwarzane są w siedzibie Gminnego Centrum Kultury w Cewicach przy ul. Węgrzynowicza 16 oraz w jego filii tzw. Dom Kultury w Maszewie Lęborskim przy ul. Drewnianej 35 .

2. Obszarami do przetwarzania danych osobowych z użyciem sprzętu komputerowego oraz sposobem ręcznym są :
   1) pomieszczenie administracyjno- biurowe w Gminnym Centrum Kultury w Cewicach
   2) pomieszczenie biurowe w Domu Kultury w Maszewie

3. Budynek Gminnego Centrum Kultury w Cewicach jest zabezpieczony od zewnątrz i wewnątrz. Ochronę przed dostępem osób nieupoważnionych zapewniają sprawdzone zabezpieczenia pomieszczeń, w których przechowuje się zbiory księgowe. Są to alarm w pomieszczeniach biurowych połączony systemem alarmowania z firmą ochroniarską sprawującą nadzór nad mieniem Gminnego Centrum Kultury w Cewicach, atestowane zamki zamontowane w drzwiach, dodatkowym zabezpieczeniem dla przechowywania dokumentów są natomiast ognioodporna kasa pancerna oraz szafy wyposażone w zamki.

ROZDZIAŁ IV

Opis zdarzeń naruszających ochronę danych osobowych

§ 6.

1. Rodzaje zagrożeń naruszających ochronę danych osobowych:

1. 1. Zagrożenia losowe:
   1) zewnętrzne, np. klęski żywiołowe, przerwy w zasilaniu – ich wystąpienie może prowadzić do utraty integralności danych lub ich zniszczenia lub uszkodzenia infrastruktury technicznej systemu: ciągłość zostaje naruszona, jednak nie dochodzi do naruszenia danych osobowych;
   2) wewnętrzne np. niezamierzone pomyłki operatorów, awarie sprzętowe, błędy oprogramowania – w wyniku ich wystąpienia może dojść do zniszczenia danych, może nastąpić zakłócenie ciągłości pracy systemu i naruszenia poufności danych.

1. 2. Zagrożenia zamierzone (świadome i celowe naruszenia poufności danych) – w wyniku ich wystąpienia zazwyczaj nie występuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy. W ramach tej kategorii zagrożeń wystąpić mogą:

1) nieuprawniony dostęp do systemu z zewnątrz;
2) nieuprawniony dostęp do systemu z wewnątrz;
3) nieuprawnione przekazanie danych;
4) bezpośrednie zagrożenie materialnych składników np. kradzież, zniszczenie.

1. 3. Okoliczności zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są dane osobowe to w szczególności:

1) sytuacje losowe lub nieprzewidywalne oddziaływanie czynników zewnętrznych na zasoby systemu, np. wybuch gazu, pożar, zalanie pomieszczeń, uszkodzenia wskutek prowadzonych prac remontowych;
2) niewłaściwe parametry środowiska, np. nadmierna wilgotność, temperatura, wstrząsy, oddziaływania pola elektromagnetycznego, przeciążenia napięcia;
3) awarie sprzętu lub oprogramowania, które są celowym działaniem na potrzeby naruszenia ochrony danych osobowych;
4) pojawienie się odpowiedniego komunikatu alarmowego od części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu;
5) pogorszenie jakości danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub niepożądaną modyfikację w systemie;
6) naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie;
7) modyfikacja danych lub zmiana w strukturze danych bez odpowiedniego upoważnienia;
8) ujawnienie osobom nieuprawnionym danych osobowych lub objętych tajemnicą procedur ochrony ich przetwarzania;
9) podmienienie lub zniszczenie nośników z danymi osobowymi bez odpowiedniego upoważnienia lub skasowanie bądź skopiowanie w sposób niedozwolony danych osobowych;
10) rażące naruszenie obowiązków w zakresie przestrzegania procedur bezpieczeństwa informacji (niewylogowywanie się przed opuszczeniem stanowiska pracy, pozostawienie danych w drukarce lub kserokopiarce, niewykonanie kopii zapasowych, prace na danych osobowych w celach prywatnych itp.);
11) nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania danych osobowych, znajdujących się na dyskach, płytach CD, kartach pamięci oraz wydrukach komputerowych w formie niezabezpieczonej (otwarte szafy, biurka, regały, archiwum).

2. Przypadek stwierdzenia naruszenia ochrony danych osobowych bądź nieuzasadnionych zaniechań obowiązków wynikających z niniejszego dokumentu, w szczególności przez osobę, która wobec naruszenia ochrony danych osobowych lub uzasadnionego domniemania takiego naruszenia, nie podjęła działań określonych w niniejszym dokumencie, może być potraktowany jako ciężkie naruszenie obowiązków pracowniczych.

3. Wobec osoby uchylającej się od powiadomienia administratora bezpieczeństwa informacji o wystąpieniu naruszenia lub zagrożenia bezpieczeństwa systemu informatycznego stosuje się karę dyscyplinarną.

4. Zastosowanie kary dyscyplinarnej, o której mowa w pkt.3.3., nie wyklucza odpowiedzialności karnej ani cywilnej.

ROZDZIAŁ V

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

§ 7

Formy zabezpieczeń pomieszczeń, w których przetwarzane są dane osobowe:

1) wszystkie pomieszczenia, w których przetwarzane są dane osobowe zamykane są na klucz, w przypadku opuszczenia przez ostatnią osobę upoważnioną do przetwarzania danych osobowych – także w godzinach pracy;
2) dane osobowe przechowywane w wersji tradycyjnej (papierowej) lub elektronicznej (pamięć flash, płyty CD, DVD, dyskietki) po zakończeniu pracy są przechowywane w zamykanych na klucz meblach biurowych, a tam, gdzie jest to możliwe w szafach pancernych lub metalowych;
3) nieaktualne lub błędne wydruki zawierające dane osobowe niszczone są w niszczarkach;

§ 8

Formy zabezpieczeń przed nieautoryzowanym dostępem do danych osobowych:

1) podłączenie urządzenia końcowego (komputera, drukarki) do sieci komputerowej dokonywane jest przez administratora systemu informatycznego;
2) udostępnianie użytkownikowi zasobów sieci zawierających dane osobowe przez administratora następuje na podstawie upoważnienia do przetwarzania danych osobowych(załącznik Nr 2); niniejsze upoważnienie skutkuje dodatkowym, zakresem obowiązków pracownika (załącznik Nr 3). Wykaz osób upoważnionych stanowi załącznik Nr 4.
3) identyfikacja użytkownika w systemie następuje poprzez zastosowanie uwierzytelniania;
4) przydzielenie indywidualnego identyfikatora każdemu użytkownikowi;
5) udostępnianie kluczy do pomieszczeń, w których przetwarzane są dane osobowe tylko osobom upoważnionym;

§ 9

Formy zabezpieczeń przed utratą danych osobowych w wyniku awarii:

1) odrębne zasilanie sprzętu komputerowego lub zastosowanie listwy zabezpieczającej chroniącej podzespoły komputera przed uszkodzeniem spowodowanym zakłóceniami sieci zasilającej;
2) ochrona przed utratą danych poprzez cykliczne wykonywanie kopii zapasowych;
3) zapewnienie właściwej temperatury i wilgotności w pomieszczeniach;
4) zastosowanie ochrony przeciwpożarowej poprzez umieszczenie w pomieszczeniach lub w ich pobliżu gaśnic;
5) profilaktykę antywirusową – poprzez stosowanie programu zabezpieczającego, w tym skanowanie programem antywirusowym przychodzącej poczty elektronicznej,

§ 10

Organizację ochrony danych osobowych realizuje się poprzez:

1) zapoznanie każdej osoby z przepisami dotyczącymi ochrony danych osobowych przed dopuszczeniem do pracy;
2) przeszkolenie osób w zakresie bezpiecznej obsługi urządzeń i programów związanych z przetwarzaniem danych i programów;
3) kontrolowanie pomieszczeń budynku;
4) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych;
5) wyznaczenie administratora bezpieczeństwa informacji

GMINNE CENTRUM KULTURY
84-312 w Cewicach, ul.Węgrzynowicza 16
tel./fax 8611 490
REGON 770925061, NIP 841-14-78-368

Załącznik Nr 1
do „Polityki bezpieczeństwa
przetwarzania danych osobowych
w Gminnym Centrum Kultury
w Cewicach"

Wykaz zbiorów danych osobowych przetwarzanych w Gminnym Ośrodku Kultury w Cewicach ze wskazaniem programów zastosowanych do ich przetwarzania

Lp.	Nazwa zbioru danych	Zakres przetwarzanych danych	Program
1.	Zbiór 1	Kadry i płace pracowników Gminnego Centrum Kultury w Cewicach	system ręczny RADIX-płace RADIX - kadry
2.	Zbiór 2	Dzienniki zajęć listy obecności, listy uczestników zespołów, grup zajęciowych	system ręczny
3.	Zbiór 3	zgody na uczestnictwo w inicjatywach organizowanych przez instytucję	system ręczny

Załącznik Nr 2
do Polityki Bezpieczeństwa
przetwarzania danych osobowych
w Gminnym Centrum Kultury
w Cewicach

Data nadania upoważnienia: .....

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Upoważniam Panią/Pana .....
   o numerze PESEL .....
   zatrudnioną/-ego na stanowisku .....
   w .....

   do dostępu do następujących zbiorów danych osobowych w celu ich przetwarzania:
   (należy określić zbiory zgodnie z wykazem ujętym w rozdziale II Polityki Bezpieczeństwa)
   - .....
   - .....
   - .....

2. Identyfikator/Login: .....
3. Okres trwania upoważnienia: .....

Wystawił: .....

(podpis Administratora Danych Osobowych lub ABI zgodnie z § 12 Polityki Bezpieczeństwa)

4. Osoba upoważniona do przetwarzania danych, objętych zakresem, o którym mowa wyżej, jest zobowiązana do zachowania ich w tajemnicy, również po ustaniu zatrudnienia oraz zachowania w tajemnicy informacji o ich zabezpieczeniu.

Data i podpis osoby upoważnionej:

OŚWIADCZENIE

Zobowiązuję się do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, do których mam, lub będę miał/-a dostęp w związku z wykonywaniem jakichkolwiek czynności na rzecz ..... .

Zobowiązuję się przestrzegać wszelkich procedur obowiązujących w wyżej wymienionej jednostce organizacyjnej dotyczących ochrony danych osobowych – w szczególności określonych w Polityce Bezpieczeństwa oraz Instrukcji Zarządzania Systemem Informatycznym.

Oświadczam, że zapoznałem/-am się z przepisami dotyczącymi ochrony danych osobowych, w tym z ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2002 r. Nr 101, poz. 926 z poźn.zm.), w tym z zasadami odpowiedzialności karnej określonymi w rozdziale 8 wyżej wymienionej ustawy.

.....

(data i podpis osoby oświadczającej)

Załącznik Nr 3
do „Polityki bezpieczeństwa
przetwarzania danych osobowych
w Gminnym Centrum Kultury
w Cewicach'

DODATKOWY ZAKRES OBOWIĄZKÓW
DLA PRACOWNIKÓW GMINNEGO CENTRUM KULTURY W CEWICACH

1. Pracownik zobowiązany jest dbać o bezpieczeństwo powierzonych mu do przetwarzania, archiwizowania lub przechowywania danych zgodnie z obowiązującą w instytucji polityką bezpieczeństwa, regulaminami i instrukcjami wewnętrznymi, w tym m. in.:
   a) chronić dane przed dostępem osób nieupoważnionych,
   b) chronić dane przed przypadkowym lub nieumyślnym zniszczeniem, utratą lub modyfikacją,
   c) chronić nośniki magnetyczne i optyczne oraz wydruki komputerowe przed dostępem osób nieupoważnionych oraz przed przypadkowym zniszczeniem,
   d) utrzymywać w tajemnicy powierzone identyfikatory, hasła, częstotliwość ich zmiany oraz szczegóły technologiczne systemów także po ustaniu zatrudnienia w szkole.
   e) archiwizować dane zgodnie z przyjętymi zasadami

2. Zabrania się pod rygorem odpowiedzialności służbowej i karnej:
   a) ujawniać dane – w tym dane osobowe zawarte w obsługiwanych systemach,
   b) kopiować bazy danych lub ich części poza przewidzianymi instrukcją technologiczną kopiami bezpieczeństwa,
   c) zabrania się przetwarzania danych w sposób inny niż opisany instrukcją technologiczną

Załącznik Nr 4
do „Polityki bezpieczeństwa
przetwarzania danych osobowych
w Gminnym Centrum Kultury
w Cewicach"

Wykaz osób upoważnionych do przetwarzania danych osobowych w Gminnym Centrum Kultury

Lp.	Imię nazwisko	Nr upoważnienia	Nazwa zbioru
1.	Bożena Szeląg	1/2013	1,2,3
2.	Malwina Reszkowska	2/2013	1,2,3
3.	Weronika Olenej	3/2013	1,2,3
4.	Ewa Cybula	2/2015	1,2,3
5.	Weronika Puzdrowska	3/2015	1,2,3
6.	Ludwika Janczak	4/2015	1,2,3

GMINNE CENTRUM KULTURY
84-312 w Cewicach, ul.Węgrzynowicza 16
tel./fax 8611 490
REGON 770025061, NIP 841-14-78-368

Załącznik Nr 2
do Zarządzenia Nr.21/2013
Dyrektora Gminnego Centrum
Kultury w Cewicach
z dnia....6 sierpnia.....2013r.

Instrukcja bezpieczeństwa przetwarzania danych osobowych w Gminnym Centrum Kultury w Cewicach

§ 1

Nadawanie uprawnień do przetwarzania danych oraz ich rejestrowanie w systemie informatycznym.

1. Do obsługi systemu informatycznego służącego do przetwarzania danych osobowych, może być dopuszczona wyłącznie osoba posiadająca upoważnienie do przetwarzania danych osobowych, wydane przez administratora danych osobowych.
2. Upoważnienia do przetwarzania danych osobowych, o których mowa w punkcie 1 przechowywane są w teczkach akt osobowych pracowników oraz prowadzona jest ich ewidencja.
3. Dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po :
   a) podaniu identyfikatora użytkownika i właściwego hasła w przypadku obsługi programu BIP,
   b) podaniu właściwego hasła dostępu do stanowiska komputerowego w przypadku obsługi programów RADIX- Kadry, RADIX-Płace, PŁATNIK.
4. Dla każdego użytkownika systemu informatycznego, który przetwarza dane osobowe, Administrator bezpieczeństwa Informacji ustala identyfikator i hasło początkowe.
5. Identyfikator użytkownika nie powinien być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego, nie powinien być przydzielany innej osobie.
6. W przypadku utraty przez daną osobę uprawnień do dostępu do danych osobowych w systemie informatycznym identyfikator osoby, która utraciła uprawnienia do dostępu do danych osobowych, należy niezwłocznie wyrejestrować z systemu informatycznego, unieważnić jej hasło oraz podjąć inne stosowne działania w celu zapobieżenia dalszemu dostępowi tej osoby do danych. Za realizację procedury rejestrowania i wyrejestrowywanie użytkowników w systemie informatycznym odpowiedzialny jest administrator bezpieczeństwa Informacji.

§ 2

Metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem.

1. Dane osobowe przetwarzane są z użyciem dedykowanych serwerów, komputerów stacjonarnych.
2. Hasło użytkownika powinno mieć ilość znaków określoną programem .
3. Hasło oprócz znaków małych i dużych liter winno zawierać ciąg znaków alfanumerycznych i specjalnych.
4. Hasła wpisywane z klawiatury nie mogą pojawiać się na ekranie monitorów w formie jawnej;
5. Hasło nie może zawierać żadnych informacji, które można kojarzyć z użytkownikiem komputera, np. osobiste dane użytkownika, tj. nazwisko, inicjały, imiona, marka lub nr rejestracyjny samochodu itp.
6. Hasło nie może być zapisywane w miejscu dostępnym dla osób nieuprawnionych. Użytkownik nie może udostępnić swojego identyfikatora oraz hasła jak również dostępu do stanowiska roboczego po uwierzytelnieniu w systemie osobom nieuprawnionym ani żadnej osobie postronnej.
7. Hasło użytkownika, umożliwiające dostęp do systemu informatycznego należy utrzymywać w tajemnicy również po upływie jego ważności.
8. Raz użyty identyfikator nie może być przydzielony innemu użytkownikowi.
9. Hasła są zdeponowane w kasie pancernej w siedzibie dyrektora
10. W przypadku, gdy istnieje podejrzenie, że hasło mogła poznać osoba nieuprawniona, użytkownik zobowiązany jest do natychmiastowej zmiany hasła, lub w razie problemów powiadomić o tym fakcie administratora bezpieczeństwa Informacji.

§ 3

Procedury rozpoczęcia, zawieszenia i zakończenia pracy.

1. Dane osobowe, których administratorem jest Gminne Centrum Kultury w Cewicach mogą być przetwarzane sposobem tradycyjnym lub z użyciem systemu informatycznego tylko na potrzeby realizowania zadań statutowych i organizacyjnych placówki.
2. Rozpoczęcie pracy użytkownika w systemie informatycznym następuje po poprawnym uwierzytelnieniu (zalogowaniu się do systemu).
3. Rozpoczęcie pracy w aplikacji musi być przeprowadzone zgodnie z instrukcją zawartą w dokumentacji aplikacji.
4. Zakończenie pracy użytkownika następuje po poprawnym wylogowaniu się z systemu oraz poprzez uruchomienie odpowiedniej dla danego systemu opcji jego zamknięcia zgodnie z instrukcją zawartą w dokumentacji.
5. Niedopuszczalne jest zakończenie pracy w systemie bez wykonania pełnej i poprawnej operacji wylogowania z aplikacji i poprawnego zamknięcia systemu.
6. Monitory stanowisk komputerowych znajdujące się w pomieszczeniach, gdzie przebywają osoby, które nie posiadają upoważnień do przetwarzania danych osobowych, a na których przetwarzane są dane osobowe, należy ustawić w taki sposób, aby uniemożliwić osobom postronnym wgląd w dane.
7. Użytkownik ma obowiązek wylogowania się w przypadku zakończenia pracy. Stanowisko komputerowe nie może pozostać z uruchomionym i dostępnym systemem bez nadzoru pracującego na nim pracownika;
8. Wydruki zawierające dane osobowe należy przechowywać w miejscu uniemożliwiającym ich odczytanie przez osoby postronne. Wydruki nieprzydatne

należy zniszczyć w stopniu uniemożliwiającym ich odczytanie w niszczarce dokumentów.

9. Użytkownik niezwłocznie powiadamia administratora bezpieczeństwa Informacji w przypadku podejrzenia fizycznej ingerencji w przetwarzane dane osobowe lub użytkowane narzędzia programowe lub sprzętowe. Wówczas użytkownik jest zobowiązany do natychmiastowego wyłączenia sprzętu.

§ 4

Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi do ich przetwarzania.

1. Zbiory danych osobowych w systemie informatycznym są zabezpieczane przed utratą lub uszkodzeniem za pomocą:
   a) urządzeń zabezpieczających przed awarią zasilania lub zakłóceniami w sieci zasilającej, o ile jest to możliwe,
   b) sporządzanie kopii zapasowych (kopie pełne).
2. Pełne kopie zapasowe zbiorów danych tworzone są 2 razy w ciągu roku;
3. W szczególnych sytuacjach, np. przed aktualizacją lub zmianą oprogramowania lub systemu należy wykonać bezwzględnie pełną kopię zapasową systemu;
4. Kopie zapasowe zbiorów danych należy okresowo sprawdzać pod kątem ich przydatności do odtworzenia w przypadku awarii systemu.
5. Nośniki danych po ustaniu ich użyteczności należy pozbawić danych lub zniszczyć w sposób uniemożliwiający odczyt danych

§ 5

Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych

1. Okresowe kopie zapasowe wykonywane są na płytach CD lub innych elektronicznych nośnikach informacji. Kopie zapasowe przechowuje się w sposób uniemożliwiający nieuprawnione przejęcie, modyfikacje, uszkodzenie lub zniszczenie w kasie pancernej siedziby dyrektora.

2. Dostęp do nośników z kopiami zapasowymi systemu oraz kopiami danych osobowych ma wyłącznie administrator bezpieczeństwa informacji.

3. Kopie miesięczne przechowuje się przez okres 6 miesięcy. Wykonywane co pół roku pełne kopie systemu kadrowego przechowuje się przez 50 lat. Kopie zapasowe należy bezzwłocznie usuwać po ustaniu ich użyteczności.

4. Usunięcie danych z systemu powinno zostać zrealizowane przy pomocy oprogramowania przeznaczonego do bezpiecznego usuwania danych z nośnika informacji.

5. W przypadku kopii zapasowych sporządzanych indywidualnie przez użytkownika odpowiedzialnością za ich zniszczenie obarczony jest użytkownik.

6. W przypadku nośników informacji przez ich zniszczenie rozumie się ich trwałe i nieodwracalne zniszczenie fizyczne do stanu niedającego możliwości ich rekonstrukcji i odzyskania danych.

§ 6

Sposób zabezpieczenia systemu informatycznego przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego

1. W związku z istnieniem zagrożenia dla zbiorów danych osobowych, ze strony wirusów komputerowych, których celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego, konieczna jest ochrona sieci komputerowej i stanowisk komputerowych.

2. Wirusy komputerowe mogą pojawić się systemach placówki poprzez: internet, nośniki informacji takie jak: dyskietki, płyty CD, dyski przenośne, itp.

3. Przeciwdziałanie zagrożeniom ze strony wirusów komputerowych realizowane jest następująco:
   a) Komputer z dostępem do Internetu musi być zabezpieczony za pomocą oprogramowania antywirusowego.
   b) Zainstalowany program antywirusowy powinien być tak skonfigurowany, by regularnie dokonywał aktualizacji bazy wirusów oraz co najmniej raz w tygodniu dokonywane było automatycznie sprawdzenie komputera pod kątem obecności wirusów komputerowych.
   c) Elektroniczne nośniki informacji, takie jak dyskietki, dyski przenośne, należy każdorazowo sprawdzać programem antywirusowym przed użyciem po zainstalowaniu ich w systemie. Czynność powyższą realizuje użytkownik systemu. W przypadku problemów ze sprawdzeniem zewnętrznego nośnika danych użytkownik jest zobowiązany zwrócić się z tym do administratora bezpieczeństwa informacji.
   d) Komputery i systemy pracujące muszą mieć zainstalowany program antywirusowy a w przypadku komputerów z dostępem do Internetu również posiadać oprogramowanie i mechanizmy zabezpieczające przed nieautoryzowanym dostępem z sieci (firewall).
   e) W przypadku, gdy użytkownik stanowiska komputerowego zauważy komunikat oprogramowania zabezpieczającego system wskazujący na zaistnienie zagrożenia lub rozpozna tego typu zagrożenie, zobowiązany jest zaprzestać jakichkolwiek czynności w systemie i niezwłocznie skontaktować się z administratorem bezpieczeństwa informacji.
   f) Przy korzystaniu z poczty elektronicznej należy zwrócić szczególną uwagę na otrzymywane załączniki dołączane do treści wiadomości. Zabrania się otwierania załączników i wiadomości poczty elektronicznej od „niezaufanych" nadawców.
   g) Zabrania się użytkownikom komputerów wyłączania, blokowania odinstalowywania programów zabezpieczających komputer (skaner antywirusowy, firewall) przed oprogramowaniem złośliwym oraz nieautoryzowanym dostępem.

§ 7

Udostępnianie danych osobowych i sposób odnotowania informacji o udostępnionych danych

Udostępnienie danych instytucjom może odbywać się wyłącznie na pisemny uzasadniony wniosek lub zgodnie z przepisami prawa.

§ 8

Wykonywanie przeglądów systemu oraz nośników informacji służących do przetwarzania danych

1. Przeglądy systemu oraz zbiorów danych wykonuje administrator bezpieczeństwa informacji na bieżąco.
2. Administrator bezpieczeństwa informacji okresowo sprawdza możliwość odtworzenia danych z kopii zapasowej.
3. Umowy dotyczące instalacji i konserwacji sprzętu należy zawierać z podmiotami, których kompetencje nie budzą wątpliwości, co do wykonania usługi oraz których wiarygodność finansowa zostały sprawdzone na rynku.
4. Naprawy sprzętu należy zlecać podmiotom, których kompetencje nie budzą wątpliwości co do wykonania usługi. Naprawa sprzętu, na którym mogą znajdować się dane osobowe, powinna odbywać się pod nadzorem osób użytkujących sprzęt oraz administratora bezpieczeństwa informacji w miejscu jego użytkowania.
5. W przypadku konieczności naprawy poza miejscem użytkowania sprzęt komputerowy, przed oddaniem do serwisu, powinien być odpowiednio przygotowany. Dane należy zarchiwizować na nośniki informacji, a dyski twarde bezwzględnie wymontować na czas naprawy.
6. Zmiana konfiguracji sprzętu komputerowego, na którym znajdują się dane osobowe lub zmiana jego lokalizacji, może być dokonana tylko za wiedzą i zgodą administratora bezpieczeństwa informacji.

§ 9

Zalecenia w zakresie przetwarzania danych osobowych sposobem tradycyjnym

1. Miejscem tworzenia, uzupełniania, przechowywania dokumentacji dotyczącej przetwarzania danych osobowych sposobem tradycyjnym są pomieszczenia administracyjno biurowe Gminnego Centrum Kultury w Cewicach
2. Osoby prowadzące dokumentację zobowiązane są do zachowania tajemnicy służbowej.
3. Dokumentacji, o której mowa w punkcie 1 nie można wynosić poza teren szkoły.
4. Dokumentację, o której mowa w punkcie 1 archiwizuje się zgodnie z Instrukcją kancelaryjną.

5. Osoby prowadzące dokumentację zobowiązane są do niezwłocznego poinformowania administratora bezpieczeństwa informacji o podejrzeniu dostępu do dokumentacji przez osoby nieupoważnione

§ 10
Ustalenia końcowe

1. Osobom korzystającym z systemu informatycznego, w którym przetwarzane są dane osobowe zabrania się:

a) ujawniania loginu i hasła współpracownikom i osobom z zewnątrz,

b) pozostawiania haseł w miejscach widocznych dla innych osób,

c) udostępniania stanowisk pracy wraz z danymi osobowymi osobom nieuprawnionym,

d) udostępniania osobom nieuprawnionym programów komputerowych zainstalowanych w systemie,

e) używania oprogramowania w innym zakresie niż pozwala na to umowa licencyjna,

f) przenoszenia programów komputerowych, dysków twardych z jednego stanowiska na inne,

g) kopiowania danych na nośniki informacji, kopiowania na inne systemy celem wynoszenia ich poza placówkę,

h) samowolnego instalowania i używania jakichkolwiek programów komputerowych w tym również programów do użytku prywatnego; programy komputerowe instalowane są przez administratora bezpieczeństwa informacji,

i) używania nośników danych udostępnionych przez osoby postronne,

j) przesyłania dokumentów i danych z wykorzystaniem konta pocztowego prywatnego (niesłużbowego),

k) otwierania załączników i wiadomości poczty elektronicznej od nieznanych i „niezaufanych" nadawców,

l) używania nośników danych niesprawdzonych, niewiadomego pochodzenia lub niezwiązanych z wykonywaną pracą; w przypadku konieczności użycia niesprawdzonych przenośnych nośników danych, należy zgłosić te nośniki, w celu sprawdzenia - przeskanowania programem antywirusowym, administratorowi bezpieczeństwa informacji,

m) tworzenia kopii zapasowych niechronionych hasłem i/lub bez odpowiednich zabezpieczeń miejsca ich przechowywania.

2. Ponadto zabrania się:

a) wyrzucania dokumentów zawierających dane osobowe bez uprzedniego ich trwałego zniszczenia,

b) pozostawiania dokumentów, kopii dokumentów zawierających dane osobowe w drukarkach, kserokopiarkach,

c) pozostawiania kluczy w drzwiach, szafach, biurkach, zostawiania otwartych pomieszczeń, w których przetwarza się dane osobowe,

d) pozostawiania bez nadzoru osób trzecich przebywających w pomieszczeniach szkoły, w których przetwarzane są dane osobowe,

e) pozostawiania dokumentów na biurku po zakończonej pracy, pozostawiania otwartych dokumentów na ekranie monitora bez blokady konsoli,

f) ignorowania nieznanych osób z zewnątrz poruszających się w obszarze przetwarzania danych osobowych,

g) przekazywania informacji będącymi danymi osobowymi osobom nieupoważnionym,

h) ignorowania zapisów polityki bezpieczeństwa szkoły.

3. Konieczne jest:

a) posługiwanie się własnym loginem i hasłem w celu uzyskania dostępu do systemów informatycznych,
b) tworzenia haseł trudnych do odgadnięcia dla innych,
c) traktowanie konta pocztowego szkoły jako narzędzia pracy i wykorzystywanie go jedynie w celach służbowych,

ROZDZIAŁ II

Wykaz zbiorów danych osobowych w Gminnym Centrum Kultury w Cewicach

§ 3

1. Szczególnej ochronie poddane są:

- sprzęt komputerowy użytkowany w dziale księgowości,
- księgowy system informatyczny,
- system informatyczny danych osobowych
- kopie zapisów księgowych,
- dowody księgowe,
- dokumentacja inwentaryzacyjna,
- sprawozdania budżetowe i finansowe
- dokumentacja rachunkowa opisująca przyjęte przez jednostkę zasady rachunkowości

2. Dane osobowe gromadzone są w zbiorach:

1) Zbiór 1 – Ewidencja osób zatrudnionych przy przetwarzaniu danych osobowych;
2) Zbiór 2 – Kontrola wewnętrzna - wyniki, opracowania, protokóły, notatki,;
3) Zbiór 3 – Akta osobowe pracowników;
4) Zbiór 4 – Dokumentacja dotycząca polityki kadrowej – opiniowanie awansów, wyróżnień, nagród, wnioski itp;
5) Zbiór 5 – Notatki służbowe oraz postępowanie dyscyplinarne;
6) Zbiór 6 – Zbiory informacji o pracownikach;
7) Zbiór 7 – Ewidencja zwolnień lekarskich;
8) Zbiór 8 – Skierowania na badania okresowe, specjalistyczne;
9) Zbiór 9 – Ewidencja urlopów, karty czasu pracy;
10) Zbiór 10 – Kartoteki wydanej odzieży ochronnej i środków ochrony indywidualnej;
11) Zbiór 11 – Rejestr delegacji służbowych;
12) Zbiór 12 – Listy płac pracowników;
13) Zbiór 13 – Kartoteki zarobkowe pracowników, nakazy komornicze;
14) Zbiór 14 – Deklaracje ubezpieczeniowe pracowników;
15) Zbiór 15 – Deklaracje i kartoteki ZUS pracowników;
16) Zbiór 16 – Deklaracje podatkowe pracowników;
17) Zbiór 17– Dzienniki zajęć, listy obecności, listy uczestników zespołów i grup zajęciowych;
18) Zbiór 18- Zgody na uczestnictwo w inicjatywach organizowanych przez placówkę
19) Zbiór 19 – Zaświadczenia, inne orzeczenia i opinie;
20) Zbiór 20 – Rejestr zaświadczeń wydanych pracownikom
21) Zbiór 21 – Rejestr wypadków,
22) Zbiór 22 – Księga druków ścisłego zarachowania;
23) Zbiór 23 – Zbiór upoważnień;
24) Zbiór 24 – Umowy zawierane z osobami fizycznymi;
25) Zbiór 25 – Protokóły z posiedzeń Rady Programowej, rejestr uchwał;

2.1. Niniejszy zbiór ma charakter otwarty. Tabelaryczny wykaz zbiorów przedstawia załącznik nr 1 do niniejszej polityki

§ 4

Zbiory danych osobowych wymienione w § 3 ust.1 podlegają przetwarzaniu w sposób tradycyjny oprócz zbiorów Nr 7,11,14,15, które gromadzone są i przetwarzane przy użyciu systemu informatycznego.

ROZDZIAŁ III

Wykaz budynków, pomieszczeń i stref do przetwarzania danych osobowych.

§ 5

1. Dane osobowe gromadzone i przetwarzane są w siedzibie Gminnego Centrum Kultury w Cewicach przy ul. Węgrzynowicza 16 oraz w jego filii tzw. Dom Kultury w Maszewie Lęborskim przy ul. Drewnianej 35 .

2. Obszarami do przetwarzania danych osobowych z użyciem sprzętu komputerowego oraz sposobem ręcznym są :
   1) pomieszczenie administracyjno- biurowe w Gminnym Centrum Kultury w Cewicach
   2) pomieszczenie biurowe w Domu Kultury w Maszewie

3. Budynek Gminnego Centrum Kultury w Cewicach jest zabezpieczony od zewnątrz i wewnątrz. Ochronę przed dostępem osób nieupoważnionych zapewniają sprawdzone zabezpieczenia pomieszczeń, w których przechowuje się zbiory księgowe. Są to alarm w pomieszczeniach biurowych połączony systemem alarmowania z firmą ochroniarską sprawującą nadzór nad mieniem Gminnego Centrum Kultury w Cewicach, atestowane zamki zamontowane w drzwiach, dodatkowym zabezpieczeniem dla przechowywania dokumentów są natomiast ognioodporna kasa pancerna oraz szafy wyposażone w zamki.

ROZDZIAŁ IV

Opis zdarzeń naruszających ochronę danych osobowych

§ 6.

1. Rodzaje zagrożeń naruszających ochronę danych osobowych:

1. 1. Zagrożenia losowe:
   1) zewnętrzne, np. klęski żywiołowe, przerwy w zasilaniu – ich wystąpienie może prowadzić do utraty integralności danych lub ich zniszczenia lub uszkodzenia infrastruktury technicznej systemu: ciągłość zostaje naruszona, jednak nie dochodzi do naruszenia danych osobowych;
   2) wewnętrzne np. niezamierzone pomyłki operatorów, awarie sprzętowe, błędy oprogramowania – w wyniku ich wystąpienia może dojść do zniszczenia danych, może nastąpić zakłócenie ciągłości pracy systemu i naruszenia poufności danych.

GMINNE CENTRUM KULTURY
84-312 w Cewicach, ul. Węgrzynowicza 16
tel./fax 8611 490
REGON 770025061, NIP 841-14-78-368

MATERIAŁY POMOCNICZE DO ZARZĄDZENIA (podziony)

Wykaz zbiorów danych osobowych przetwarzanych w Gminnym Ośrodku Kultury w Cewicach ze wskazaniem programów zastosowanych do ich przetwarzania

	Lp.	Nazwa zbioru danych	Zakres przetwarzanych danych	Program
	1	Zbiór 1	Ewidencja osób zatrudnianych przy przetwarzaniu danych osobowych	system ręczny
	2	Zbiór 2	Kontrola wewn. wyniki, sprawozdania, protokoły, notatki	system ręczny
	3	Zbiór 3	Akta osobowe pracowników	RADIX - Kadry
	4	Zbiór 4	Dokumentacja podatkowa kadrowa - awanse, wynagrodzenia, nagrody	system ręczny
	5	Zbiór 5	Notatki służbowe oraz postępowania dyscyplinarne	system ręczny
	6	Zbiór 6	Zbiory informacji o pracownikach	system ręczny
	7	Zbiór 7	Ewidencja zwolnień lekarskich	system ręczny
Zbiór 1	8	Zbiór 8	Skierowania na badania lekarskie	system ręczny
	9	Zbiór 9	Ewidencja urlopów, karty czasu pracy	system ręczny
	10	Zbiór 10	Kartoteki odzieży roboczej i środków ochrony indywidualnej	system ręczny
	11	Zbiór 11	Rejestr delegacji służbowych	system ręczny
	12	Zbiór 12	Listy płac pracowników	RADIX - Płace
	13	Zbiór 13	Kartoteki zarobkowe, nakazy komornicze	system ręczny
	14	Zbiór 14	Deklaracje ubezpieczeniowe	RADIX - Kadry
	15	Zbiór 15	Deklaracje i kartoteki ZUS	RADIX - Kadry
	16	Zbiór 16	Deklaracje podatkowe	
Zbiór 2	17	Zbiór 17	Dzienniki zajęć, listy obecności, listy zespołów i grup zajęciowych	system ręczny
Zbiór 3	18	Zbiór 18	Zgody na udział w imprezach	system ręczny
Zbiór 1	19	Zbiór 19	Zaświadczenia, orzeczenia, opinie	system ręczny
	20	Zbiór 20	Rejestr zaświadczeń wydanych pracownikom	system ręczny

Zbiór 1

nie podlega zgłoszeniu do GIODO – poz. 25 przy Urzędzie Gminy

21	zbiór 21	Rejestr wypadków	system ręczny
22	zbiór 22	Księga dowodów ścisłego zarachowania	system ręczny
23	zbiór 23	zbiór upoważnień	system ręczny
24	zbiór 24	Umowy zawierane z osobami fizycznymi	system ręczny
25	zbiór 25	Protokoły z posiedzeń Rady Gminy, Prezydium, rejestr uchwał	system ręczny