ZARZĄDZENIE Nr 5.2015
DYREKTORA MIEJSKO - GMINNEGO ZESPOŁU OŚWIATY
z dnia 09.09.2015 r.

w sprawie: Polityki bezpieczeństwa w Miejsko – Gminnym Zespole Oświaty w Drezdenku

Na podstawie § 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, poz. 1024).

zarządza się co następuje:

§ 1

Wprowadza się do stosowania „Politykę bezpieczeństwa w Miejsko – Gminnym Zespole Oświaty, stanowiącą załącznik Nr 1 oraz „Instrukcję zarządzania systemem informatycznym w Miejsko – Gminnym Zespole Oświaty", stanowiącą załącznik Nr 2 do niniejszego zarządzenia.

§ 2

Zobowiązuje się pracowników Miejsko – Gminnego Zespołu Oświaty do zapoznania się z treścią oraz stosowania niniejszego zarządzenia.

§ 3

Zarządzenie wchodzi w życie z dniem podpisania z mocą obowiązującą od 09 września 2015r.

Załącznik Nr 1
do Zarządzenia Nr 5.2015 Dyrektora
Miejsko - Gminnego Zespołu Oświaty
z dnia 09.09.2015 r.

„Polityka bezpieczeństwa”
w Miejsko - Gminnym Zespole Oświaty w Drezdenku

Drezdenko, wrzesień 2015 r.

Historia Zmian dokumentu:

Data	*Osoba*	*opis*
04.05.2008r.	Ewa Pręt	Utworzenie dokumentu
09.09.2015r.	Ewa Pręt	Aktualizacja

1. Wprowadzenie

Dokument opracowano na podstawie § 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, poz. 1024).

Niniejszy dokument opisuje reguły dotyczące bezpieczeństwa danych osobowych zawartych w systemach informacyjnych w Miejsko – Gminnym Zespole Oświaty (MGZO).

Opisane reguły określają zachowanie wszystkich użytkowników systemów informatycznych oraz użytkujących systemy tradycyjne. Dokument zwraca uwagę na konsekwencje jakie mogą ponosić osoby nie przestrzegające zasad określonych w niniejszej polityce oraz procedury postępowania dla zapobiegania i minimalizowania skutków zagrożeń. Polityka bezpieczeństwa ma na celu uświadomienie potrzeby ochrony danych niezależnie od przyjmowanej przez nie formy (programy komputerowe, wydruki, dokumenty papierowe). Bezpieczeństwo systemów informatycznych odnosi się do wszystkich procesów związanych z przetwarzaniem informacji to jest: wytwarzania, przechowywania, archiwizowania, przesyłania, zbierania, prezentowania oraz niszczenia.

Deklaracja

Dyrektor Miejsko - Gminnego Zespołu Oświaty w Drezdenku deklaruje zaangażowanie w proces prawidłowego zarządzania bezpieczeństwem informacji w Miejsko - Gminnym Zespole Oświaty oraz oświadcza, iż dołoży wszelkich starań celem zapewnienia bezpieczeństwa informacji.

Definicje pojęć

MGZO – Miejsko – Gminny Zespół Oświaty w Drezdenku, ul. Ogrodowa 1, 66-530 Drezdenko.
Dane osobowe - każda informacja dotycząca osoby fizycznej pozwalająca na określenie tożsamości tej osoby.
Dane powierzone – każde dane powierzone Zespołowi zgodnie z porozumieniami ustalającymi zakres obowiązków dotyczących rachunkowości budżetowej oraz umowami powierzenia przetwarzania danych osobowych.
Zbiór danych – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępny według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.
Przetwarzanie danych osobowych – wykonywanie jakichkolwiek operacji na danych osobowych, takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, udostępnianie i ich usuwanie.
Administrator bezpieczeństwa informacji (ABI) – komórka w strukturze organizacyjnej nadzorująca przestrzeganie zasad ochrony przetwarzanych danych osobowych wynikających z przepisów i wewnętrznych ustaleń administratora danych.
Administrator systemu informatycznego (ASI) – osoba odpowiedzialna za administrację, konfigurację, prawidłowe funkcjonowanie sprzętu i oprogramowania, techniczno-organizacyjną obsługę oraz bezpieczeństwo danych osobowych przetwarzanych w systemach informatycznych, w tym w szczególności za przeciwdziałanie dostępowi osób trzecich do systemów oraz podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w tych systemach. Przy czym funkcję ASI, mogą pełnić osoby z firm zewnętrznych, które w ramach outsourcingu świadczą takie usługi na podstawie stosownej umowy.
Użytkownik systemu, zwany dalej użytkownikiem – osoba posiadająca upoważnienie wydane przez administratora danych, w zakresie w nim wskazanym, jako użytkownik do przetwarzania danych osobowych w systemie informatycznym danej komórki organizacyjnej.

Osoba trzecia – każda osoba nieupoważniona i przez to nieuprawniona do dostępu do danych osobowych zbiorów będących w posiadaniu administratora danych. Osobą trzecią jest również osoba posiadająca upoważnienie wydane przez administratora danych podejmująca czynności w zakresie przekraczającym ramy jej upoważnienia.
System informatyczny, zwany dalej systemem - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
System informacyjny - zespół współpracujących ze sobą urządzeń, nośników danych, programów, procedur przetwarzania informacji i narzędzi zastosowanych w celu przetwarzania danych.
Pod tym pojęciem rozumiemy systemy informatyczne jak i tradycyjne (papierowe).
Zabezpieczenie systemu informatycznego – wdrożenie przez administratora bezpieczeństwa informacji oraz administratora systemu informatycznego stosownych środków organizacyjnych i technicznych w celu zabezpieczenia zasobów oraz ochrony danych przed dostępem, modyfikacją ujawnieniem, pozyskaniem lub zniszczeniem przez osobę trzecią.
Zapewnienie bezpieczeństwa systemów informatycznych oznacza, utrzymanie takich atrybutów informacji jak:
Poufność, która oznacza ograniczony i ściśle zdefiniowany krąg osób mających dostęp do informacji.
Integralność, to jest zapewnienie niezmienności postaci informacji (postać oryginalna), za wyjątkiem momentów, kiedy informacja ta jest w sposób legalny modyfikowana.
Autentyczność (informacji, nadawcy, adresata) – oznacza to zgodność tożsamości informacji (nadawcy, adresata) z deklaracją do niej przypisaną.
Dostępność (informacji) dla wszystkich uprawnionych do tego osób.
Rozliczalność – oznaczająca precyzyjne i jednoznaczne powiązanie każdego dostępu do informacji z właściwą uprawnioną osobą, która tego dokonała.

W systemach informacyjnych MGZO są przetwarzane informacje stanowiące dane osobowe w rozumieniu art. 6 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Z 2014r., poz. 1182 z późn. zm.). Osobą odpowiedzialną za właściwy i niezakłócony przebieg przetwarzania danych jest Dyrektor MGZO.

Celem niniejszej Polityki Bezpieczeństwa jest wskazanie intencji i kierunków działań podjętych przez dyrekcje, dotyczących bezpieczeństwa informacji w działalności MGZO. Polityka Bezpieczeństwa Informacji jest dokumentem publicznie dostępnym, nadrzędnym dla bardziej szczegółowych polityk, regulaminów, instrukcji i procedur bezpieczeństwa.

Przez **bezpieczeństwo danych** (w tym danych osobowych) rozumie się zabezpieczenie danych (prowadzonych w sposób papierowy oraz w systemach informatycznych) rozumiane jako wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem. Ogólnym celem bezpieczeństwa danych jest niedopuszczenie do utraty integralności, poufności i dostępności przetwarzanych danych. Współużytkowanie informacji jest podstawą sprawnie działającej organizacji.

2. Krótkie wyjaśnienie polityki bezpieczeństwa, zasad, standardów i wymagań zgodności

1. Polityka bezpieczeństwa jest zgodna z następującymi aktami prawnymi:
    1) ustawą z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. z 2014 r. poz. 1182 z późn. zm.),
    2) rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024).

2. Konieczne jest stałe podnoszenie wiedzy poprzez kształcenie się w dziedzinie bezpieczeństwa przede wszystkim przez osoby zaangażowane w organizację i wdrażanie rozwiązań podnoszących bezpieczeństwo.
3. Podstawowym środkiem zapewnienia bezpieczeństwa systemom informatycznym jest bezwzględne stosowanie systemów antywirusowych oraz wykrywających i blokujących działalność szkodliwego oprogramowania. System taki winien być dwupoziomowy: na poziomie stacji roboczej oraz na styku lokalnej sieci komputerowej z siecią publiczną.
4. Systemy informatyczne muszą mieć zapewnione rozwiązania na wypadek awarii w celu zapewnienia ciągłości działania
5. Polityka bezpieczeństwa obowiązuje wszystkich pracowników MGZO. W przypadku jej naruszenia będą wyciągane konsekwencje służbowe lub karne.
6. Realizacja postanowień tego dokumentu ma zapewnić ochronę danych osobowych, właściwą ocenę i udokumentowanie przypadków naruszenia bezpieczeństwa systemów oraz zapewnić właściwy tryb działania w celu przywrócenia bezpieczeństwa danych przetwarzanych w systemach informatycznym. Każdy zauważony przypadek naruszenia bezpieczeństwa należy obowiązkowo zgłaszać do ABI.
7. Administrator danych, którym jest Dyrektor Miejsko - Gminnego Zespołu Oświaty wyznacza Administratora Bezpieczeństwa Informacji. Administrator Bezpieczeństwa Informacji realizuje zadania w zakresie ochrony danych, a w szczególności:
   1) Zapewnienia przestrzegania przepisów o ochronie danych osobowych,
   2) podejmowania stosownych działań w przypadku wykrycia nieuprawnionego dostępu do bazy danych lub naruszenia zabezpieczenia danych,
   3) niezwłocznego informowania Administratora Danych lub osobę przez niego upoważnioną o przypadkach naruszenia przepisów ustawy o ochronie danych osobowych,,
   4) wdrożenie fizycznego zabezpieczenia danych osobowych oraz obiektów, w których są gromadzone i przetwarzane.

3. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przy przetwarzaniu danych

1) Administrator danych osobowych jest obowiązany do zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych w systemach informatycznych, a w szczególności:

a) zabezpiecza dane przed ich udostępnieniem osobom nieupoważnionym,
b) zapobiega przed pobraniem danych przez osobę nieuprawnioną,
c) zapobiega zmianie, utracie, uszkodzeniu lub zniszczeniu danych,
d) zapewnia przetwarzanie danych zgodnie z obowiązującymi przepisami prawa.

2) Techniczną ochronę danych i ich przetwarzania realizuje się poprzez:

a) przetwarzanie danych osobowych w wydzielonych pomieszczeniach,
b) zabezpieczenie pomieszczeń, przed nieuprawnionym dostępem,
c) wyposażenie pomieszczeń dające gwarancję bezpieczeństwa dokumentacji (szafy, biurka, itp. zamykane na klucz),
d) stosowanie systemów kontroli dostępu, systemów alarmowych,
e) zastosowanie niszczarek dokumentów.

3) W celu ochrony przed utratą danych stosowane są następujące zabezpieczenia:

a) ochrona serwerów przed zanikiem zasilania poprzez stosowanie zasilaczy awaryjnych UPS o podwyższonej mocy,
b) ochrona przed utratą zgromadzonych danych przez robienie kopii zapasowych, z którego w przypadku awarii odtwarzane są dane,

c) redundantne rozwiązania pamięci masowych w serwerach.

4) Zabezpieczenia przed nieautoryzowanym dostępem do danych:

a) Administrator Systemu Informatycznego dba o zabezpieczenia sieci lokalnej,

b) w systemie informatycznym stosuje się podwójną autoryzację użytkownika. Pierwszej autoryzacji należy dokonać w momencie uruchamiania systemu operacyjnego komputera, podając hasło; drugiej autoryzacji należy dokonać uruchamiając program użytkowy, podając login użytkownika i hasło. Dostęp do wybranej bazy danych uzyskuje się dopiero po poprawnym zalogowaniu się do systemu informatycznego,

c) hasła użytkowników są poufne. Nie należy ich ujawniać, a jeśli taka sytuacja się zdarzy natychmiast należy hasło zmienić na inne,

d) nad konfiguracją sprzętu informatycznego czuwa Administrator Systemu Informatycznego. Zabronione jest umożliwianie dostępu do systemów informatycznych osobom nie mającym zgody lub upoważnienia wydanego przez Administratora Danych.

5) Zabezpieczenia przed nieautoryzowanym dostępem do danych poprzez internet.

Dostęp do sieci rozległej Internet realizowany jest poprzez sieć miejską, która zarządzana jest przez serwer Urzędu Miejskiego w Drezdenku.

W zakresie dostępu z sieci wewnętrznej do sieci rozległej Internet zastosowano środki ochrony przed podsłuchiwaniem, penetrowaniem i atakiem z zewnątrz. Zastosowano firewall sprzętowy, który ma za zadanie uwierzytelnianie źródła przychodzących wiadomości oraz filtrowanie pakietów w oparciu o adres IP, numer portu i inne parametry. Ściana ogniowa składa się z bezpiecznego systemu operacyjnego i filtra pakietów. Ruch pakietów, który firewall przepuszcza jest określony przez Administratora Systemu Informatycznego Urzędu Miejskiego w Drezdenku.

Firewall zapisuje do logu fakt zaistnienia wyjątkowych zdarzeń i śledzi ruch pakietów przechodzących przez nią.

W efekcie zapewnione jest:

1) zabezpieczenie sieci przed atakiem z zewnątrz poprzez blokowanie wybranych portów,

2) filtrowanie pakietów i blokowanie niektórych usług,

3) zapisywanie logów połączeń użytkowników z siecią Internet.

5) Ochrona antywirusowa.

Na każdym komputerze zainstalowany jest system antywirusowy Kaspersky, na bieżąco aktualizowany, z centralnym zarządzaniem. Poprzez panel administracyjny (centralnego zarządzania) Administrator Systemu Informatycznego może dokonać kontroli aktualności oraz zdarzeń poszczególnych instalacji systemu antywirusowego na stacjach roboczych.

6) Środki organizacyjne.

a) zapoznanie każdej osoby z przepisami dotyczącymi ochrony osobowych, przed dopuszczeniem jej do pracy przy ich przetwarzaniu,

b) W tym celu osoba jest kierowana do Administratora Bezpieczeństwa Informacji celem zapoznania z przepisami Ustawy o Ochronie Danych Osobowych oraz dokumentami wewnętrznymi w tym zakresie. Oświadczenie o zaznajomieniu z przepisami, po podpisaniu, trafia do dokumentacji kadrowej danej osoby.

c) przeszkolenie osób w zakresie bezpiecznej obsługi urządzeń i programów związanych z przetwarzaniem i ochroną danych osobowych oraz zabezpieczenia pomieszczeń i budynków,

d) kontrolowanie pomieszczeń, w których są przetwarzane dane osobowe.

e) po zakończeniu pracy dokumenty przechowuje się w szafach zamkniętych na klucz.

f) Wszystkich pracowników MGZO obowiązuje polityka czystego biurka i czystego ekranu. Polityka czystego biurka oznacza chowanie do szaf dokumentów po zakończeniu pracy. Żadne dokumenty nie zostają po godzinach pracy na biurkach. Polityka czystego ekranu oznacza stosowanie środków uniemożliwiających wgląd osobom trzecim do informacji przetwarzanych na ekranie komputera.
g) Wszystkie dokumenty niepotrzebne muszą być niszczone w sposób nie pozwalający na odtworzenie zawartych w nich informacji, np. w niszczarkach dokumentów
h) Po każdej aktualizacji w/w dokumentacji organizowane są szkolenia celem zaznajomienia pracowników ze zmianami.
i) Na stanowiskach pracy należy dbać, by po zakończeniu pracy wszystkie dokumenty były chowane do szaf zamykanych na klucz.
j) Klucze do pomieszczeń podlegają szczególnej ochronie.
k) Klucze do pomieszczeń, w których są przetwarzane dane osobowe znajdują się w dyspozycji osób upoważnionych do przetwarzania danych i nie są udostępniane osobom postronnym. Z wyjątkiem personelu sprzątającego i usuwającego zaistniałe w tych pomieszczeniach awarie posiadającego zgodę administratora danych.
l) Zabrania się umożliwianiu dostępu osób nieupoważnionych do danych osobowych, w tym do systemów informatycznych.
m) ABI prowadzi rejestr zdarzeń, w którym odnotowuje wszystkie zdarzenia związane z bezpieczeństwem systemów informatycznych w szczególności incydentów, wg wzoru:

l.p.	**data**	**opis zdarzenia**	**podjęte czynności**	**uwagi**
1.				
2.				
3.				

n) Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, wszczyna się postępowanie dyscyplinarne.
o) Przebywanie w pomieszczeniach w których są przetwarzane dane osobowe osób nieupoważnionych do zapoznania się z danymi osobowymi jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania danych.
p) Dla nowo zatrudnionego pracownika stosuje się następujące zasady:
    - Pracownik odbywa szkolenie u Administratora Bezpieczeństwa Informacji polegające na zapoznaniu się z przepisami Ustawy o Ochronie Danych osobowych, Polityki Bezpieczeństwa i Instrukcji Zarządzania Systemem Informatycznym. Na szkolenie kieruje pracownik ds. Kadr.
    - Po szkoleniu pracownik potwierdza odbycie szkolenia własnoręcznym podpisem na oświadczeniu. Oświadczenie trafia do akt osobowych osoby zatrudnionej przy przetwarzaniu danych osobowych
    - Pracownik otrzymuje upoważnienie do przetwarzania danych osobowych oraz zostaje zobowiązany do przestrzegania zasad dot. ochrony danych
    - ABI prowadzi ewidencję upoważnień wg. wzoru:

Ewidencja
upoważnień do przetwarzania danych osobowych
w Miejsko - Gminnym Zespole Oświaty w Drezdenku

L.p	Użytkownik: Imię Nazwisko	data nadania uprawnień data ustania uprawnień	zakres upoważnienia	Identyfikator (login)
1.				

.....
(data i podpis administratora danych

- Upoważnienia do przetwarzania danych osobowych sporządza ABI, dla każdej osoby której obowiązki służbowe wymagają dostępu do danych osobowych. Upoważnienie zatwierdza administrator danych

- Upoważnienie sporządza się wg. wzoru:

Drezdenko, dnia …… r.

Upoważnienie do przetwarzania danych osobowych
załącznik do „Polityki Bezpieczeństwa" zgodnie z Art 37 Ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r.

…..... jako Administrator Danych dnia ..... nadaje upoważnienie do przetwarzania danych osobowych
w podmiocie ..... dla:

Imię i nazwisko: .....

Adres zamieszkania: .....

Nr PESEL: .....

Stanowisko służbowe: .....

Upoważniony otrzymuje dostęp do poniższych zasobów danych osobowych w celu ich przetwarzania:

….....

….....

….....

Upoważnienie nadaje się do dnia .....
Upoważniony zobowiązuje się do przestrzegania zasad panujących w podmiocie w zakresie ochrony danych osobowych a w szczególności „Polityki Bezpieczeństwa" oraz respektowania zapisów **Ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r.** Upoważnionego obowiązuje tajemnica dotycząca danych osobowych przetwarzanych w podmiocie oraz sposobów zabezpieczeń.

Administrator Danych

….....
Podpis

Użytkownik

….....
Podpis

q) Dla pracownika, który kończy zatrudnienie stosuje się następujące zasady:
- Pracownik stanowiska ds. Kadr informuje ABI o zakończeniu pracy pracownika podając jego imię i nazwisko oraz datę zakończenia zatrudnienia..
- Administrator Systemu Informatycznego blokuje dostęp do uprawnień w systemach informatycznych - blokowane są konta z których pracownik korzystał.
- Zostaje odnotowany fakt ustania uprawnień w ewidencji upoważnień.

q) Używanie nośników danych
r) Zabrania się używania innych nośników danych niż nośniki służbowe.
s) Zabronione jest samowolne instalowanie oprogramowania na stanowiskach komputerowych.
t) Zmiany i udostępnienie tekstu Polityki Bezpieczeństwa
- Dopuszcza się dokonywanie zmian w niniejszym dokumencie, w przypadku zmian warunków lub stanu opisanego w nim
- Tekst Polityki Bezpieczeństwa zostanie udostępniony użytkownikom w formie zarządzenia opublikowanego w BIP.

u) Przekazywanie danych powierzonych
- Dane osobowe powierzone Miejsko – Gminnemu Zespołowi Oświaty w drodze umowy będą przekazywane: upoważnionemu pracownikowi danej placówki w formie papierowej, drogą elektroniczną, pocztą, przez kuriera w zabezpieczonej odpowiednio przesyłce.
- Osoby upoważnione weryfikowane będą na podstawie przekazanego Miejsko – Gminnemu Zespołowi Oświaty wykazu osób upoważnionych przez daną placówkę.

4. KONTROLA PRZESTRZEGANIA ZASAD ZABEZPIECZENIA DANYCH OSOBOWYCH

- Administrator Bezpieczeństwa Informacji sprawuje nadzór nad przestrzeganiem zasad ochrony danych osobowych wynikający z ustawy o ochronie danych osobowych oraz zasad ustanowionych w niniejszym dokumencie.
- Administrator Bezpieczeństwa Informacji przeprowadza audyt stanu bezpieczeństwa przetwarzania danych osobowych
- Administrator Systemu Informatycznego przeprowadza audyt stanu bezpieczeństwa przetwarzana danych w systemach informatycznych.
- Wnioski z audytu przedstawiane są Administratorowi Danych Osobowych.

5. POSTĘPOWANIE W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

a) W przypadku stwierdzenia naruszenia:
- zabezpieczenia systemu informatycznego,
- technicznego stanu urządzeń,
- zawartości zbioru danych osobowych,
- jakości transmisji danych w sieci telekomunikacyjnej mogącej wskazywać na naruszenie zabezpieczeń tych danych,
- innych zdarzeń mogących mieć wpływ na naruszenie danych osobowych (np. zalanie, pożar, kradzież itp.)

Każda osoba jest zobowiązana do niezwłocznego powiadomienia o tym fakcie Administratora Bezpieczeństwa Informacji i bezpośredniego przełożonego.

b) Następnie należy:

- niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia, o ile istnieje taka możliwość, a następnie uwzględnić w działaniu również ustalenie przyczyn lub sprawców,
- rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia,
- zaniechać - o ile to możliwe - dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę zdarzenia,
- podjąć stosowne działania, jeśli zaistniały przypadek jest określony w dokumentacji systemu operacyjnego lub aplikacji użytkowej,
- zastosować się do innych instrukcji i regulaminów, jeżeli odnoszą się one do zaistniałego przypadku,
- nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Administratora Bezpieczeństwa Informacji lub osoby upoważnionej.

Po przybyciu na miejsce naruszenia lub ujawnienia ochrony danych osobowych, Administrator Bezpieczeństwa Informacji:

- zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania mając na uwadze ewentualne zagrożenia dla prawidłowości pracy,
- może żądać dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem,
- w razie potrzeby powiadamia o zaistniałym naruszeniu Dyrektora MGZO,
- jeżeli zachodzi taka potrzeba zleca usunięcie występujących naruszeń, oraz powiadamia odpowiednie instytucje,
- Administrator Bezpieczeństwa Informacji dokumentuje zaistniały przypadek naruszenia oraz sporządza raport wg wzoru.
- Raport Administrator Bezpieczeństwa Informacji niezwłocznie przekazuje Administratorowi Danych Osobowych, a w przypadku jego nieobecności osobie uprawnionej.
- Zaistniałe naruszenie może stać się przedmiotem szczegółowej analizy prowadzonej przez zespół powołany przez Dyrektora MGZO.
- Analiza powinna zawierać wszechstronną ocenę zaistniałego naruszenia, wskazanie odpowiedzialnych, wnioski co do ewentualnych przedsięwzięć proceduralnych, organizacyjnych, kadrowych i technicznych, które powinny zapobiec podobnym naruszeniom w przyszłości.

6. Obszar przetwarzania danych osobowych:

Wykaz pomieszczeń, w których przetwarzane są dane osobowe.

Lp.	Nazwa komórki	Lokalizacja
1.	Miejsko - Gminny Zespół Oświaty	Budynek Miejsko – Gminnego Zespołu Oświaty w Drezdenku

7. Wykaz zbiorów danych osobowych

7.1 Zbiory informatyczne

Lp	Zbiór danych	Poziom bezp.	metoda dostępu	Systemy informatyczny	Lokalizacja fizyczna, pomieszczenia w którym są przetwarzane dane	Rejestracja w GIODO	Dane osobowe	Cel przetwarzania danych w zbiorze
1.	System Qwant – System księgowy	Wysoki	LAN	Qwant	Budynek Miejsko - Gminnego Zespołu Oświaty, pomieszczenia: Księgowość, Kasa	N	Imię nazwisko, adres (ulica, nr domu, miasto), nr rachunku bankowego, NIP	ewidencja dokumentów księgowych, sprawozdawczość system archiwalny
2.	System Qwark – System płacowy	Wysoki	LAN	Qwark	Budynek Miejsko – Gminnego Zespołu Oświaty, pomieszczenia: Płace,	T	Imię nazwisko, adres pracownika (ulica, nr domu, miasto), data urodzenia, nr rachunku bankowego, NIP, PESEL, nr tel., nr dowodu osobistego, nazwisko rodowe, imiona rodziców,	ewidencja kartoteki osób dla których wyliczane są płace, eksport danych do systemu płatnik, drukowanie list płac, drukowanie indywidualnych pasków wypłaty, drukowanie dokumentów PIT ewidencje nieobecności, system archiwalny
3.	System Płatnik	Wysoki	LAN	Płatnik	Budynek Miejsko – Gminnego Zespołu Oświaty, pomieszczenia: Płace	T	Imię nazwisko, adres pracownika (ulica, nr domu, miasto), data urodzenia, NIP, PESEL, nr dowodu osobistego, nazwisko rodowe, imię i nazwisko członka rodziny	Prowadzenie ewidencji osób ubezpieczonych w ZUS, wymiana elektroniczna dokumentów z ZUS
4.	System SIO – system informacji oświatowej	Wysoki	bezpośredni	SIO	Budynek Miejsko – Gminnego Zespołu Oświaty, Dyrektor, Sekretariat	T	imię i nazwisko użytkownika	Sprawozdawczość

5.	System SJO Besti@	Wysoki	bezpośre dni	SJO Besti@	Budynek Miejsko – Gminnego Zespołu Oświaty, pomieszczenia: Księgowość	T	imię i nazwisko użytkownika	Sporządzanie sprawozdań finansowych i budżetowych
6.	System sQola – Integra - FK	Wysoki	LAN	sQola – Integra	Budynek Miejsko – Gminnego Zespołu Oświaty, pomieszczenia: Księgowość, Kasa	T	Imię nazwisko, adres (ulica, nr domu, miasto), nr rachunku bankowego, NIP	ewidencja dokumentów księgowych, sprawozdawczość
7.	System sQola – Integra – Płace	Wysoki	LAN	sQola – Integra	Budynek Miejsko – Gminnego Zespołu Oświaty, pomieszczenia: Płace, Księgowość	T	Imię nazwisko, adres pracownika (ulica, nr domu, miasto), data urodzenia, nr rachunku bankowego, NIP, PESEL, nr tel., nr dowodu osobistego, nazwisko rodowe, imiona rodziców,	ewidencja kartoteki osób dla których wyliczane sa płace, eksport danych do systemu płatnik, drukowanie list płac, drukowanie indywidualnych pasków wypłaty, drukowanie dokumentów PIT ewidencje nieobecności
8.	Przelewy 2001, Klient Home Banking	Wysoki	bezpośre dni	Przelewy 2001	Budynek Miejsko – Gminnego Zespołu Oświaty, pomieszczenia: Kasa	N	Imię nazwisko, adres (ulica, nr domu, miasto), nr rachunku bankowego,	przygotowywanie i wysyłanie przelewów bankowych
9.	Kasa ZP	Wysoki	LAN	sQola - Integra	Budynek Miejsko – Gminnego Zespołu Oświaty, pomieszczenia: Księgowość, Kasa, Sekretariat	T	Imię nazwisko, adres pracownika (ulica, nr domu, miasto), data urodzenia, nr rachunku bankowego, NIP, PESEL, nr tel., nr dowodu osobistego, nazwisko rodowe, imiona rodziców,	Dokumentacja związana z prowadzeniem Kasy Zapomogowo Pożyczkowej, Prowadzenie kartotek członków KZP, przygotowywanie i wysyłanie przelewów.

10.	System sQola – Integra – Kadry	Wysoki	LAN	sQola - Integra	Budynek Miejsko – Gminnego Zespołu Oświaty, pomieszczenia: Sekretariat, Płace	T	Imię, nazwisko, adres pracownika (ulica, nr domu, miasto), data urodzenia, miejsce urodzenia, NIP, PESEL, nr tel., nr dowodu osobistego, nazwisko rodowe, imiona rodziców,	Ewidencja kartoteki osób dla których wyliczane są płace.
11.	Przetargi	Wysoki	bezpośredni	Forum Media Polska	Budynek Miejsko – Gminnego Zespołu Oświaty, pomieszczenia: Kasa	T	Imię, nazwisko, nazwa firmy, NIP, adres	Przygotowanie i przeprowadzanie postępowania przetargowego
12.	Pomoc Materialna dla Uczniów	Wysoki	LAN oraz bezpośredni	Sputnik Software	Budynek Miejsko – Gminnego Zespołu Oświaty, pomieszczenia: Stypendia	T	Imię nazwisko ucznia oraz wnioskodawcy, adres (ulica, nr domu, miasto), data urodzenia, miejsce urodzenia, NIP, PESEL, nr tel., nr dowodu osobistego, nazwisko rodowe, imiona rodziców,	Ewidencja ubiegających się o pomoc materialną, przygotowanie list wypłat dla osób uprawnionych do uzyskania pomocy materialnej
13.	System sQola – Integra - QDeklaracje	Wysoki	LAN	sQola	Budynek Miejsko – Gminnego Zespołu Oświaty, pomieszczenia: Płace	T	Imię nazwisko, adres pracownika (ulica, nr domu, miasto), data urodzenia, PESEL, przychody,	Przygotowywanie i przesyłanie deklaracji podatkowych

7.2 Zbiory manualne

l.p.	zbiory	Lokalizacja fizyczna, pomieszczenia w którym są przetwarzane dane	Rejestra -cja w GIODO	Dane osobowe	**Cel przetwarzania danych w zbiorze**
1.	**Zbiór dokumentów dotyczące stypendiów dla uczniów** o Zbiór list wypłat stypendiów	Budynek Miejsko – Gminnego Zespołu Oświaty, pomieszczenia: Stypendia, Księgowość, Kasa,	T	imię i nazwisko	ewidencjonowanie list wypłat stypendiów
2.	**Zbiór dokumentów księgowych** o Dowody księgowe o Kwitariusz – rejestr wpłat (T) o Rejestr faktur o Rejestr umów cywilno-prawnych o Tabele kalkulacyjne płac o Rejestr czeków pozostający w dyspozycji MGZO o Zbiór dokumentów dotyczących wyjazdów szkolnych uczniów o Zbiór dokumentów dotyczących pomocy materialnej dla uczniów (T) o Zbiór dokumentów dotyczących wyprawki szkolnej (T) o Zbiór dokumentów dotyczących pracowników młodocianych (T)	Budynek Miejsko – Gminnego Zespołu Oświaty, pomieszczenia: Księgowość, Kasa, Stypendia,	N	Imię nazwisko, adres (ulica, nr domu, miasto), nr rachunku bankowego, NIP	gromadzenie papierowych dokumentów księgowych,
3.	**Zbiór danych dotyczących pracowników MGZO** o Teczki akt osobowych pracowników własnych o Zbiór dokumentów dot. umów zleceń i cywilno-prawnych o Listy płac i wypłat świadczeń z funduszu socjalnego o Karty wynagrodzeń i zasiłkowe o Rozliczenia miesięczne i roczne (pity) o Deklaracje rozliczeniowe pracowników o Tabele miesięcznych wynagrodzeń pracowników	Budynek Miejsko – Gminnego Zespołu Oświaty, pomieszczenia: Sekretariat, Płace, Kasa,	N	Imię nazwisko, adres pracownika (ulica, nr domu, miasto), data urodzenia, nr rachunku bankowego, NIP, PESEL, nr tel., nr dowodu osobistego, nazwisko	gromadzenie dokumentów papierowych

	o Dokumenty związane z przeszeregowaniem pracowników o Roczna karta ewidencji obecności w pracy i karty urlopowe o Dokumenty zgłoszeniowe pracowników o Dokumenty pod nazwą kapitał początkowy o Dokumenty dot. badań okresowych pracowników o Zbiór pism dot. spraw BHP o Rejestr wypadków w pracy i poza pracą pracowników o Zbiór list obecności pracowników MGZO o Zbiór dokumentów dot. badań lekarskich pracowników MGZO o Zbiór okresowych ocen pracowników			rodowe, imiona rodziców,	
4.	**Zbiór kopii akt osobowych dyrektorów jednostek oświatowych**	Budynek Miejsko - Gminnego Zespołu Oświaty, pomieszczenia: Sekretariat,	T	Imię nazwisko, adres pracownika (ulica, nr domu, miasto), data urodzenia, nr rachunku bankowego, NIP, PESEL, nr tel., nr dowodu osobistego, nazwisko rodowe, imiona rodziców	naliczanie płac
5.	**Zbiór umów i porozumień**	Budynek Miejsko - Gminnego Zespołu Oświaty, pomieszczenia: Sekretariat, Księgowość, Archiwum	T	Imię nazwisko, adres pracownika (ulica, nr domu, miasto), nr rachunku bankowego, NIP, PESEL, nr tel.	ewidencjonowanie umów i porozumień w celach statutowych
6.	**Zbiór dokumentów dotyczących płac**	Budynek Miejsko – Gminnego Zespołu Oświaty, pomieszczenia: Płace,	T	Imię nazwisko, adres pracownika (ulica, nr domu, miasto), data urodzenia, nr rachunku bankowego, NIP, PESEL, nr tel.,	ewidencjonowanie i archiwizowanie

				nr dowodu osobistego, nazwisko rodowe, imiona rodziców,	
7.	**Zbiór pocztowych książek nadawczych**	Budynek Miejsko – Gminnego Zespołu Oświaty, pomieszczenia: Sekretariat,	T	Imię nazwisko, adres pracownika (ulica, nr domu, miasto)	wysyłanie korespondencji
8.	**Ewidencja korespondencji wpływającej i wychodzącej**	Budynek Miejsko – Gminnego Zespół Oświaty, pomieszczenia: Sekretariat,	T	Imię nazwisko, adres pracownika (ulica, nr domu, miasto)	ewidencjonowanie korespondencji
9.	**Zbiór dokumentów dotyczących kapitału początkowego i świadczeń emerytalno-rentowych pracowników jednostek oświatowych**	Budynek Miejsko – Gminnego Zespołu Oświaty, pomieszczenia: Płace,	T	Imię nazwisko, adres pracownika (ulica, nr domu, miasto), data urodzenia, nr rachunku bankowego, NIP, PESEL, nr tel., nr dowodu osobistego, nazwisko rodowe, imiona rodziców,	ewidencjonowanie dokumentów
10.	**Zbiór dokumentów BHP pracowników jednostek oświatowych**	Budynek Miejsko – Gminnego Zespołu Oświaty, pomieszczenia: Sekretariat,	T	Imię nazwisko, adres (ulica, nr domu, miasto), data urodzenia, miejsce urodzenia, Pesel	ewidencjonowanie szkoleń BHP
11.	**Zbiór dokumentów BHP dotyczących wypadków** • **dokumentacja wypadkowa** • **rejestr wypadków**	Budynek Miejsko – Gminnego Zespołu Oświaty, pomieszczenia: Sekretariat,	T wrażliwe	Imię nazwisko, adres (ulica, nr domu, miasto), data urodzenia, numer dowodu osobistego	protokoły ustaleń przyczyn wypadków

12.	**Dokumentacja dotycząca dofinansowania do dokształcania i doskonalenia nauczycieli**	Budynek Miejsko – Gminnego Zespołu Oświaty, pomieszczenia: Sekretariat, Księgowość,	T	Imię nazwisko, adres (ulica, nr domu, miasto), NIP, PESEL	Prowadzenie dokumentacji dofinansowania doskonalenia zawodowego nauczycieli
13.	**Zbiór dokumentów dotyczących dowożenia dzieci do szkół**	Budynek Miejsko – Gminnego Zespołu Oświaty, pomieszczenia: Sekretariat, Kasa	T	Imię nazwisko, adres (ulica, nr domu, miasto)	realizacja obowiązku dowożenia dzieci
14.	**Zbiór dokumentów dotyczących ZFŚS pracowników i emerytów jednostek oświatowych**	Budynek Miejsko – Gminnego Zespołu Oświaty, pomieszczenia: Sekretariat, Księgowość,	T	Imię nazwisko, adres (ulica, nr domu, miasto)	realizacja świadczeń z ZFŚS
15.	**Zbiór dokumentów dotyczących grupowych ubezpieczeń pracowniczych pracowników jednostek oświatowych**	Budynek Miejsko – Gminnego Zespołu Oświaty, pomieszczenia: Płace,	T	Imię nazwisko, adres (ulica, nr domu, miasto), nr tel., data urodzenia, miejsce urodzenia, PESEL, nr. tel., email	realizacja umów, potrącanie składek, zgłaszanie spraw do ubezpieczyciela
16.	**Zbiór dokumentów ubezpieczeń społecznych, zdrowotnych i funduszu pracy pracowników jednostek oświatowych**	Budynek Miejsko – Gminnego Zespołu Oświaty, pomieszczenia: Płace,	T	Imię nazwisko, adres (ulica, nr domu, miasto), nr tel., data urodzenia, miejsce urodzenia, PESEL, nr. tel,	naliczanie płac, zgłaszanie do ZUS, rozliczanie składek z ZUS, rejestrowanie i wyrejestrowywanie osób
17.	**Zbiór arkuszy organizacyjnych**	Budynek Miejsko Gminnego Zespołu Oświaty, pomieszczenia: Sekretariat,	T	Imię nazwisko	wyliczanie godzin pracy i etatów
18.	**Zbiór wykazów uczniów korzystających z żywienia** - wykazy stołówki szkolnej - wykazy stołówki przedszkolnej	Budynek Miejsko – Gminnego Zespołu Oświaty, pomieszczenia: Księgowość, Sekretariat,	T	Imię nazwisko	rozliczanie z żywienia uczniów
19.	**Zbiór wykazów opłat za świadczenia udzielane przez Publiczne Przedszkole**	Budynek Miejsko – Gminnego Zespołu	T	Imię nazwisko	rozliczanie godzin ponad obowiązkowy wymiar

		Oświaty, pomieszczenia: Księgowość,			
20.	**Zbiór pełnomocnictw, upoważnień i oświadczeń**	Budynek Miejsko – Gminnego Zespołu Oświaty, pomieszczenia: Sekretariat,	T	Imię nazwisko	realizacja zadań statutowych
21.	**Zbiór zaświadczeń o zatrudnieniu i wynagrodzeniu pracowników jednostek oświatowych**	Budynek Miejsko – Gminnego Zespołu Oświaty, pomieszczenia: Płace,	T	Imię nazwisko, adres (ulica, nr domu, miasto), NIP, PESEL, nazwisko rodowe, nr tel.	ewidencjonowanie wydanych zaświadczeń
22.	**Zbiór zwolnień lekarskich**	Budynek Miejsko – Gminnego Zespołu Oświaty, pomieszczenia: Płace, Sekretariat,	T	Imię nazwisko, adres (ulica, nr domu, miasto), NIP, PESEL	rozliczanie nieobecności do płac
23.	**Ewidencja delegacji pracowników MGZO**	Budynek Miejsko – Gminnego Zespołu Oświaty, pomieszczenia: Sekretariat, Księgowość,	N	Imię nazwisko	ewidencjonowanie wyjazdów służbowych
24.	**Zbiór dokumentów dotyczących inwentaryzacji**	Budynek Miejsko - Gminnego Zespołu Oświaty, pomieszczenia: Księgowość	T	Imię nazwisko	przeprowadzanie inwentaryzacji
25.	**Dokumentacja Administratora Bezpieczeństwa Informacji**	Budynek Miejsko – Gminnego Zespołu Oświaty, pomieszczenia: Sekretariat	N	Imię nazwisko	realizacja obowiązków ABI
26.	**Rejestr Skarg i Wniosków**	Budynek Miejsko – Gminnego Zespołu Oświaty, pomieszczenia: Sekretariat	T	Imię nazwisko	Dopełnienie obowiązków określonych w przepisach prawa
27.	**Kandydaci na Dyrektorów**	Budynek Miejsko – Gminnego Zespołu	T	Imię nazwisko,	Dopełnienie obowiązków określonych w przepisach prawa

		Oświaty, pomieszczenia: Sekretariat			
28.	**Archiwum**	Budynek Miejsko – Gminnego Zespołu Oświaty, pomieszczenia: Archiwum		Imię nazwisko, adres pracownika (ulica, nr domu, miasto), data urodzenia, nr rachunku bankowego, NIP, PESEL, nr tel., nr dowodu osobistego, nazwisko rodowe, imiona rodziców,	Dopełnienie obowiązków określonych w przepisach prawa

7.3. ABI prowadzi rejestr zbiorów danych zgodnie z Rozporządzeniem Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych.

8. Opis zawartości zbiorów

8.1 System sQola

Wszelkie dane osobowe pracowników z których korzystają dowolne programy autorstwa QNT pracujące w środowisku Windows z użyciem baz danych Sybase Adaptive Server Anywhere, zlokalizowane są w jednym zbiorze o nazwie qnt_dane.db. Baza danych systemu umieszczona jest na serwerze w lokalizacji wskazanej przez użytkownika w czasie pierwszej instalacji systemu. Dodatkowo baza danych tworzy zbiór o nazwie qnt_dane.log, w którym umieszczany jest pełen dziennik wszystkich wykonanych przez użytkowników operacji, dotyczących pobrania, modyfikacji bądź wprowadzenia danych do bazy danych systemu.
Oba wyżej wymienione zbiory, zawierające bazę danych systemu, zabezpieczone są przed nieautoryzowanym dostępem, poprzez zaszyfrowanie. Osoba może uzyskać dostęp do tych danych tylko z poziomu odpowiedniej aplikacji, po wcześniejszym podaniu nazwy użytkownika oraz hasła. Dodatkowo użytkownik systemu, który chce uzyskać dostęp do danych, musi posiadać odpowiednie uprawnienia nadane mu przez administratora systemu.

- Opis struktury bazy danych systemu FK zawarty jest w dokumencie „Architektura bazy danych"
- Opis struktury bazy danych systemu Płace zawarty jest w dokumencie **"**Struktura bazy danych QNT Systemy Informatyczne"
- Opis struktury bazy danych systemu Płatnik zawarty jest w dokumencie „Program Płatnik Struktury danych osobowych"

9. Sposób przepływu danych pomiędzy systemami *(§4 pkt 4 rozporządzenia)*

Przedstawiony przepływ danych pomiędzy systemami określa sposób współpracy między różnymi systemami informatycznymi oraz relacje, jakie istnieją pomiędzy danymi zgromadzonymi w zbiorach do przetwarzania.

9.1 Wymiana danych pomiędzy programami płacowym i kadrowym, a programem Płatnik

Programy płacowy i kadrowy posiadają funkcję tworzenia deklaracji do programu Płatnik i ich automatycznego eksportowania do tego programu. Eksport deklaracji odbywa się za pośrednictwem plików tekstowych, które potem program Płatnika importuje.
Program płacowy tworzy następujące deklaracje ZUS: ZUA, ZZA, DRA, RCA, RSA, RZA, ZWUA,
Program kadrowy tworzy następujące deklaracje ZUS: ZUA, ZWUA, ZCZA, ZCNA, ZIUA.
Szczegółowa specyfikacja zawartości plików opisana jest w dokumencie "Specyfikacja wejścia – wyjścia", (dokument obowiązujący dla nowej wersji programu Płatnik) na stronach internetowych ZUS (www.zus.gov.pl)

9.2 Wymiana danych pomiędzy programem płacowym a systemami bankowości elektronicznej

Program płacowy umożliwia tworzenie plików zawierających przelewy na konta osobiste pracowników. Przelewy wykonywane są na podstawie kwot z wybranych wypłat pracowników. Do tego celu służy zlecenie Wydruki, Przelewy, Eksport elektronicznych przelewów z wypłat.
Po wybraniu zlecenia dokonuje się wyboru formatu eksportu oraz nazwy tworzonego pliku z przelewami.
W zależności od wybranego formatu eksportowane są różne informacje dotyczące pracownika:

- Nazwisko,
- Imię,
- Adres,

- Oddział banku,
- Numer konta,
- Kwota przelewu,
- Tytuł przelewu.

10. OPIS ZDARZEŃ NARUSZAJĄCYCH OCHRONĘ DANYCH OSOBOWYCH

10.1 Podział zagrożeń:

1) Zagrożenia losowe zewnętrzne (np. klęski żywiołowe, przerwy w zasilaniu) - ich występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu; ciągłość systemu zostaje zakłócona, nie dochodzi do naruszenia poufności danych.
2) Zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki operatorów, administratora, awarie sprzętowe, błędy oprogramowania, pogorszenie jakości sprzętu i oprogramowania) - może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych.
3) Zagrożenia zamierzone - świadome i celowe działania powodujące naruszenia poufności danych, (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy), zagrożenia te możemy podzielić na:
    - nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu),
    - nieuprawniony dostęp do systemu z jego wnętrza,
    - nieuprawnione przekazanie danych,
    - bezpośrednie zagrożenie materialnych składników systemu (np. kradzież sprzętu),
      wprowadzenie oprogramowania zagrażającemu bezpieczeństwu informacji przetwarzanych przez MGZO

10.2 Naruszenie lub podejrzenie naruszenia systemu informatycznego, w którym przetwarzane są dane osobowe następuje w sytuacji:

1) losowego lub nieprzewidzianego oddziaływania czynników zewnętrznych na zasoby systemu jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, itp.,
2) niewłaściwych parametrów środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych,
3) awarii sprzętu lub oprogramowania, które wyraźnie wskazuje na umyślne działanie w kierunku naruszenia ochrony danych,
4) pojawienia się odpowiedniego komunikatu alarmowego,
5) podejrzenia nieuprawnionej modyfikacji danych w systemie lub innego odstępstwa od stanu oczekiwanego,
6) naruszenia lub próby naruszenia integralności systemu lub bazy danych w tym systemie,
7) pracy w systemie wykazującej odstępstwa uzasadniające podejrzenie przełamania lub zaniechania ochrony danych osobowych - np. praca osoby, która nie jest formalnie dopuszczona do obsługi systemu,
8) ujawnienia nieautoryzowanych kont dostępu do systemu,
9) naruszenia dyscypliny pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (np. nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, itp.).

10.3 Za naruszenie ochrony danych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia fizycznego miejsc przechowywania i przetwarzania danych osobowych np.

10.3.1.1 niezabezpieczone pomieszczenia,
10.3.1.2 nie nadzorowane, otwarte szafy, biurka, regały,
10.3.1.3 niezabezpieczone urządzenia archiwizujące,
10.3.1.4 pozostawianie danych w nieodpowiednich miejscach – kosze, stoły itp.,
10.3.1.5 pozostawienie dokumentów niezabezpieczonych po zakończeniu pracy,
10.3.1.6 używanie prywatnych nośników danych.

11. Analiza ryzyka

lp	ryzyko	prawdopodobie	skutek	wartość	odpowiedź na ryzyko
1.	włamanie	1	4	4	
2.	kradzież	1	5	5	
3.	awaria stacji roboczej (sprzęt)	2	4	8	
4.	awaria stacji roboczej (oprogramowanie)	2	4	8	
5.	awaria serwera (sprzęt)	2	5	10	zapewnienie obsługi informatycznej w celu szybkiej naprawy
6.	awaria serwera (oprogramowanie)	2	5	10	wykonywanie codziennych kopii całościowych serwera, monitorowanie
7.	awaria infrastruktury sieciowej (połączeń sieciowych)	2	5	10	zapewnienie obsługi informatycznej w celu szybkiej naprawy
8.	brak obsługi informatycznej	1	5	5	
9.	awaria dostępu do Internetu	2	1	2	
10.	błędy oprogramowania systemowego	2	3	6	
11.	błędy oprogramowania dziedzinowego (FK, Płace, Płatnik itp.)	1	4	4	
12.	włamania heckerów	2	3	6	
13.	ataki wirusów komputerowych	4	4	16	zapewnienie aktualnej wersji systemu antywirusowego, zapewnienie funkcjonalności firewall na styku z siecią publiczną
14.	błędy użytkownika	2	5	10	zapewnienie odpowiedniego przeszkolenia pracowników, udzielanie im pomocy w razie potrzeby
15.	uzyskanie dostępu osoby nieupoważnionej do stacji roboczej	2	5	10	zapewnienie odpowiedniego poziomu złożoności haseł oraz ich okresowej wymiany

16.	uzyskanie dostępu osoby nieupoważnionej do serwera	2	5	10	zapewnienie odpowiedniego poziomu złożoności haseł oraz ich okresowej wymiany
17.	uzyskanie dostępu osoby nieupoważnionej do szafy teleinformatycznej	2	5	10	zabezpieczenie dostępu do szafy
18.	awarie zasilania	3	4	12	zapewnienie podtrzymania zasilania w razie awarii - UPS
19.	awarie UPS serwerów	3	5	15	okresowe sprawdzanie poprawności działania UPSów, w razie potrzeby wymiana UPS
20.	złośliwe działania użytkowników	2	5	10	podnoszenie świadomości wśród pracowników, monitorowanie ich pracy, zapewnienie tworzenia codziennych kopii danych
21.	błędy użytkowników	3	4	12	zapewnienie tworzenia codziennych kopii danych
22.	używanie prywatnych nośników danych (pendrive)	3	4	12	podnoszenie świadomości wśród pracowników, blokowanie pendrive'ów niesłużbowych
23.	długie przerwy w pracy systemów w związku z długotrwałą naprawą	1	4	4	zapewnienie obsługi informatycznej w celu szybkiej naprawy
24.	brak wykonywanych kopii danych	2	5	10	monitorowanie mechanizmu tworzenia kopii danych
25.	uszkodzenia powodowane przez burze (pioruny)	3	5	15	zapewnienie ochrony przepięciowej, zastosowanie światłowodów przy dłuższych połączeniach w celu wyeliminowania zjawiska indukcji
26.	utrata danych z lokalnych dysków	2	5	10	zapewnienie tworzenia codziennych kopii danych z lokalnych dysków, przeniesienie danych lokalnych do serwera (moje dokumenty, pulpit)
27.	awarie dysków serwera	2	5	10	stosowanie macierzy dyskowej, monitorowanie działania macierzy, natychmiastowa wymiana uszkodzonych dysków
28.	używanie zbyt prostych haseł	3	4	12	wdrożenie mechanizmów wymuszających złożoność haseł i ich okresowej wymiany
29.	pożar	3	4	12	wdrożenie mechanizmów wymuszających złożoność haseł i ich okresowej wymiany
30.	zalanie	3	4	12	wdrożenie mechanizmów wymuszających złożoność haseł i ich okresowej wymiany

skala: prawdopodobieństwo 1-5, skutek 1-5

prawd. / skutek	**1**	**2**	**3**	**4**	**5**
1	1	2	3	4	5

2	2	3	6	8	10
3	3	6	9	12	15
4	4	8	12	16	20
5	5	10	15	20	25

ryzyko akceptowalne

ryzyko nieakceptowalne

Załącznik Nr 2
do Zarządzenia Nr 5.2015
Dyrektor Miejsko - Gminnego Zespołu
Oświaty
z dnia 09.09.2015 r.

Instrukcja zarządzania systemem informatycznym

Historia Zmian dokumentu:

Data	*Wersja*	*Osoba*	*opis*
04.058.2008		Ewa Pręt	Utworzenie dokumentu
		Ewa Pręt	Aktualizacja

§ 1. Podstawa prawna

Na podstawie § 3 i 5 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024).

§ 2. Postanowienia ogólne

1. Ilekroć mowa w niniejszym dokumencie o Instrukcji, należy przez to rozumieć „Instrukcję zarządzania systemem informatycznym".
2. Ilekroć mowa w niniejszym dokumencie o MGZO należy przez to rozumieć Miejsko - Gminny Zespół Oświaty w Drezdenku.
3. Ilekroć mowa w niniejszym dokumencie o ABI należy przez to rozumieć Administratora Bezpieczeństwa Informacji.
4. Ilekroć mowa w niniejszym dokumencie o ASI należy przez to rozumieć Administratora Systemu Informatycznego. Przy czym funkcję ASI, mogą pełnić osoby z firm zewnętrznych, które w ramach outsourcingu świadczą takie usługi na podstawie stosownej umowy.

§ 3. Zagadnienia organizacyjne

1. Pracownicy upoważnieni do przetwarzania danych osobowych w systemie informatycznym, zobowiązani są do zapoznania się z treścią Instrukcji i jej przestrzegania.
2. Fakt zapoznania się z Instrukcją pracownik potwierdza własnoręcznym podpisem

§ 4. Wykaz zbiorów danych osobowych

Lp	Zbiór danych	Poziom bezp.	metoda dostępu	Systemy informatyczny	Lokalizacja fizyczna, pomieszczenia w którym są przetwarzane dane	Rejestra-cja w GIODO	Dane osobowe
1	System Qwant – System księgowy	Wysoki	LAN	Qwant	Budynek Miejsko – Gminnego Zespołu Oświaty, pomieszczenia: Księgowość, Kasa	N	Imię nazwisko, adres (ulica, nr domu, miasto), nr rachunku bankowego, NIP
2	System Qwark – System płacowy	Wysoki	LAN	Qwark	Budynek Miejsko – Gminnego Zespołu Oświaty, pomieszczenia: Płace	T	Imię nazwisko, adres pracownika (ulica, nr domu, miasto), data urodzenia, nr rachunku bankowego, NIP, PESEL, nr tel., nr dowodu osobistego, nazwisko rodowe, imiona rodziców,
3	System Płatnik	Wysoki	LAN	Płatnik	Budynek Miejsko – Gminnego Zespołu Oświaty, pomieszczenia: Płace	T	Imię nazwisko, adres pracownika (ulica, nr domu, miasto), data urodzenia, NIP, PESEL, nr dowodu osobistego, nazwisko rodowe, imię i nazwisko członka rodziny
4	System SIO – system informacji oświatowej	Wysoki	bezpośredni	SIO	Budynek Miejsko – Gminnego Zespołu Oświaty, pomieszczenia: Dyrektor, Sekretariat	T	imię i nazwisko użytkownika
5	System SJO Besti@	Wysoki	bezpośredni	SJO Besti@	Budynek Miejsko – Gminnego Zespołu Oświaty, pomieszczenia: Księgowość	N	imię i nazwisko użytkownika
6	System sQola – Integra - FK	Wysoki	LAN	sQola – Integra	Budynek Miejsko – Gminnego Zespołu Oświaty, pomieszczenia: Księgowość, Kasa	N	Imię nazwisko, adres (ulica, nr domu, miasto), nr rachunku bankowego, NIP

7	System sQola – Integra – Płace	Wysoki	LAN	sQola – Integra	Budynek Miejsko – Gminnego Zespołu Oświaty, pomieszczenia: Płace, Księgowość	T	Imię nazwisko, adres pracownika (ulica, nr domu, miasto), data urodzenia, nr rachunku bankowego, NIP, PESEL, nr tel., nr dowodu osobistego, nazwisko rodowe, imiona rodziców,
8	Przelewy 2001, Klient Home Bankong	Wysoki	bezpośredni	Przelewy 2001	Budynek Miejsko – Gminnego Zespołu Oświaty, pomieszczenia: Kasa	T	Imię nazwisko użytkownika
9	Kasa ZP	Wysoki	LAN	sQola – Integra	Budynek Miejsko – Gminnego Zespołu Oświaty, pomieszczenia: Księgowość, Kasa, Sekretariat	T	Imię nazwisko, adres (ulica, nr domu, miasto), data urodzenia, nr rachunku bankowego, NIP, PESEL, nr te., nr dowodu osobistego, nazwisko rodowe, imiona rodziców.
10	System sQola – Integra – Kadry	Wysoki	LAN	sQola – Integra	Budynek Miejsko – Gminnego Zespołu Oświaty, pomieszczenia: Sekretariat, Płace	T	Imię nazwisko, adres (ulica, nr domu, miasto), data urodzenia, nr rachunku bankowego, NIP, PESEL, nr te., nr dowodu osobistego, nazwisko rodowe, imiona rodziców.
11	Przetargi	Wysoki	bezpośredni	Forum Media Polska	Budynek Miejsko – Gminnego Zespołu Oświaty, pomieszczenia: Kasa	T	Imię nazwisko, adres (ulica, nr domu, miasto), nazwa firmy, NIP,
12	Pomoc materialna dla uczniów	Wysoki	Bezpośredni oraz LAN	Sputnik Software	Budynek Miejsko – Gminnego Zespołu Oświaty, pomieszczenia: Stypendia	T	Imię nazwisko, adres (ulica, nr domu, miasto), data urodzenia, nr rachunku bankowego, NIP, PESEL, nr te., nr dowodu osobistego, nazwisko rodowe, imiona rodziców.
13	System sQola – Integra – QDeklaracje	Wysoki	LAN	sQola – Integra	Budynek Miejsko – Gminnego Zespołu Oświaty, pomieszczenia: Płace	T	Imię nazwisko, adres (ulica, nr domu, miasto), data urodzenia, PESEL, przychody

§ 5. Zasady pracy w systemach informatycznych.

1) Dostęp do systemu informatycznego jest możliwy po uwierzytelnieniu użytkownika
2) Zabroniony jest dostęp do systemów informatycznych osób trzecich.
3) Zabronione jest udostępnianie hasła osobom trzecim
4) Dostęp do sieci LAN mają tylko komputery będące aktywami organizacji. Za bezpieczeństwo fizyczne stacji roboczej odpowiada jej operator.
5) Serwery powinny mieć dodatkowe zabezpieczenie przed dostępem fizycznym do nich. Przykładowo może to być szafa teleinformatyczne zamykana na klucz.

§ 6. Sposób, miejsce i okres przechowywania nośników danych:

1. Elektroniczne nośniki informacji zawierających dane osobowe przechowywane są w zamykanych metalowych szafach.. Niezwłocznie po ustaniu ich przydatności informacje są usuwane z nośników lub, gdy jest to niemożliwe są niszczone razem z nośnikiem.

§ 7. Sposób, miejsce i okres przechowywania kopii zapasowych:

1. Nośnikiem kopii zapasowych danych jest nagrywalna płyta optyczna CD/DVD
2. Kopie danych tworzone są codziennie automatycznie i przechowywane na dysku w określonym katalogu. Plik kopii zawiera w swej nazwie datę i godzinę powstania. W ten sposób przechowywane są kopie z co najmniej ostatnich 2 miesięcy.
3. Na oddzielnym dysku jest przechowywana kopia całego systemu wraz ze wszystkimi programami serwera. Kopia jest tworzona automatycznie codziennie.

§ 8. Sposób zabezpieczenia systemu informatycznego przed działalnością złośliwego oprogramowania którego celem może być uzyskanie nieuprawnionego dostępu do systemu informatycznego.

1. Na każdej stacji roboczej zainstalowany jest i aktualizowany na bieżąco system antywirusowy Kaspersky
2. Systemy operacyjne komputerów są aktualizowane na bieżąco, bądź przez ustawienie automatycznych aktualizacji lub pozostawienie użytkownikowi wyboru kiedy taka aktualizacja (bez zbędnej zwłoki) ma się odbyć:

na styku z siecią publiczną stosuje się firewall.

§ 9. Sposób realizacji wymogów, o których mowa w § 7 ust. 1 pkt 4 rozporządzenia

System informatyczny, który przetwarza dane osobowe i udostępnia dane odbiorcom powinien zapewnić odnotowanie komu, kiedy i jakie dane i w jakim zakresie zostały udostępnione. Obowiązkiem użytkownika jest postąpić w takiej sytuacji zgodnie z instrukcją obsługi danego systemu informatycznego przy udostępnianiu takich danych.

System informatyczny posiada funkcjonalność zapewniającą ta czynność. W przypadku gdy system informatyczny nie posiada takiej możliwości należy, poprzez kontakt z producentem systemu, doprowadzić do zgodności z w/w rozporządzeniem.

§ 10. Procedury:

1) Procedura nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności.
2) Metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem.
3) Procedura rozpoczęcia pracy systemu informatycznego przeznaczona dla użytkowników systemu.
4) Procedura zawieszenia pracy systemu informatycznego przeznaczona dla użytkowników systemu.
5) Procedura zakończenia pracy systemu informatycznego przeznaczona dla użytkowników systemu.
6) Procedura tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania.
7) Procedura likwidacji nośników zawierających kopie zapasowe danych po ich wycofaniu na skutek utraty przydatności lub uszkodzenia.
8) Procedura postępowania użytkownika na okoliczność zidentyfikowania określonego typu zagrożeń przez program antywirusowy Kaspersky.
9) Procedura wykonywania przeglądów i konserwacji systemów.
10) Procedura wykonywania przeglądów i konserwacji nośników informacji służących do przetwarzania danych.
11) Procedura postępowania w sytuacji naruszenia ochrony danych osobowych.

Procedura nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności	
numer procedury: 1	
dotyczy:	wszystkich użytkowników systemów informatycznych
osoby odpowiedzialne:	Administrator Danych Osobowych

1. Rejestrowanie użytkownika i nadawanie uprawnień przeprowadza osobiście ASI, na podstawie upoważnienia do przetwarzania danych osobowych.
2. Rejestrowanie użytkownika i nadawanie uprawnień wprowadza się zgodnie z procedurami obsługi danego systemu informatycznego w zakresie niezbędnym do realizacji obowiązków służbowych.
3. Hasła użytkowników uprzywilejowanych (administratora) przechowywane są we wskazanym miejscu przez Dyrektora Jednostki w kopertach oddzielnie.
4. Użytkowników uprzywilejowanych rejestruje w systemie informatycznym dostawca oprogramowania, chyba że użytkownik uprzywilejowany jest kontem wbudowanym w systemie (admin, administrator).
5. Użytkownikiem uprawnionym do korzystania z kont administracyjnych jest Administrator Danych Osobowych.
6. W przypadku nieobecności Administratora Danych Osobowych , w razie konieczności, ABI lub ASI może użyć hasła do konta administracyjnego.

Metody i środki uwierzytelnienia oraz procedura związana z ich zarządzaniem i użytkowaniem	
numer procedury: 2	
dotyczy:	wszystkich użytkowników systemów informatycznych
osoby odpowiedzialne:	wszyscy użytkownicy systemów informatycznych

1. W systemie, służącym do przetwarzania danych osobowych, stosowane jest uwierzytelnianie użytkownika przy pomocy jego identyfikatora i hasła.
2. Użytkowników systemu obowiązuje następująca polityka haseł:
    a) minimalna długość hasła wynosi 8 (osiem) znaków,
    b) zmiana hasła nie rzadziej niż co 30 dni,
    c) hasło zawiera małe i wielkie litery oraz cyfry lub znaki specjalne.
3. Nazwa użytkownika (login) jest przydzielana pracownikowi odgórnie podczas upoważnienia pracownika do przetwarzania danych osobowych. Login składa się z liter lub liter i cyfr i kojarzy się z imieniem i nazwiskiem użytkownika
4. Użytkownik chroni hasło przed osobami postronnymi
5. Każdy użytkownik zarządza swoimi hasłami oraz utrzymuje hasła w tajemnicy.
6. System informatyczny winien pamiętać historię ostatnich haseł by nie pozwolić na użytkowanie tego samego hasła cały czas.
7. Hasła w systemie informatycznym powinny być przechowywane w postaci zaszyfrowanej.
8. ASI nadaje pierwszy raz hasło oraz zaznajamia użytkownika z obsługą mechanizmu uwierzytelniania oraz zmiany hasła.
9. Pierwsze hasło przekazywane jest użytkownikowi ustnie.
10. Użytkownik po otrzymaniu hasła jest zobowiązany do niezwłocznej jego zmiany, chyba, że system nie umożliwia wykonania takiej operacji.

Procedura rozpoczęcia pracy systemu informatycznego przeznaczona dla użytkowników systemu	
numer procedury: 3	
dotyczy:	wszystkich użytkowników systemów informatycznych
osoby odpowiedzialne:	wszyscy użytkownicy systemów informatycznych

1. Przed przystąpieniem do pracy należy sprawdzić stanowisko pracy.
2. Włączyć komputer.
3. Dokonać uwierzytelnienia zgodnie z monitem systemu operacyjnego komputera.
4. Bezwzględnie należy zapewnić zachowanie poufności podczas wprowadzania hasła.
5. Po uruchomieniu sytemu operacyjnego można rozpocząć pracę na programie użytkowym.
6. W razie problemów związanych z uruchamianiem systemu lub uwierzytelnianiem, lub stwierdzeniem fizycznej ingerencji w przetwarzane dane, należy się skontaktować z ASI.

Procedura zawieszenia pracy systemu informatycznego przeznaczona dla użytkowników systemu	
numer procedury: 4	
dotyczy:	wszystkich użytkowników systemów informatycznych
osoby odpowiedzialne:	wszyscy użytkownicy systemów informatycznych

1. Podczas nawet chwilowego opuszczenia stanowiska pracy należy zablokować możliwość wglądu do przetwarzanych danych przez osoby postronne poprzez zablokowanie stacji używając klawiszy **[Windows] + L** lub wylogowanie użytkownika z aplikacji / systemu operacyjnego.
2. Na czas dłuższej nieobecności zalecane jest wyłączenie stanowiska komputerowego.

Procedura zakończenia pracy systemu informatycznego przeznaczona dla użytkowników systemu	
numer procedury: 5	
dotyczy:	wszystkich użytkowników systemów informatycznych
osoby odpowiedzialne:	wszyscy użytkownicy systemów informatycznych

1. Wyrejestrować się z aplikacji użytkowej używając do tego odpowiedniej opcji.
2. Dokonać zamknięcia sytemu operacyjnego odpowiednią funkcją.
3. Odczekać aż system operacyjny zostanie wyłączony.
4. W razie problemów związanych z zamykaniem systemu informatycznego należy się skontaktować z ASI.

Procedura tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania	
numer procedury: 6	
dotyczy:	ASI
osoby odpowiedzialne:	ASI

1. Konfiguracja programów użytkowych powinna zapewniać przechowywanie zbiorów danych na wydzielonym zasobie serwera.
2. Serwer zapewniają automatyczną całościową archiwizację danych w cyklu codziennym lub z odstępem parudniowym w zależności od częstości wprowadzania danych.
3. Czasookres przechowywania kopii zapasowych na zasobach pamięci dyskowej wynosi nie mniej niż pół roku.
4. Każda kopia jest zachowywana z odnotowaniem daty i godziny powstania jako części jej nazwy
5. Do utworzenia kopii używane są narzędzia przewidziane w serwerach baz danych (Sybase, SQL Serwer) oraz program WinRAR.
6. Nad poprawnością funkcjonowania systemu archiwizacji czuwa ASI
7. Kopie awaryjne tworzone doraźnie należy usuwać bezzwłocznie po ustaniu ich użyteczności.

Procedura likwidacji nośników zawierających kopie zapasowe danych po ich wycofaniu na skutek utraty przydatności lub uszkodzenia	
numer procedury: 7	
dotyczy:	wszystkich użytkowników systemów informatycznych
osoby odpowiedzialne:	ASI

1. Celem likwidacji nośnika jest doprowadzenie do takiego fizycznego uszkodzenia, że niemożliwe jest odczytanie jakiegokolwiek nawet jego fragmentu.
2. Nośniki przeznaczone do likwidacji należy przekazać do ASI
3. Dane z nośników należy przed likwidacją usunąć, np. programem ERASER (http://eraser.heidi.ie)
4. Jeśli jest to niemożliwe, należy postąpić zgodnie z następnymi punktami procedury
5. **Dyskietki**. Należy wydobyć nośnik z obudowy dyskietki. Nożyczkami wykonać kilkanaście cięć mających na celu podzielenie fizyczne powierzchni nośnika.
6. **CDRomy**. Płytę należy zniszczyć w niszczarce dokumentów.
7. **Twarde dyski**. Rozmontować urządzenie w celu odsłonięcia talerzy z zapisem magnetycznym. Używając twardego i ostrego narzędzia zniszczyć powierzchnię dysku poprzez jej zarysowanie kilkudziesięcioma rysami (szczotka druciana). Ewentualnie użyć młotka w celu zniszczenia talerzy magnetycznych. Zastosować tą metodę odpowiednio do ilości talerzy zainstalowanych w napędzie. W przypadku talerzy ceramicznych należy je potłuc.
8. **Pendrive**. Użyć młotka w celu uszkodzenia układów pamięci poprzez ich fizyczne zniszczenie.

Procedura postępowania użytkownika na okoliczność zidentyfikowania określonego typu zagrożeń przez program antywirusowy Kaspersky	
numer procedury: 8	
dotyczy:	wszystkich użytkowników systemów informatycznych
osoby odpowiedzialne:	wszyscy użytkownicy systemów informatycznych

1. Użytkownik powinien zapoznać się z obsługą systemu antywirusowego dostępną w formie podręcznika pod adresem:
   http://www.kaspersky.pl/download.html?s=docs&prod_id=233
2. Po odebraniu zainfekowanej wiadomości e-mail, wykrycia zagrożenia na nośniku lub zagrożenia pochodzącego ze strony sieci internet system antywirusowy podejmuje działanie usuwając zagrożenie. W przypadku monitu o podjęcie działania zaleca się wybór opcji **Wylecz, Usuń** lub **Rozłącz**.

Procedura wykonywania przeglądów i konserwacji systemów	
numer procedury: 9	
dotyczy:	wszystkich użytkowników systemów informatycznych
osoby odpowiedzialne:	ASI

1. Przeglądu oraz konserwacji systemów informatycznych dokonuje się raz na rok.
2. Przegląd obejmuje sprawdzenie stanu pamięci dyskowej, rejestru komunikatów systemowych (jeśli takie są w systemie operacyjnym komputera), sprawdzenie konfiguracji systemu.
3. Konserwacja obejmuje: czyszczenie z kurzu, sprawdzenie napięć wyjściowych z zasilacza. Ocena stanu systemu chłodzenia, wymianę wadliwych elementów, oraz usunięcie błędów logicznych.
4. Każda usterka jest natychmiast usuwana osobiście przez ASI. Podzespoły lub części nie zawierające danych osobowych mogą być przekazywane do naprawy podmiotom zewnętrznym.
5. W razie niestabilności systemu informatycznego dokonuje się przeglądu doraźnego.

Procedura wykonywania przeglądów i konserwacji nośników informacji służących do przetwarzania danych	
numer procedury: 10	
dotyczy:	wszystkich użytkowników systemów informatycznych
osoby odpowiedzialne:	ASI

.

1. Nośniki informacji służące do przetwarzania danych takie jak twarde dyski, płyty CD oraz dyskietki podlegają przeglądowi polegającemu na ocenie ich stanu technicznego.
2. Twarde dyski sprawdza się programami narzędziowymi do wykrywania błędów i usterek. W razie braku możliwości naprawy błędu dysk podlega formatowaniu. Przy błędach pozostałych dysk czyści się zapisując z weryfikacją wszystkie sektory dysku. Jeśli błędy pozostają dysk uznaje się jako niesprawny i przeznacza do zniszczenia.
3. Płyty CD niezdatne do użytku (wykazujące błędy) przeznacza się do zniszczenia.
4. Dyskietki poddaje się procesowi formatowania. Błędy po formatowaniu dyskwalifikują nośnik do dalszego użytku, podlega on zniszczeniu.
5. Zniszczenie nośnika określa procedura likwidacji nośników zawierających dane osobowe.

Procedura postępowania w sytuacji naruszenia ochrony danych osobowych w systemach informatycznych	
numer procedury: 11	
dotyczy:	wszystkich użytkowników systemów informatycznych
osoby odpowiedzialne:	ASI

1. W przypadku stwierdzenia naruszenia ochrony danych osobowych na co może wskazywać: stan urządzeń, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej należy niezwłocznie powiadomić Administratora Danych Osobowych oraz Administratora Systemu Informatycznego.
2. ASI dokonuje niezwłocznie zabezpieczenia zbiorów danych osobowych oraz logów systemów operacyjnych komputerów celem analizy.
3. ASI dokona sprawdzenia czy naruszenie miało faktycznie miejsce na podstawie zebranych dowodów oraz wyjaśnień.
4. Na podstawie sporządzonego przez ASI ustaleń Administrator Danych podejmuje odpowiednie decyzje.