Polityka Bezpieczeństwa oraz Instrukcja Bezpieczeństwa danych osobowych w Lokalnej Grupie Działania Równiny Wołomińskiej

W celu zapewnienia ochrony przetwarzanych danych osobowych, administrator danych osobowych LGD, które na gruncie **rozporządzenia Parlamentu Europejskiego i Rady Unii Europejskiej 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (RODO)** i ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2018 poz. 1000), mają charakter danych osobowych wprowadza poniższą Politykę bezpieczeństwa.

§ 1
Cel i zakres regulacji

1. Celem Polityka Bezpieczeństwa ochrony danych osobowych jest określenie obowiązków i zasad postępowania w **Lokalnej Grupie Działania Równiny Wołomińskiej z siedzibą w ul. Przemysłowa 70, 05-240 Tłuszcz (dalej „LGD")** w przypadku zagrożenia bezpieczeństwa danych osobowych administrowanych przez LGD. Poprzez bezpieczeństwo należy rozumieć stan faktyczny uniemożliwiający wykorzystanie, przepływ, modyfikację lub zniszczenie informacji uzyskanych w bieżącej działalności LGD. Dokument szczegółowo opisuje podstawowe zasady organizacji pracy przy zbiorach osobowych przetwarzanych metodami tradycyjnymi oraz w systemie informatycznym wyrażone w niniejszej Polityce.
2. Niniejszy dokument powstał w oparciu o rozporządzenie Parlamentu Europejskiego i Rady Unii Europejskiej 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (RODO oraz ustawę z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2018 poz. 1000), które zobowiązują Administratora Danych osobowych do wykonania dokumentacji opisującej środki organizacyjne i techniczne służące ochronie przetwarzanych danych osobowych.
3. Przetwarzanie danych osobowych jest dopuszczalne wyłącznie pod warunkiem przestrzegania przepisów ustawy o ochronie danych osobowych i wydanych na jej podstawie przepisów wykonawczych w tym niniejszej polityki i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, które powinny być spójne z polityką bezpieczeństwa informacji wymaganą przez ustawę o informatyzacji działalności podmiotów realizujących zadania publiczne.
4. Polityka Bezpieczeństwa ma zastosowanie do ochrony zbiorów danych osobowych przetwarzanych w spółce w celu ich bezpiecznego wykorzystania oraz określa zasady korzystania z systemów informatycznych.

§ 2
Stosowana terminologia

Określenia użyte w Polityce Bezpieczeństwa oznaczają:
1. Administrator Danych Osobowych (ADO) – organ, jednostka organizacyjna, podmiot lub osoba decydująca o celach i środkach przetwarzania danych osobowych; Zarząd LGD, zwany dalej „ADO". Z Administratorem można się kontaktować pisemnie, za pomocą poczty tradycyjnej na adres: Lokalna Grupa Działania Równiny Wołomińskiej z siedzibą w ul. Przemysłowa 70, 05-240 Tłuszcz pod adresem mailowym: biuro@lgdrw.pl

2. **Inspektor Ochrony Danych (IOD)** - osoba wyznaczona przez ADO, odpowiedzialna za bezpieczeństwo danych osobowych przetwarzanych w systemach informatycznych. Z Inspektorem Ochrony Danych można kontaktować się pisemnie, za pomocą poczty tradycyjnej na adres: Lokalna Grupa Działania Równiny Wołomińskiej z siedzibą w ul. Przemysłowa 70, 05-240 Tłuszcz pod adresem mailowym: biuro@lgdrw.pl
3. **Dokumentacja przetwarzania danych** – dokumentacja opisująca sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną.
4. **Integralność danych** – właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany.
5. **Osoba upoważniona** lub **użytkownik systemu** – osobę posiadającą upoważnienie wydane przez ADO lub IOD do przetwarzania danych osobowych w systemie informatycznym danej komórki organizacyjnej w zakresie wskazanym w upoważnieniu, zwaną dalej „użytkownikiem”;
6. **Osoby zatrudnione przy przetwarzaniu danych osobowych** – wszystkie osoby, w tym użytkowników systemu informatycznego, mające dostęp do danych osobowych.
7. **Poufność danych** – właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom.
8. **Rozliczalność** - właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi
9. **RODO** lub **rozporządzenie ogólne** - rozporządzenia Parlamentu Europejskiego i Rady Unii Europejskiej 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE
10. **LGD** – Lokalna Grupa Działania Równiny Wołomińskiej
11. **System informatyczny** - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
12. **Uwierzytelnianie** – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu

§ 3
Rejestr czynności

1. Na podstawie art. 30 ust. 1 RODO tworzy się Rejestr czynności przetwarzania danych osobowych, za które odpowiada ADO oraz w związku z przetwarzaniem danych które nie ma charakteru sporadycznego, tworzy się Rejestr czynności przetwarzania danych osobowych. Rejestr obejmuje:

1) imię i nazwisko lub nazwa oraz dane kontaktowe administratora oraz wszelkich współadministratorów, a także gdy ma to zastosowanie – przedstawiciela administratora oraz inspektora ochrony danych;
2) cele przetwarzania;
3) opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;
4) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych;
5) gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi, dokumentacja odpowiednich zabezpieczeń;

6) jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;
7) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1.

2. Dane osobowe są przetwarzane na podstawie art. 6 ust. 1 lit. f RODO, tj. w oparciu o niezbędność przetwarzania do celów wynikających z prawnie uzasadnionych interesów realizowanych przez Administratora lub przez stronę trzecią.
2. LGD nie przetwarza szczególnych kategorii danych osobowych ani danych osobowych dotyczących wyroków skazujących oraz naruszeń prawa lub powiązanych środków bezpieczeństwa.
3. LGD nie przekazuje danych osobowych do państwa trzeciego (poza UE/EOG),
4. Z uwagi na połączenie komputerów z siecią Internet, dla zbiorów przetwarzanych elektronicznie stosuje się, zgodnie z § 6 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. środki bezpieczeństwa na poziomie WYSOKIM.
5. W związku z przetwarzaniem danych osobowych osobie której dane są przetwarzane przysługuje prawo do:

- żądania od Administratora dostępu do swoich danych osobowych,
- żądania od Administratora sprostowania swoich danych osobowych,
- żądania od Administratora usunięcia swoich danych osobowych,
- żądania od Administratora ograniczenia swoich przetwarzania danych osobowych,
- wniesienia sprzeciwu wobec przetwarzania swoich danych osobowych,
- przenoszenia swoich danych osobowych,
- wniesienia skargi do organu nadzorczego.

Z praw wskazanych powyżej można skorzystać poprzez kontakt e-mailowy pod adresem biuro@lgdrw.pl lub kontakt pisemny, za pomocą poczty tradycyjnej na adres: Lokalna Grupa Działania Równiny Wołomińskiej z siedzibą w ul. Przemysłowa 70, 05-240 Tłuszcz.

§ 4
Wykaz osób upoważnionych do przetwarzania danych osobowych

1. Wprowadza się ewidencję osób upoważnionych do przetwarzania danych, która stanowi załącznik nr 2, **Wykaz osób upoważnionych przetwarzania danych osobowych.**
2. Wykaz zawiera: imię i nazwisko osoby upoważnionej, datę nadania i ustania uprawnień oraz zakres, a w przypadku kiedy dane są przetwarzane za pomocą programu komputerowego również identyfikator dostępowy do tego programu.
3. Ewidencja stanowi podstawę wydania Upoważnienia do przetwarzania danych osobowych. Upoważnienie wydaje ADO lub działający z jego upoważnienia IOD.

§ 5
Okres przetwarzania danych osobowych

Dane osobowe przetwarzane są do czasu istnienia podstawy do ich przetwarzania:

- w przypadku przetwarzania danych w celu realizacji Umowy (np. zrealizowania zamówienia) – przez okres realizowania Umowy (realizowania zamówienia),
- w przypadku przetwarzania danych dla realizacji naszych uzasadnionych interesów – do czasu istnienia tego uzasadnionego interesu,

— w przypadku przetwarzania danych na podstawie zgody osoby – do momentu jej cofnięcia.

§ 6
Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe

1. Na podstawie § 4 pkt 1 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 tworzy się wykaz pomieszczeń tworzących obszar fizyczny przetwarzania danych. Wyznaczają go pomieszczenia zlokalizowane w **siedzibie LGD**.
2. Obszar, w którym przetwarzane są dane osobowe obejmuje pomieszczenia biurowe w biurze LGD. W tych pomieszczeniach przechowywane są segregatory, które zawierają dane osobowe, zabezpieczone poprzez umieszczenie tych segregatorów w szafie zamykanej na klucz. W pomieszczeniach znajdują się trzy komputery przenośne – wszystkie połączone siecią, posiadające dostęp do Internetu i służą do przetwarzania danych osobowych administratora danych. Komputery są własnością administratora danych, posiadają dostęp do Internetu.
3. Szczegółowy wykaz pomieszczeń, stanowi załącznik nr 3**. Wykaz miejsc przetwarzania danych osobowych.** Pomieszczenia zabezpieczone są przed dostępem osób trzecich.

§ 7
Administrator Danych Osobowych (ADO)

ADO jest Zarząd LGD. ADO dokonuje powołania Inspektora Ochrony Danych (IOD).

§ 8
Obowiązki IOD

Do zadań IOD należy zapewnianie przestrzegania przepisów o ochronie danych osobowych, w szczególności przez:

1) Dokonanie przeglądu obecnego zasobu danych osobowych w celu przeprowadzenia nowych dokumentów i określenia środków technicznych spełniających wymagania RODO i IOD.
2) Przeszkolenie pracowników w zakresie nowych przepisów.
3) Przeprowadzenie oceny skutków planowanych operacji przetwarzania danych przed rozpoczęciem ich przetwarzania (analiza ryzyka - art. 35 RODO).
4) Monitorowanie przestrzegania przepisów ochrony danych osobowych w jednostce oraz pełnienie funkcji doradczych w tym zakresie.
5) Prowadzenie rejestru czynności przetwarzania ochrony danych osobowych (art. 31 RODO)
6) Zgłaszania naruszenia ochrony danych osobowych do organu nadzorczego oraz zawiadamianie o tym osób, których dane te dotyczą (art. 33 i 34 RODO).
7) Pełnienie funkcji punktu kontaktowego dla organu nadzorczego, dla właścicieli danych osobowych oraz współdziałanie z organem nadzorczym.
8) Zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności do zabezpieczenia danych przed ich udostępnieniem osobom

nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą i uszkodzeniem.

9) Prowadzenia dokumentacji opisującej sposób przetwarzania danych oraz zastosowane środki ochrony.
10) Zapewnienia kontroli, jakie dane osobowe, kiedy i przez kogo zostały wprowadzone do zbioru oraz komu są przekazywane.
11) Prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych.
12) Prowadzenie okresowych szkoleń dla osób upoważnionych do przetwarzania danych osobowych
13) Dokonywanie sprawdzania czyli czynności mających na celu zweryfikowanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych

§ 10

Zarządzanie przetwarzaniem danych osobowych oraz czuwanie nad ich bezpieczeństwem

IOD zobowiązany jest do zbierania, ewidencjonowania i przechowywania:

— oświadczeń osób przetwarzających dane osobowe o zachowaniu w tajemnicy danych, z którymi mają styczność, oraz środkach bezpieczeństwa stosowanych przy przetwarzaniu danych osobowych
— oświadczeń osób zatrudnianych na podstawie umowy zlecenia, umowy o dzieło lub innej umowy cywilnej o zachowaniu tajemnicy
— porozumień zawartych z osobami zatrudnionymi przy przetwarzaniu danych osobowych w zakresie wykorzystania oddanego im do dyspozycji sprzętu informatycznego, oprogramowania oraz zasobów sieci informatycznej

§ 11

Umowa o przetwarzaniu danych osobowych

1. Dopuszcza przepływ danych pomiędzy systemami, zgodnie z zapisami umowy o powierzeniu i przetwarzaniu danych.
2. Powierzanie przetwarzania danych osobowych odbywa się zgodnie przepisami RODO na podstawie umowy zawartej na piśmie pomiędzy ADO, a danym podmiotem, któremu zleca się czynności związane z przetwarzaniem danych osobowych. Właściciel zasobów danych osobowych informuje IOD o zamiarze powierzenia danych osobowych do przetwarzania. Właściciel zasobów danych osobowych przygotowuje projekt umowy powierzenia danych osobowych innemu podmiotowi. W projekcie umowy należy wyspecyfikować zakres czynności związanych z przetwarzaniem powierzonych danych osobowych, zakres danych oraz wymagania dotyczące ochrony danych.
3. Każda osoba delegowana do wykonywania zadań na rzecz LGD związanych z powierzeniem przetwarzania danych osobowych zobowiązana jest podpisać oświadczenie o zachowaniu tajemnicy danych osobowych oraz sposobów ich zabezpieczania. Oświadczenie podpisuje IOD.

§ 12
Ochrona danych przez podmiot przetwarzający dane osobowe

Podmiot przetwarzający dane osobowe jest zobowiązany do zastosowania środków organizacyjnych i technicznych, zabezpieczających zbiór przed dostępem osób nieupoważnionych na zasadach określonych w przepisach o ochronie danych osobowych. Podmiot przetwarzający dane osobowe ponosi odpowiedzialność za ochronę przetwarzanych danych osobowych, i jest zobowiązany przetwarzać dane osobowe wyłącznie w zakresie określonym w umowie.

§ 13
Środki organizacyjne ochrony danych osobowych

1. W celu stworzenia właściwych zabezpieczeń, które powinny bezpośrednio oddziaływać na procesy przetwarzania danych, przetwarzanie danych osobowych w spółce może odbywać się wyłącznie w ramach wykonywania zadań służbowych. Zakres uprawnień wynika z zakresu tych zadań.
2. Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające stosowne upoważnienie. Wzór upoważnienia stanowi załącznik nr 4, **Upoważnienie do przetwarzania danych osobowych.**
3. IOD prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych oraz na jej podstawie przygotowuje Upoważnienia do przetwarzania danych osobowych. Osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych.
4. Zabrania się przetwarzania danych poza obszarem określonym w Wykazie miejsc przetwarzania danych osobowych. Osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy.
5. Każdy osoba upoważniona do przetwarzania danych osobowych obowiązana co najmniej raz na 2 lata musi odbyć szkolenie z zakresu ochrony danych osobowych. **Za organizację szkoleń odpowiedzialny jest IOD, który prowadzi w tym celu odpowiednią dokumentację**. Nowo przyjęty pracownik LGD (osoba zatrudniona na umowę cywilno-prawną) odbywa szkolenie przed przystąpieniem do przetwarzania danych. Ponadto każdy upoważniony do przetwarzania danych potwierdza pisemnie fakt zapoznania się z niniejszą dokumentacją i zrozumieniem wszystkich zasad bezpieczeństwa. Wzór potwierdzenia stanowi załącznik nr 5, **Oświadczenie upoważnionego do przetwarzania danych osobowych**. Podpisany dokument jest dołączany do akt osobowych.
6. Obszar przetwarzania danych osobowych określony w Wykazie miejsc przetwarzania danych osobowych, zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych. Przebywanie osób nieuprawnionych w w/w obszarze jest dopuszczalne za zgodą IOD lub w obecności osoby upoważnionej do przetwarzania danych osobowych.
7. Pomieszczenia stanowiące obszar przetwarzania danych powinny być zamykane na klucz. Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane.

§ 13
Środki techniczne ochrony danych osobowych

Zbiory danych zabezpiecza się poprzez poniższe środki ochrony fizycznej:

— Pomieszczenia, w których przetwarzane są zbiory danych osobowych zabezpieczone są przed skutkami pożaru za pomocą systemu przeciwpożarowego;
— zbiory danych osobowych przechowywane są w pomieszczeniach zabezpieczonych drzwiami zwykłymi, zamykanymi na klucz;
— zbiory danych osobowych w formie papierowej przechowywane są w zamkniętych niemetalowych szafach, znajdujących się w pomieszczeniach zamykanych na klucz.
— Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.

§ 14
Środki sprzętowe, infrastruktury informatycznej i telekomunikacyjnej

Zbiory danych zabezpiecza się poprzez poniższe środki sprzętowe, infrastruktury informatycznej i telekomunikacyjnej:

— Zbiory danych osobowych przetwarzane są przy użyciu komputerów przenośnych.
— Dostęp do zbiorów danych osobowych, które przetwarzane są na wydzielonej stacji komputerowej i komputerze przenośnym zabezpieczony został przed nieautoryzowanym uruchomieniem za pomocą hasła.
— Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
— Zastosowano systemowe mechanizmy wymuszający okresową zmianę haseł.
— Zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity.

§ 15
Środki ochrony w ramach systemowych narzędzi programowych i baz danych

Zbiory danych przetwarzane w spółce zabezpiecza się poprzez środki ochrony w ramach systemowych narzędzi programowych i baz danych:

— Dostęp do zbiorów danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła
— Zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu informatycznego
— Zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do zbiorów danych osobowych.
— Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe.
— Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.

§ 16

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

1. Użytkowników systemu informatycznego tworzy oraz usuwa IOD.
2. Do przetwarzania danych osobowych zgromadzonych w systemie informatycznym jak również w rejestrach tradycyjnych wymagane jest upoważnienie.
3. Uprawnienia do pracy w systemie informatycznym odbierane są czasowo, poprzez zablokowanie konta w przypadku nieobecności pracownika w pracy trwającej dłużej niż 21 dni kalendarzowych lub zawieszenia w pełnieniu obowiązków służbowych.
4. Uprawnienia do przetwarzania danych osobowych odbierane są trwale w przypadku ustania stosunku pracy.
5. Osoby, które zostały upoważnione do przetwarzania danych, są obowiązane zachować w tajemnicy te dane osobowe oraz sposoby ich zabezpieczenia nawet w przypadku ustania stosunku pracy.

§ 17
Zasady korzystania z Internetu

1. Użytkownik zobowiązany jest do korzystania z Internetu wyłącznie w celach służbowych.
2. Zabrania się zgrywania na dysk twardy komputera oraz uruchamia jakichkolwiek programów nielegalnych oraz plików pobranych z niewiadomego źródła. Pliki takie powinny być ściągane tylko za każdorazową zgodą IOD i tylko w uzasadnionych przypadkach.
3. Użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie ściągnięte z Internetu i przez niego zainstalowane.
4. Zabrania się wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, hakerskim, pornograficznym, lub innym zakazanym przez prawo (na większości stron tego typu jest zainstalowane szkodliwe oprogramowanie, infekujące w sposób automatyczny system operacyjny komputera szkodliwym oprogramowaniem).
5. Nie należy w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł.
6. W przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, należy zwracać uwagę na pojawienie się odpowiedniej ikonki (kłódka, protokół https).

§ 18
Zasady korzystania z poczty elektronicznej

1. Przesyłanie informacji poza organizację może odbywać się tylko przez osoby do tego upoważnione.
2. Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu.
3. Zaleca się, aby użytkownik podczas przesyłania danych osobowych mailem zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata.
4. Nie należy otwierać załączników (plików) w korespondencji elektronicznej nadesłanej przez nieznanego nadawcę lub podejrzanych załączników nadanych przez znanego nadawcę.
5. Użytkownicy nie powinni rozsyłać za pośrednictwem poczty elektronicznej informacji o zagrożeniach dla systemu informatycznego, „łańcuszków szczęścia" itp.

6. Użytkownicy nie powinni rozsyłać, wiadomości zawierających załączniki o dużym rozmiarze dla większej liczby adresatów - określenie krytycznych rozmiarów przesyłek i krytycznej liczby adresatów jest uzależnione od wydajności systemu poczty elektronicznej.
7. Użytkownicy powinni okresowo kasować niepotrzebne wiadomości pocztowe.

§ 19
Zasady rozpoczęcia, zawieszenia i zakończenia pracy

1. Użytkownik rozpoczyna pracę z systemem informatycznym przetwarzającym dane osobowe z użyciem identyfikatora i hasła.
2. Użytkownik jest zobowiązany do powiadomienia IOD o próbach logowania się do systemu osoby nieupoważnionej, jeśli system to sygnalizuje.
3. W przypadku, gdy użytkownik podczas próby zalogowania się zablokuje system, zobowiązany jest powiadomić o tym IOD, który odpowiada za odblokowanie systemu użytkownikowi.
4. Użytkownik jest zobowiązany do uniemożliwienia osobom niepowołanym wglądu do danych wyświetlanych na monitorach komputerowych – tzw. *polityka czystego ekranu*.
5. Przed czasowym opuszczeniem stanowiska pracy, użytkownik zobowiązany jest wywołać blokowany hasłem wygaszacz ekranu lub wylogować się z systemu. Jeżeli tego nie uczyni – po upływie 20 minut system automatycznie aktywuje wygaszasz ekranu.
6. Po zakończeniu pracy, użytkownik zobowiązany jest wylogować się z systemu informatycznego, a następnie wyłączyć sprzęt komputerowy oraz zabezpieczyć stanowisko pracy, w szczególności wszelką dokumentację oraz nośniki magnetyczne i optyczne, na których znajdują się dane osobowe.

§ 20
Zasady zabezpieczenia dokumentów i wydruków

1. Dokumenty i wydruki trwałe z danymi osobowymi przechowuje się w archiwum lub w zabezpieczonych fizycznie pomieszczeniach, biurkach i szafach.
2. Pracownicy są zobowiązani do zabezpieczania dokumentów (np. zamykanie dokumentów na klucz w szafach, biurkach) przed dostępem osób nieupoważnionych podczas swojej nieobecności w pomieszczeniach lub po zakończeniu pracy tzw. *polityka czystego biurka*.
3. Zabrania się pozostawiania wydruków oraz ksero na drukarkach, skanerach i kserokopiarkach bez nadzoru.
4. Pracownicy są zobowiązani do niszczenia dokumentów i tymczasowych wydruków w niszczarkach niezwłocznie po ustaniu celu ich przetwarzania.

§ 21
Zasady wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych

1. Przeglądy i konserwacje systemu oraz nośników informacji służących do przetwarzania danych mogą być wykonywane jedynie przez osoby posiadające upoważnienie wydane przez IOD.
2. Wszelkie prace związane z naprawami i konserwacją systemu informatycznego przetwarzającego dane osobowe muszą uwzględniać zachowanie wymaganego poziomu zabezpieczenia tych danych

przed dostępem do nich osób nieupoważnionych, w szczególności poprzez bezpośredni nadzór prowadzony przez IOD.
3. W przypadku uszkodzenia zestawu komputerowego, nośniki danych, na których są przechowywane dane osobowe powinny zostać zabezpieczone przez IOD.
4. W przypadku konieczności przeprowadzenia prac serwisowych poza LGD dane osobowe znajdujące się w naprawianym urządzeniu muszą zostać w sposób trwały usunięte.
5. IOD wykonuje okresowy przegląd nośników danych osobowych eliminując te, które nie zapewniają odpowiedniego poziomu bezpieczeństwa oraz niezawodności

§ 22
Postępowanie w przypadkach naruszenia bezpieczeństwa ochrony danych osobowych

1. Przepisy niniejszego paragrafu stosuje się w przypadku stwierdzenia naruszenia zabezpieczenia systemu informatycznego lub dokumentacji prowadzonej w wersji papierowej w obszarze danych osobowych oraz podejrzenia naruszenia bezpieczeństwa danych osobowych ze względu na stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci komputerowej.
2. W przypadku naruszenia zasad ochrony danych osobowych IOD niezwłocznie sporządza raport zgodnie ze wzorem będącym załącznikiem nr 6, **Raport z naruszenia bezpieczeństwa zasad ochrony danych osobowych.**
3. Naruszenia zabezpieczeń systemu informatycznego lub dokumentacji prowadzonej w wersji papierowej, przetwarzających dane osobowe jest każdy stwierdzony fakt nieuprawnionego ujawniania danych osobowych, udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną, uszkodzenia jakiegokolwiek elementu systemu informatycznego, a w szczególności :
   - nieautoryzowany dostęp do danych
   - nieautoryzowane modyfikacje lub zniszczenie danych
   - udostępnianie danych nieautoryzowanym podmiotom,
   - nielegalne ujawnianie danych
   - pozyskiwanie danych z nielegalnych źródeł

4. IOD podejmuje działania mające na celu:
   - minimalizację negatywnych skutków zdarzenia,
   - wyjaśnienie okoliczności zdarzenia,
   - zabezpieczenie dowodów zdarzenia,
   - umożliwienie dalszego bezpiecznego przetwarzania danych.

5. Dla realizacji celów określonych w ust. 1 IOD ma prawo do podejmowania wszelkich działań dopuszczonych przez prawo, w szczególności:
   - żądania wyjaśnień od pracowników,
   - korzystania z pomocy konsultantów,
   - nakazania przerwania pracy, zwłaszcza w zakresie przetwarzania danych osobowych.

6. Odmowa udzielenia wyjaśnień lub współpracy z IOD traktowana będzie jako naruszenie obowiązków pracowniczych.

§ 23
Przepisy końcowe

W sprawach nieuregulowanych w niniejszej Polityce Bezpieczeństwa oraz Instrukcji bezpieczeństwa mają zastosowanie odpowiednie przepisy RODO oraz ustawodawstwa krajowego w przedmiocie ochrony danych osobowych.

Załącznik 1 do Polityki Bezpieczeństwa oraz Instrukcji Bezpieczeństwa danych osobowych w Lokalnej Grupie Działania Równiny Wołomińskiej

REJESTR CZYNNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH

Lp	Nazwa czynności przetwarzania	Jednostka organizacyjna/ organ LGD	Cel przetwarzania	Kategorie osób	Kategorie danych	Podstawa prawna	Źródło danych	Planowany termin usunięcia kategorii danych (jeżeli jest to możliwe)	Nazwa współadministratora i dane kontaktowe (jeśli dotyczy)	Nazwa podmiotu przetwarzającego i dane kontaktowe (jeśli dotyczy)	Kategorie odbiorców (innych niż podmiot przetwarzajacy)	Nazwa systemu lub oprogramowania	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa zgodnie z art. 32 ust. 1 (jeżeli jest to możliwe)	DPIA (jeśli tak, lokalizacja raportu)	Transfer do kraju trzeciego lub organizacji międzynarodowej (nazwa kraju i podmiotu)
	-	-	Art. 30 ust. 1 pkt b RODO	Art. 30 ust. 1 pkt c RODO	Art. 30 ust. 1 pkt c RODO	-	-	Art. 30 ust. 1 pkt f RODO	Art. 30 ust. 1 pkt a RODO	Art. 30 ust. 1 pkt d RODO	Art. 30 ust. 1 pkt d RODO	-	Art.. 30 ust. 1 pkt g RODO		Art. 30 ust. 1 pkt e RODO
1.	Rekrutacja pracownikó w Biura LGD	Biuro LGD	Rekrutacja pracowników	Kandydaci do pracy	Dane identyfikacyjne, dane adresowe, dane o wykształceniu, stażu pracy, uprawnieniach zawodowych, historia zatrudnienia, informacje na temat stanu zdrowia	● Przepis prawa. art. 23 ust. 1 pkt 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, Art. 22 oraz 229 § 7 ustawy z dnia 26 czerwca 1974 r. Kodeks pracy	Kandydaci do pracy	Po zakończeniu procesu rekrutacyjnego	Nie dotyczy	Nie dotyczy	Dane nie są przekazywane innym podmiotom	Akta osobowe (papierowe)	Zamykane szafy w pomieszczeniach zamykanych, dostępnych tylko dla upoważnionych osób. Kontrola dostępu do systemu informatycznego, dostęp tylko dla osób upoważnionych. Środki ochrony w ramach systemowych narzędzi programowych i baz danych	Po przeprowadzeniu oceny ryzyka podjęto decyzję, że ocena skutków dla ochrony danych nie jest wymagana.	Nie dotyczy

2.	Prowadzenie rejestru pracowników, akt pracowniczych i ewidencji czasu ich pracy	Biuro LGD, Zarząd LGD	Prowadzenie ewidencji pracowników zgodnie z Kodeksem Pracy	Pracownic stażyści	Dane identyfikacyjne, dane adresowe, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, PESEL, wykształcenie, przebieg dotychczasowego zatrudnienia, daty urodzenia dzieci, imiona i nazwiska dzieci, stan zdrowia, numer konta bankowego	● Umowa o pracę. ● Przepis prawa. Ustawa z dnia 26 czerwca 1974 r. Kodeks Pracy (Dz. U. z 2018 r., poz. 108 t.j.) - w szczeg. art. 221 w związku z art. 94 pkt 9a i 9b	Pracownik, Stażysta	50 lat [art. 51u ust 1 ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz. U. z 2018 r., poz. 217 t.j.)]	Nie dotyczy	Biuro Księgowe (księgowy)	ZUS, inne firmy ubezpieczeniowe - dotyczy tylko osób posiadających polisy ubezpieczeniowe	Program – Płatnik Program FK – firmy RAKS Akta osobowe (papierowe) Listy płac-papierowe Karty wynagrodzeń – papierowe BHP-papierowe Umowy o pracę Umowy zlecenia Rachunki	Zamykane szafy w pomieszczeniach zamykanych, dostępnych tylko dla upoważnionych osób. Kontrola dostępu do systemu informatycznego, dostęp tylko dla upoważnionych osób, instalacja oprogramowania zabezpieczającego typu firewall, system antywirusowy	Po przeprowadzeniu oceny ryzyka podjęto decyzję, że ocena skutków dla ochrony danych nie jest wymagana.	Nie dotyczy
3.	Zgłoszenie pracowników i członków ich rodzin do ZUS, ich aktualizacja i przekazywanie danych o zwolnieniach.	Biuro LGD, Zarząd LGD, biuro księgowe (księgowy)	Zgłoszenia pracownika i członków jego rodziny do ZUS, ich aktualizacja oraz przekazywanie informacji o zwolnieniach.	Pracownicy	Dane identyfikacyjne, dane adresowe, dane o Odziale NFZ oraz inne dane wymagane w formularzu zgłoszenia ZUS ZUA -zgłoszenie, ZUS IUA - zmiana danych, ZUS ZWUA - wyrejestrowanie, ZUS ZCNA - zgłoszenie członka rodziny, ZAS - wniosek o	● Przepis prawa. Ustawa z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych (Dz.U. z 2017 r., poz. 1778 t.j.) - art. 1, 6 oraz 6a	Pracownik	50 lat [art. 51u ust 1 ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwaln	Nie		Banki, urzędy skarbowe, ZUS, inne firmy ubezpieczeniowe - dotyczy tylko osób posiadających polisy	Program – Płatnik Program FK – firmy RAKS Akta osobowe (papierowe) Listy płac-papierowe Karty wynagrodzeń –	Zamykane szafy w pomieszczeniach zamykanych, dostępnych tylko dla upoważnionych osób. Kontrola dostępu do systemu informatycznego, dostęp tylko dla upoważnionych osób, instalacja oprogramowania zabezpieczającego typu firewall, system antywirusowy,	Po przeprowadzeniu oceny ryzyka podjęto decyzję, że ocena skutków dla ochrony	Nie dotyczy

					ustalenie okresu zasiłkowego, OL-2 - wniosek o kontrolę zaśw. lekarskiego, Z15a - zgłoszenie opieki nad dzieckiem, Z15B - zgłoszenie opieki nad innym członkiem rodziny			ym i archiwach (Dz. U. z 2018 r., poz. 217 t.j.)]	dotyczy	Nie dotyczy	ubezpieczeniowe,	papierowe BHP-papierowe Umowy o pracę Umowy zlecenia Rachunki	system wykrywania włamań..	danych nie jest wymagana.	
4.	Wystawianie i płacenie faktur lub rachunków	Biuro LGD, Zarząd LGD, biuro księgowe (księgowy)	Kontrahenci podmioty współpracujące		Dane identyfikacyjne, dane adresowe, numer rachunku bankowego, numer telefonu, adres e-mail, numer NIP, numer REGON, PESEL, przedmiot i kwota zobowiązania	Umowa (stosunek zobowiązaniowy)	Kontrahenci podmioty współpracujące	10 lat	Nie dotyczy	Nie dotyczy	Dane nie są przekazywane innym podmiotom	Oświadczenia i deklaracje Program – Płatnik Akta osobowe (papierowe) Listy płac-papierowe Microsoft Office	Zamykane szafy w pomieszczeniach zamykanych, dostępnych tylko dla upoważnionych osób. Kontrola dostępu do systemu informatycznego, dostęp tylko dla upoważnionych osób, instalacja oprogramowania zabezpieczającego typu firewall, system antywirusowy	Po przeprowadzeniu oceny ryzyka podjęto decyzję, że ocena skutków dla ochrony danych nie jest wymagana.	Nie dotyczy
5.	Realizacja zadań na rzecz członków stowarzyszenia	Biuro LGD, Zarząd LGD	Realizacja zadań statutowych kierowanych do członków stowarzyszenia i zbieranie składek członkowskich	Członkowie Stowarzyszenia	Dane identyfikacyjne, dane adresowe, adres do korespondencji, numer dowodu osobistego, telefon, adres e-mail, numer NIP, numer PESEL, seria i numer dowodu osobistego, miejsce pracy - przynależność do sektora	Deklaracja członkowska	Członkostwo, Zgoda na przetwarzanie	10 lat	Nie dotyczy	Nie dotyczy	Urząd Marszałkowski zgodnie z prowadzonym nadzorem na LGD zgodnie z ustawą o RLKS	Deklaracje przystąpienia do stowarzyszenia – papierowe i w programie Excel	Zamykane szafy w pomieszczeniach zamykanych, dostępnych tylko dla upoważnionych osób. Kontrola dostępu do systemu informatycznego, dostęp tylko dla upoważnionych osób, instalacja oprogramowania zabezpieczającego typu firewall, system	Po przeprowadzeniu oceny ryzyka podjęto decyzję, że ocena skutków dla ochrony danych nie jest wymagana.	Nie dotyczy

													antywirusowy		
6.	Ocena i wybór operacji w ramach poddziałania 19.2 Wsparcie na wdrażanie operacji w ramach strategii rozwoju lokalnego kierowanego przez społeczność" objętego PROW 2014-2020	Biuro LGD, Zarząd LGD, Rada LGD	Ocena i wybór operacji zgodnie z Umową ramową zawartą przez LGD a SW	Wnioskodawcy i beneficjenci środków pomocowych PROW 2014-2020, poddziałanie 19.2	Dane identyfikacyjne, dane adresowe, numer telefonu, adres e-mail, numer ewidencyjny producenta ARiMR, NIP, REGON (jeżeli nadany), KRS (jeżeli nadany), numer konta bankowego	● Przepis prawa. art. 21 Ustawy z dnia 20 lutego 2015 r. o rozwoju lokalnym z udziałem lokalnej społeczności oraz Zgoda na przetwarzanie	Wniosek o dofinansowanie	10 lat	Agencja Restrukturyzacji i Modernizacji Rolnictwa, Urząd Marszałkowski Województwa Mazowieckiego	Podmiot utrzymujący aplikację elektroniczną w celu serwisu aplikacji służącej zdalnej ocenie operacji przez Radę LGD	Nie dotyczy	Baza uczestników – Excel i papierowo, Wnioski o dofinansowanie, Ewidencja w programie Excel i papierowa, Szkolenia Karty zgłoszeń (papierowe) Listy obecności (papierowe) Ewidencja w programie Excel Konkursy: karty zgłoszeń papierowe	Zamykane szafy w pomieszczeniach zamykanych, dostępnych tylko dla upoważnionych osób. Kontrola dostępu do systemu informatycznego, dostęp tylko dla upoważnionych osób, instalacja oprogramowania zabezpieczającego typu firewall, system antywirusowy	Po przeprowadzeniu oceny ryzyka podjęto decyzję, że ocena skutków dla ochrony danych nie jest wymagana.	Nie dotyczy
7.	Wsparcie beneficjentów w ramach Sieci Ośrodków Działaj		Umową zawarta z podmiotem w celu aktywizowania lokalnych społeczności		Dane identyfikacyjne, dane adresowe, numer telefonu, adres e-mail, numer, NIP, REGON (jeżeli	● Wniosek i zgoda na przetwarzanie	Wniosek o wsparcie z programu Działaj	10 lat	Akademia Rozwoju Filantropii w Polsce Polsko-	Nie dotyczy	Nie dotyczy	Papierowo/ Elektronicznie	Zamykane szafy w pomieszczeniach zamykanych, dostępnych tylko dla upoważnionych osób. Kontrola	Po przeprowadzeniu oceny ryzyka podjęto decyzję, że	Nie dotyczy

	Lokalnie	Biuro LGD, Zarząd LGD	na terenach wiejskich i w małych miastach poprzez projekty obywatelskie, które służą pobudzaniu aspiracji rozwojowych i poprawie jakości życia oraz przyczyniają się do budowy kapitału społecznego	Stowarzyszenie pragnące pozyskać wsparcie w ramach programu Działaj Lokalnie	nadany), KRS (jeżeli nadany), numer konta bankowego	danych osobowych	Lokalnie		Amerykańska Fundacja Wolności (PAFW)				dostępu do systemu informatycznego, dostęp tylko dla upoważnionych osób, instalacja oprogramowania zabezpieczającego typu firewall, system antywirusowy	ocena skutków dla ochrony danych nie jest wymagana.	
8.	Kolonie	Biuro LGD, Zarząd LGD	Umową na realizację kolonii (w ramach promocji zdrowia i profilaktyki zdrowotnej dofinansowany ze środków Funduszu Składkowego Ubezpieczenia Społecznego Rolników)	Dzieci i młodzież udająca się na kolonie wiejskie finansowane ze środków publicznych (KRUS)	Dane identyfikacyjne, dane adresowe dziecka i opiekuna prawnego (rodzica), numer telefonu, adres e-mail, numer, numer konta bankowego jeżeli podane	● Wniosek i zgoda na przetwarzanie danych osobowych	Wniosek o udział w kolonii	10 lat	Kasa Rolniczego Ubezpieczenia Społecznego Fundusz Ubezpieczenia Społecznego Rolników Starostwo Powiatowe finansujące kolonie	Nie dotyczy	Nie dotyczy	Papierowo/ Elektronicznie	Zamykane szafy w pomieszczeniach zamykanych, dostępnych tylko dla upoważnionych osób. Kontrola dostępu do systemu informatycznego, dostęp tylko dla upoważnionych osób, instalacja oprogramowania zabezpieczającego typu firewall, system antywirusowy	Po przeprowadzeniu oceny ryzyka podjęto decyzję, że ocena skutków dla ochrony danych nie jest wymagana.	Nie dotyczy
9.	Organizacja imprez i wydarzeń		Organizacja wydarzeń aktywizujących lub promocyjnych w celu	Mieszkańcy gmin	Dane identyfikacyjne, miejsce zamieszkania, telefon, adres e-mail	● Zgoda na przetwarzanie	Lista obecności	5 lat	Nie dotyczy	Nie dotyczy	Nie dotyczy	Formularz na stronie LGD Karty wolontarius	Zamykane szafy w pomieszczeniach zamykanych, dostępnych tylko dla upoważnionych osób. Kontrola	Po przeprowadzeniu oceny ryzyka podjęto decyzję, że	Nie dotyczy

		Biuro LGD	realizacji zadań statutowych/ realizacja obowiązków wynikających z umowy ramowej zawartej pomiędzy LGD a SW na Funkcjonowanie w ramach poddziałania 19.4 PROW	członkowskich LGD, turyści								zy (papierowe)	dostępu do systemu informatycznego, dostęp tylko dla upoważnionych osób, instalacja oprogramowania zabezpieczającego typu firewall, system antywirusowy	ocena skutków dla ochrony danych nie jest wymagana.	

Załącznik 2 do Polityki Bezpieczeństwa oraz Instrukcji Bezpieczeństwa danych osobowych w Lokalnej Grupie Działania Równiny Wołomińskiej

WYKAZ OSÓB UPOWAŻNIONYCH PRZETWARZANIA DANYCH OSOBOWYCH

Lp.	Imię Nazwisko	Nr zbioru (czynności przetwarzania)	Okres upoważnienia		Uwagi
			OD	DO	
1					
2					
3					
4					
5					

Załącznik 3 do Polityki Bezpieczeństwa oraz Instrukcji Bezpieczeństwa danych osobowych w Lokalnej Grupie Działania Równiny Wołomińskiej

WYKAZ MIEJSC PRZETWARZANIA DANYCH OSOBOWYCH

Lp.	Nazwa pomieszczenia	Adres
1	Pomieszczenia biurowe LGD	ul. Przemysłowa 70, 05-240 Tłuszcz

Załącznik 4 do Polityki Bezpieczeństwa oraz Instrukcji Bezpieczeństwa danych osobowych w Lokalnej Grupie Działania Równiny Wołomińskiej

WAŻNOŚĆ

od: **……...**
do: ***do odwołania***

UPOWAŻNIENIE / UNIEWAŻNIENIE

Na podstawie RODO

upoważniam Panią/Pana:

……..

do przetwarzania, w ramach wykonywanych obowiązków i zadań, z wykorzystaniem następujących zbiorów danych osobowych:

Nr zbioru (czynności przetwarzania)
…….

……..……..
(data, podpis IOD)

Załącznik 5 do Polityki Bezpieczeństwa oraz Instrukcji Bezpieczeństwa danych osobowych w Lokalnej Grupie Działania Równiny Wołomińskiej

OŚWIADCZENIE UPOWAŻNIONEGO DO PRZETWARZANIA DANYCH OSOBOWYCH

……., dn. ……

…….
(imię i nazwisko osoby upoważnionej)

OŚWIADCZENIE

1. Stwierdzam własnoręcznym podpisem, że znana mi jest treść:

   a) Polityki Bezpieczeństwa i Instrukcji ochrony danych osobowych
   b) 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).

2. Jednocześnie zobowiązuję się nie ujawniać wiadomości, z którym zapoznałem/-am się z racji wykonywanych zadań, a w szczególności nie będę:

   a) ujawniać danych zawartych w eksploatowanych w systemach informatycznych, zwłaszcza danych osobowych znajdujących się w tych systemach,
   b) ujawniać szczegółów technologicznych używanych w systemów oraz oprogramowania,
   c) udostępniać osobom nieupoważnionym nośników magnetycznych i optycznych oraz wydruków komputerowych,
   d) kopiować lub przetwarzać danych w sposób inny niż dopuszczony obowiązującą w Polityce Bezpieczeństwa ochrony danych osobowych

……
(podpis osoby upoważnionej)

Załącznik 6 do Polityki Bezpieczeństwa oraz Instrukcji Bezpieczeństwa danych osobowych w Lokalnej Grupie Działania Równiny Wołomińskiej

RAPORT
Z NARUSZENIA BEZPIECZEŃSTWA ZASAD OCHRONY DANYCH OSOBOWYCH
w …….

1. Data: …….. …… Godzina: ……
(dd.mm.rr) (gg: mm)

2. Osoba powiadamiająca o zaistniałym zdarzeniu:

……..……
(imię, nazwisko, stanowisko służbowe, nazwa użytkownika (jeśli występuje)

3. Lokalizacja zdarzenia:

……..……
(np. nr pokoju, nazwa pomieszczenia)

4. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:
……..……
……..……...…
……..……

5. Przyczyny wystąpienia zdarzenia:
……..……
……..……...…

6. Podjęte działania:
……..……
……..……...…

7. Postępowanie wyjaśniające:
……..……
……..……...…

……..……..
(data, podpis IOD)