

ZARZĄDZENIE NR 23/2005

Starosty Lęborskiego

z dnia 23.12.2005 roku

w sprawie ochrony danych osobowych oraz wprowadzenia dokumentacji polityki bezpieczeństwa informacji w Starostwie Powiatowym w Lęborku

Na podstawie art.36 ust.1 Ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (t.j. Dz. U 2002 nr 101, poz. 926 z późn. zmian.), § 3 ust.3 Rozporządzenia 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 2004 nr 100, poz. 1024) oraz § 23 ust.1 Regulaminu organizacyjnego Starostwa Powiatowego w Lęborku, ustalonego uchwałą Nr III/12/98 z dnia 30.12.1998 roku ze zmianami

zarządza się co następuje:

§1

Wprowadza się dokumentację ochrony danych osobowych w celu stosowania i przestrzegania zasad postępowania w procesach przetwarzania danych osobowych, oraz ochrony interesów osób fizycznych, których dane są lub mogą być przetwarzane w zbiorach danych w **Starostwie Powiatowym w Lęborku**.

§2

W skład dokumentacji wchodzi:

- 1) Instrukcja Ochrony Danych Osobowych
- 2) Instrukcja eksploatacji systemów informatycznych, w których przetwarzane są dane osobowe
- 3) Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych.

§3

Odpowiedzialnym za nadzór i przestrzeganie zasad w Instrukcjach wymienionych w §2 czynię p. Jarosława Horodeckiego, któremu powierzam funkcję Administratora Bezpieczeństwa Informacji.

§5

Traci moc Zarządzenie Nr 9/2001 Starosty Lęborskiego z dnia 14 listopada 2001 r. w sprawie wyznaczenia administratorów bezpieczeństwa informacji o danych osobowych w systemach informatycznych służących do przetwarzania danych osobowych będących w administrowaniu Starosty Lęborskiego.

§6

Zarządzenie wchodzi w życie z dniem podpisania.

STAROSTA

Witold Piórkowski



INSTRUKCJA
Postępowania w sytuacji
naruszenia ochrony danych
osobowych



POLITYKA BEZPIECZEŃSTWA INFORMACJI STAROSTWA POWIATOWEGO W LĘBORKU

ROZDZIAŁ I

§1

Celem instrukcji jest określenie sposobu postępowania w przypadku, gdy:

- 1) Stwierdzono naruszenie zabezpieczenia systemu informatycznego w obszarze danych osobowych.
- 2) Stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci komputerowej mogą wskazywać na naruszenie bezpieczeństwa danych osobowych.

§2

Instrukcja określa zasady postępowania wszystkich osób zatrudnionych przy przetwarzaniu danych osobowych w systemach informatycznych.

§3

Naruszeniem zabezpieczenia systemu informatycznego, przetwarzającego dane osobowe jest każdy stwierdzony fakt nieuprawnionego ujawnienia danych osobowych, udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną, uszkodzenia lub jakiegokolwiek elementu systemu informatycznego, a w szczególności:

- 1) nieautoryzowany dostęp do danych,
- 2) nieautoryzowane modyfikacje lub zniszczenie danych,
- 3) udostępnienie danych nieautoryzowanym podmiotom,
- 4) nielegalne ujawnienie danych,
- 5) pozyskiwanie danych z nielegalnych źródeł.

ROZDZIAŁ II

§4

1. W przypadku stwierdzenia naruszenia zabezpieczenia systemu informatycznego lub zaistnienia sytuacji, które mogą wskazywać na naruszenie zabezpieczenia danych osobowych, każdy pracownik zatrudniony przy przetwarzaniu danych osobowych w **Starostwie Powiatowym w Lęborku** jest zobowiązany przerwać przetwarzanie danych osobowych i niezwłocznie powiadomić o tym fakcie



POLITYKA BEZPIECZEŃSTWA INFORMACJI STAROSTWA POWIATOWEGO W LĘBORKU

bezpośredniego przełożonego lub ABI (ewentualnie osobę przez niego upoważnioną), a następnie postępować stosownie do podjętej przez niego decyzji.

2. Zgłoszenie naruszenia ochrony danych osobowych powinno zawierać:

- 1) opisanie symptomów naruszenia ochrony danych osobowych,
- 2) określenie sytuacji i czasu w jakim stwierdzono naruszenie ochrony danych osobowych,
- 3) określenie wszelkich istotnych informacji mogących wskazywać na przyczynę naruszenia,
- 4) określenie znanych danej osobie sposobów zabezpieczenia systemu oraz wszelkich kroków podjętych po ujawnieniu zdarzenia.

§5

Administrator Bezpieczeństwa Informacji lub inna upoważniona przez niego osoba podejmuje wszelkie działania mające na celu:

- 1) minimalizację negatywnych skutków zdarzenia,
- 2) wyjaśnienie okoliczności zdarzenia,
- 3) zabezpieczenie dowodów zdarzenia,
- 4) umożliwienie dalszego bezpiecznego przetwarzania danych.

§6

W celu realizacji zadań niniejszej Instrukcji Administrator Bezpieczeństwa Informacji lub inna upoważniona przez niego osoba ma prawo do podejmowania wszelkich działań dopuszczonych przez prawo, a w szczególności:

- 1) żądania wyjaśnień od pracowników,
- 2) korzystania z pomocy konsultantów,
- 3) nakazania przerwania pracy, zwłaszcza w zakresie przetwarzania danych osobowych.

§7

Polecenie Administratora Bezpieczeństwa Informacji wydawane w czasie realizacji zadań wynikających z niniejszej instrukcji są priorytetowe i winny być wykonywane przed innymi.



POLITYKA BEZPIECZEŃSTWA INFORMACJI STAROSTWA POWIATOWEGO W LĘBORKU

§8

Odmowa udzielenia wyjaśnień lub współpracy z Administratorem Bezpieczeństwa Informacji traktowana będzie jako ciężkie naruszenie obowiązków pracowniczych.

§9

Administrator Bezpieczeństwa Informacji po zażegnaniu sytuacji nadzwyczajnej opracowuje raport końcowy, w którym przedstawia **Staroście Lęborskiemu** przyczyny i skutki zdarzenia oraz wnioski, w tym kadrowe, ograniczające możliwość wystąpienia zdarzenia w przyszłości.

ROZDZIAŁ III

§10

Nieprzestrzeganie zasad postępowania określonych w niniejszej instrukcji stanowi ciężkie naruszenie obowiązków pracowniczych i może być przyczyną odpowiedzialności dyscyplinarnej określonej w Kodeksie Pracy.

§11

Jeżeli skutkiem działania określonego w §10 jest ujawnienie informacji osobie nieupoważnionej, sprawca może zostać pociągnięty do odpowiedzialności karnej wynikającej z przepisów Kodeksu Karnego.

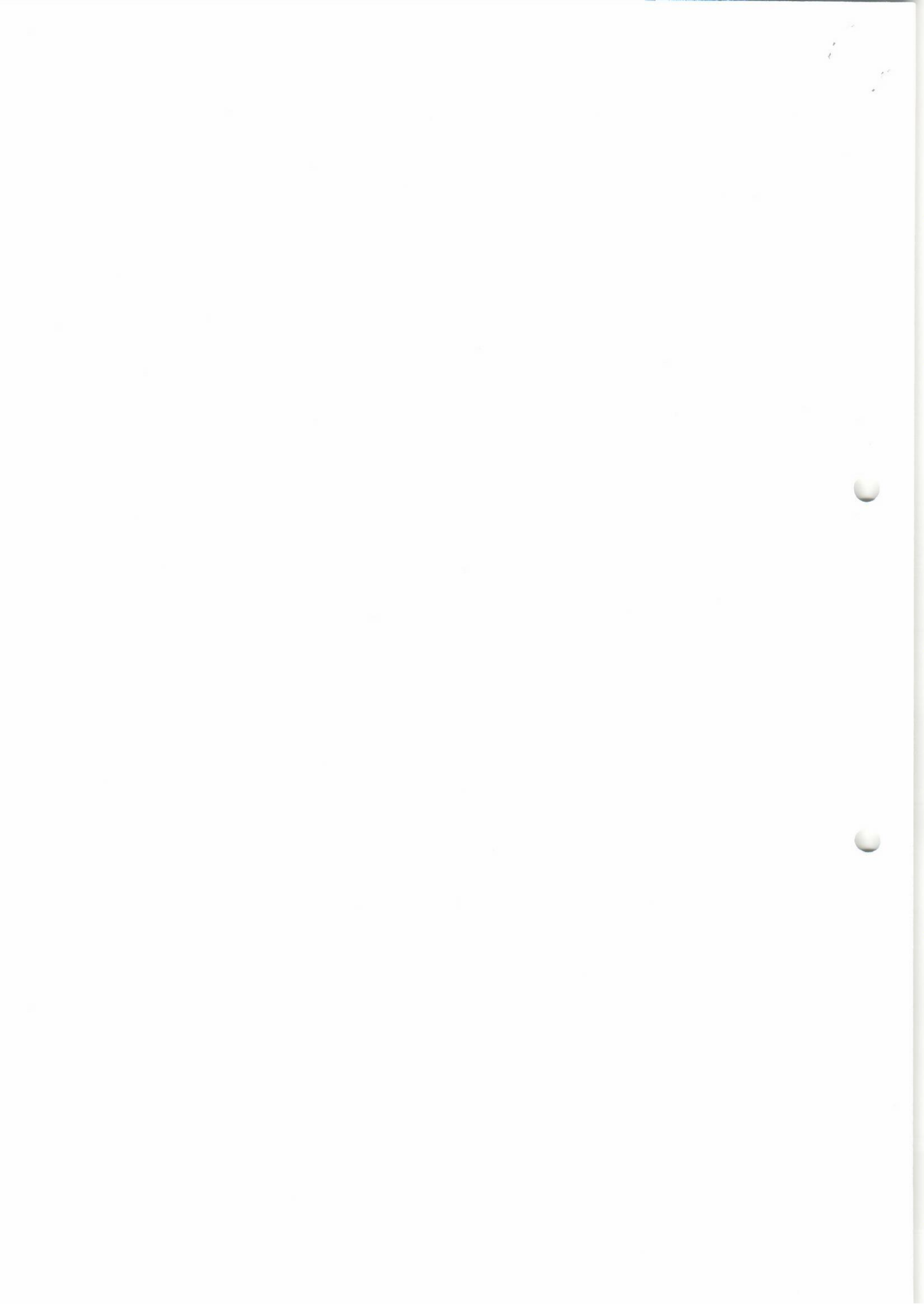
§12

Jeżeli skutkiem działania określonego w §10 jest szkoda, sprawca ponosi odpowiedzialność materialną na warunkach określonych w przepisach Kodeksu Pracy oraz Prawa Cywilnego.



POLITYKA BEZPIECZEŃSTWA INFORMACJI
STAROSTWA POWIATOWEGO W LĘBORKU

INSTRUKCJA **Ochrony Danych Osobowych**





ROZDZIAŁ I

§1

Polityka Bezpieczeństwa Informacji Starostwa Powiatowego w Lęborku jest zbiorem zasad i procedur obowiązujących przy zbieraniu, przetwarzaniu i wykorzystywaniu danych osobowych w wszystkich zbiorach zarządzanych w Starostwie.

Przetwarzanie danych osobowych w **Starostwie Powiatowym w Lęborku** jest dopuszczalne tylko pod warunkiem przestrzegania Ustawy i wydanych na jej podstawie przepisów wykonawczych, oraz Zarządzenia Starosty Lęborskiego, a także przepisów wdrożonych w **INSTRUKCJACH**.

§2

Przez użyte w treści Zarządzenia sformułowania należy rozumieć:

- 1) **Dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.
- 2) **Zbiór danych osobowych** – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego czy zestaw ten jest rozproszony czy zarządzany centralnie.
- 3) **Przetwarzanie danych** – jakiekolwiek operacje wykonywane na danych osobowych, takie jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie.
- 4) **Usuwanie danych** – zniszczenie danych osobowych lub taka ich modyfikacja, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą.
- 5) **Administrator Bezpieczeństwa Informacji (ABI)** – osoba odpowiedzialna za nadzór, kontrolę i bezpieczeństwo danych osobowych.
- 6) **Polityka Bezpieczeństwa Informacji (PBI)** – zbiór zarządzeń i instrukcji określających zasady przetwarzania danych osobowych
- 7) **System informatyczny** – system przetwarzania informacji wraz ze związanymi z nim ludźmi oraz zasobami technicznymi i finansowymi, który dostarcza i rozprowadza informacje.
- 8) **Osoby zatrudnione przy przetwarzaniu danych osobowych** – są to wszystkie osoby, które przetwarzają dane osobowe w ramach



**POLITYKA BEZPIECZEŃSTWA INFORMACJI
STAROSTWA POWIATOWEGO W LĘBORKU**

wykonywanych zadań na danym stanowisku oraz osoby z zewnątrz jednostki organizacyjnej mające dostęp w ramach prac zleconych, czy realizacji danej umowy.

§3

1. Do realizacji postanowień Zarządzenia powołuję i czynię odpowiedzialnym **Administradora Bezpieczeństwa Informacji** – Pan Jarosław Horodecki
Do realizacji bezpieczeństwa sieci informatycznej wyznacza się **Administradora Sieci Informatycznej** – Pan Rafał Sakowicz

Starostwo Powiatowe w Lęborku jako Administrator Danych

w rozumieniu przepisów Ustawy, przetwarza dane osobowe zgodnie z celami statutowymi przy spełnieniu przynajmniej jednego z poniższych warunków:

- 1) Jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa.
 - 2) Jest to konieczne do realizacji umowy, gdy osoba której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy, na żądanie osoby, której dotyczą.
 - 3) Osoba, której dane dotyczą, wyrazi na to zgodę, chyba że chodzi o usunięcie danych jej dotyczących.
 - 4) Jest to niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego.
 - 5) Jest to niezbędne do wypełnienia usprawiedliwionych celów **Starostwa Powiatowego w Lęborku** związanych z realizacją celów statutowych, a przetwarzanie danych osobowych nie narusza praw i wolności osoby, której dotyczą.
2. **Starostwo Powiatowe w Lęborku** określa zakres przetwarzanych danych osobowych w wydawanych regulaminach lub w indywidualnych umowach z podmiotami zewnętrznymi, którym zlecono przetwarzanie danych osobowych.
 3. W przypadkach szczególnych cel i zakres przetwarzanych danych mogą określać przepisy ogólnie obowiązujące.



POLITYKA BEZPIECZEŃSTWA INFORMACJI STAROSTWA POWIATOWEGO W LĘBORKU

§4

1. Dostęp do zbioru danych osobowych oraz ich przetwarzania mają tylko osoby wpisane do ewidencji prowadzonej przez **Administrатора Bezpieczeństwa Informacji**.
2. Osoby zatrudnione w **Starostwie Powiatowym w Lęborku** przy przetwarzaniu danych osobowych są zobowiązane do przechowywania danych osobowych we właściwych zbiorach, nie dłużej niż jest to niezbędne dla osiągnięcia celu ich przetwarzania.
3. Osoby zatrudnione w **Starostwie Powiatowym w Lęborku** przy przetwarzaniu danych osobowych w systemach informatycznych są zobowiązane do postępowania zgodnie z „Instrukcją zasady eksploatacji systemów informatycznych, w których przetwarzane są dane osobowe”

§5

1. Osoby zatrudnione przy przetwarzaniu danych są zobowiązane powiadomić **Administrатора Bezpieczeństwa Informacji** o ewentualnych naruszeniach bezpieczeństwa systemu ochrony danych osobowych.
2. Tryb postępowania określa „Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych”.

§6

W Starostwie Powiatowym w Lęborku zabrania się przetwarzania w danych ujawniających:

- 1) pochodzenie rasowe lub etniczne,
 - 2) poglądy polityczne,
 - 3) przekonania religijne lub filozoficzne,
 - 4) przynależność wyznaniową,
 - 5) przynależność partyjną lub związkową,
 - 6) stan zdrowia, kod genetyczny, nałogi lub fakty z życia seksualnego.
- Chyba, że pozwalają na to obowiązujące przepisy prawa lub osoba, której powyższe dane dotyczą wyraziła pisemną zgodę.**



**POLITYKA BEZPIECZEŃSTWA INFORMACJI
STAROSTWA POWIATOWEGO W LĘBORKU**

§7

Pracownik, który:

- 1) Przetwarza w zbiorze danych:
 - a) dane osobowe, do których przetwarzania nie jest upoważniony,
 - b) dane osobowe, których przetwarzanie jest zabronione,
 - c) dane osobowe niezgodne z celem stworzenia zbioru danych.
- 2) Udostępnia lub umożliwia dostęp do danych osobowych osobom nieupoważnionym.
- 3) Nie zgłasza **Administratorowi Bezpieczeństwa Informacji** zbiorów danych podlegających rejestracji.
- 4) Nie dopełnia obowiązku poinformowania osoby, której dane dotyczą, o przysługujących jej prawach.
- 5) Uniemożliwia osobie, której dane dotyczą, korzystanie z przysługujących jej praw.

Podlega odpowiedzialności karnej zgodnie z Ustawą oraz przepisami Kodeksu Pracy.

ROZDZIAŁ II

§8

Dane osobowe przetwarzane w **Starostwie Powiatowym w Lęborku** mogą być uzyskiwane:

- 1) Bezpośrednio od osób, których te dane dotyczą.
- 2) Z innych źródeł, w granicach dozwolonych przepisami prawa.

§9

Zbierane dane osobowe muszą być wykorzystane tylko do celów, w jakich są lub będą przetwarzane. Po wykorzystaniu danych osobowych, powinny być one przechowywane w postaci uniemożliwiającej identyfikację osób, których dotyczą.



ROZDZIAŁ III

§10

1. Kierownicy komórek organizacyjnych w **Starostwie Powiatowym w Lęborku** zbierających i przetwarzających dane osobowe są odpowiedzialni za poinformowanie osób, których dane przetwarzają o:
 - 1) Adresie siedziby **Starostwa Powiatowego w Lęborku** gdzie są zbierane i przetwarzane.
 - 2) Celu zbierania danych, dobrowolności lub obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.
 - 3) Prawie dostępu do treści swoich danych oraz ich poprawiania.

Wzór pisma - Załącznik nr 1 do niniejszej instrukcji.

2. W przypadku zbierania danych osobowych nie od osoby, której one dotyczą, osobę której dotyczą należy poinformować ponadto o:
 - 1) Źródle danych
 - 2) Uprawnieniach wynikających z art. 32 ust. 1 pkt. 7 i 8 Ustawy o ochronie danych osobowych.

§11

1. Materiały dotyczące działalności **Starostwa Powiatowego w Lęborku** mogą być wysyłane tylko do tych klientów, którzy wcześniej wyrazili zgodę na piśmie na przetwarzanie ich danych osobowych w tym celu.
2. Kandydaci do pracy w **Starostwie Powiatowym w Lęborku** w procesie rekrutacji muszą podpisać pisemną zgodę na przetwarzanie ich danych osobowych.
3. Dokumenty wymienione w ust. 2 są przechowywane w jednostce organizacyjnej, która przetwarza te dane.

Wzór pisma - Załącznik nr 2 do niniejszej instrukcji.

ROZDZIAŁ IV

§12

1. Osobom, których dane przetwarza się w zbiorze danych w **Starostwie Powiatowym w Lęborku**, przysługuje prawo kontroli



POLITYKA BEZPIECZEŃSTWA INFORMACJI STAROSTWA POWIATOWEGO W LĘBORKU

ich danych osobowych, a w szczególności prawo do uzyskania wyczerpujących informacji na temat tych danych.

2. Każda osoba, która wystąpi z wnioskiem o otrzymanie informacji, o których mowa w ust. 1, musi otrzymać odpowiedź na piśmie w terminie nie przekraczającym 30 dni od daty wpłynięcia wniosku, w formie powszechnie zrozumiałej.

Wzór pisma - Załącznik nr 3 do niniejszej instrukcji.

§13

W przypadku gdy dane osoby są niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem Ustawy, albo są zbędne do realizacji celu, dla którego zostały zebrane, Administrator Bezpieczeństwa Informacji jest zobowiązany do ich uzupełnienia, uaktualnienia lub sprostowania.

ROZDZIAŁ V

§14

Kierownicy komórek organizacyjnych w **Starostwie Powiatowym w Lęborku**, w których przetwarzane są dane osobowe, są zobowiązani do zgłoszenia **Administratorowi Bezpieczeństwa Informacji**:
planowanego rejestrowania nowych zbiorów danych osobowych
wnoszenia zmian zbiorów już zarejestrowanych

ROZDZIAŁ VI

§15

Starostwo Powiatowe w Lęborku zobowiązane jest do stosowania środków organizacyjnych i technicznych, zapewniających ochronę przetwarzania danych, w szczególności przed ich udostępnieniem, kradzieżą, uszkodzeniem lub zniszczeniem przez osoby nieupoważnione.



POLITYKA BEZPIECZEŃSTWA INFORMACJI STAROSTWA POWIATOWEGO W LĘBORKU

§16

1. Całkowity nadzór i kontrolę przetwarzania danych w **Starostwie Powiatowym w Lęborku** realizuje **Starosta Lęborski** osobiście.
2. ABI wydaje i przechowuje indywidualne upoważnienia (*Załącznik nr 4*) osobom przetwarzającym dane osobowe.
3. **ABI zobowiązany jest do:**
 - 1) Prowadzenia wykazu osób, którym wydał imienne upoważnienia.
 - 2) Prowadzenia ewidencji osób zatrudnionych przy przetwarzaniu danych, zgodnie z art. 39 Ustawy i Rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 01 maja 2004r.
 - 3) Ewidencji oświadczeń (*Załącznik nr 5*) o zachowaniu w tajemnicy danych osobowych oraz o zapoznaniu się z przepisami dotyczącymi ochrony danych osobowych, od wszystkich pracowników etatowych oraz pobierania ich w przyszłości od nowozatrudnionych przy przetwarzaniu danych pracowników.
 - 4) Ewidencji oświadczeń (*Załącznik nr 6*) o zachowaniu w tajemnicy danych osobowych oraz o zapoznaniu się z przepisami dotyczącymi ochrony danych osobowych, od osób obecnie zatrudnionych na podstawie umowy zlecenia, o dzieło i innej umowy cywilnej oraz żądania ich przy nowo zawieranych umowach.
 - 5) Zapewnienia zapoznania osób zatrudnionych przy przetwarzaniu danych osobowych z przepisami dotyczącymi ochrony danych osobowych.

§17

W celu realizacji powierzonych zadań **Administrator Bezpieczeństwa Informacji** ma prawo:

- 1) Kontrolować komórki w **Starostwie Powiatowym w Lęborku** w zakresie właściwego zabezpieczenia systemów informatycznych oraz pomieszczeń, w których przetwarzane są dane osobowe.
- 2) Wydawać polecenia Kierownikom komórek organizacyjnych w **Starostwie Powiatowym w Lęborku** w zakresie bezpieczeństwa danych osobowych.
- 3) Informować Starostę Lęborskiego o przypadkach naruszenia bezpieczeństwa danych osobowych.
- 4) Żądania od wszystkich pracowników Starostwa Powiatowego w Lęborku wyjaśnień w sytuacjach naruszenia bezpieczeństwa danych osobowych.



ROZDZIAŁ VII

§18

Starostwo Powiatowe w Lęborku może udostępnić dane osobowe przetwarzane we własnych zbiorach tylko osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.

§19

1. Zbiory danych udostępnia się na pisemny, umotywowany wniosek, chyba że odrębne przepisy prawa stanowią inaczej.
2. Wniosek powinien zawierać informacje, umożliwiające wyszukanie żądanych danych osobowych w zbiorze oraz wskazywać ich zakres i przeznaczenie.
3. Wniosek jest rozpatrywany przez ABl, który jednocześnie prowadzi ich ewidencję.
4. Decyzje w sprawie udostępnienia podejmuje Starosta osobiście lub inna upoważniona przez Starostę osoba.

§20

Starostwo Powiatowe w Lęborku może odmówić udostępnienia danych osobowych, jeżeli spowodowałoby to istotne naruszenia dóbr osobistych osób, których dane dotyczą lub innych osób.

§21

1. **Starostwo Powiatowe w Lęborku** jako administrator danych może przetwarzanie danych osobowych powierzyć innemu podmiotowi **wyłącznie w drodze umowy zawartej w formie pisemnej.**
2. Podmiot, o którym mowa w ust. 1 jest zobowiązany do zastosowania środków organizacyjnych i technicznych, zabezpieczających zbiór przed dostępem osób nieupoważnionych na zasadach określonych w przepisach o ochronie danych osobowych.
3. W przypadkach opisanych w ust. 1 i 2, odpowiedzialność za ochronę przetwarzanych danych osobowych spoczywa na **Starostwie Powiatowym w Lęborku**, co nie wyłącza odpowiedzialności podmiotu, z którym zawarto umowę, z tytułu przetwarzania danych niezgodnie z umową.



**POLITYKA BEZPIECZEŃSTWA INFORMACJI
STAROSTWA POWIATOWEGO W LĘBORKU**

4. Do kontroli zgodności przetwarzanych danych przez upoważniony przez **Starostwo Powiatowe w Lęborku** podmiot, stosuje się odpowiednio przepisy art.14 –19 Ustawy o ochronie danych osobowych.



**POLITYKA BEZPIECZEŃSTWA INFORMACJI
STAROSTWA POWIATOWEGO W LĘBORKU**

Załącznik nr 4

Upoważnienie
.....

Działając na podstawie uprawnień nadanych mi w **Starostwie Powiatowym w Lęborku** w sprawie ochrony danych osobowych, upoważniam

Pani/ Pana Imię i Nazwisko

Do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład zlokalizowanych w **Starostwie Powiatowym w Lęborku** służących do przetwarzania danych osobowych zawartych w zbiorze informatycznym/nieinformatycznym noszącym nazwę.....

Wyżej wymieniona osoba została zapoznana z obecnie obowiązującymi przepisami dotyczącymi ochrony danych osobowych i dopuszczona jest do ich przetwarzania jedynie w zakresie określonym w Ustawie z dnia 29.08.1997r, o ochronie danych osobowych (tekst jednolity Dz. U z roku 2002 nr 101, poz. 926) i wydanych do niej przepisach wykonawczych oraz w Zarządzeniu Starosty Lęborskiego w sprawie ochrony danych osobowych.

Wymieniona osoba została wpisana do ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych w **Starostwie Powiatowym w Lęborku**.

.....
miejscowość, data

.....
administrator bezpieczeństwa
informacji



POLITYKA BEZPIECZEŃSTWA INFORMACJI
STAROSTWA POWIATOWEGO W LĘBORKU

Załącznik nr 5

Lębork, dnia.....

Oświadczenie*

Ja niżej podpisany(a)zobowiązuję się do zachowania w tajemnicy danych osobowych, do których mam/ będę miał(a) dostęp w związku z wykonywaniem przeze mnie zadań służbowych i obowiązków pracowniczych w **Starostwie Powiatowym w Lęborku**, zarówno w trakcie obecnie wiążącego mnie stosunku pracy, jak i po ustaniu zatrudnienia.

Zobowiązuję się przestrzegać regulaminów, instrukcji i procedur obowiązujących w **Starostwie Powiatowym w Lęborku** wiążących się z ochroną danych osobowych, a w szczególności nie będę bez upoważnienia służbowego wykorzystywał (a) danych osobowych ze zbiorów w **Starostwie Powiatowym w Lęborku**.

Stwierdzam, że jest mi znana definicja danych osobowych w rozumieniu art. 6 Ustawy z dnia 29.08.1997r, o ochronie danych osobowych (tekst jednolity Dz. U z roku 2002 nr 101, poz. 926) oraz zostałem (am) przeszkolony (a) w zakresie przepisów o ochronie danych osobowych oraz aktów wykonawczych i **instrukcji polityki bezpieczeństwa**.

Przyjmuję do wiadomości, iż postępowanie sprzeczne z powyższymi zobowiązaniami może być uznane za ciężkie naruszenie obowiązków pracowniczych w rozumieniu Kodeksu Pracy.

.....
podpis składającego
oświadczenie

.....
przyjmujący oświadczenie

- oświadczenie dotyczy umów o pracę



**POLITYKA BEZPIECZEŃSTWA INFORMACJI
STAROSTWA POWIATOWEGO W LĘBORKU**

Załącznik nr 6

Lębork, dnia.....

Oświadczenie*

Ja niżej podpisany(a)zobowiązuję się do zachowania w tajemnicy danych osobowych, do których mam/ będę miał(a) dostęp **w związku z wykonywaniem umowy** zawartej z....., zarówno w trakcie trwania umowy jak i po jej wygaśnięciu lub rozwiązaniu.

Zobowiązuję się do ścisłego przestrzegania warunków ww. umowy, które wiążą się z ochroną danych osobowych a w szczególności nie będę bez upoważnienia służbowego wykorzystywał (a) danych osobowych ze zbiorów w **Starostwie Powiatowym w Lęborku** w celach nie związanych z wykonywaniem tej umowy.

Stwierdzam, że jest mi znana definicja danych osobowych w rozumieniu art. 6 Ustawy z dnia 29.08.1997r, o ochronie danych osobowych (tekst jednolity Dz. U z roku 2002 nr 101, poz. 926) oraz zostałem (am) zaznajomiony (a) z przepisami o ochronie danych osobowych.

Przyjmuję do wiążącej wiadomości, iż postępowanie sprzeczne z powyższymi zobowiązaniami oznacza naruszenie warunków umowy zawartej z

.....
podpis składającego
oświadczenie

.....
przyjmujący oświadczenie

oświadczenie dotyczy umów cywilno – prawnych



POLITYKA BEZPIECZEŃSTWA INFORMACJI
STAROSTWA POWIATOWEGO W LĘBORKU

INSTRUKCJA
eksploatacji systemów
informatycznych,
w których przetwarzane są dane
osobowe

$\frac{t}{t^2}$ $\frac{t}{t^2}$



POSTANOWIENIA OGÓLNE

ROZDZIAŁ I

§1

Przez użyte w treści instrukcji sformułowania należy rozumieć:

- 1) **instrukcja** – dokument zarządzania systemami informatycznymi, w których przetwarzane są dane osobowe w **Starostwie Powiatowym w Lęborku**
- 2) **system informatyczny w Starostwie Powiatowym w Lęborku** – zespół środków technicznych (urządzenia komputerowe wraz z okablowaniem i oprogramowaniem), zbiorów, ludzi oraz zasobów technicznych i finansowych, umożliwiające przetwarzanie danych osobowych
- 3) **dane** – każda informacja (tekst, cyfry, wykres, rysunek, dźwięk, animacja itp.), która może być przetworzona przy użyciu systemu informatycznego, bez względu na jej rzeczywiste znaczenie; dane te przechowywane są w systemie informatycznym w postaci elektronicznej (jako tzw. pliki lub zbiory)
- 4) **przetwarzanie danych** – jakiejkolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych
- 5) **użytkownik** – każda osoba, której przydzielono uprawnienia pozwalające na korzystanie z systemu informatycznego i przetwarzanie danych w nim zawartych w określonym przez te uprawnienia zakresie oraz zapewniono fizyczny dostęp do systemu

Szczegółowy zakres praw i obowiązków oraz umiejscowienie w strukturze organizacyjnej w **Starostwie Powiatowym w Lęborku** Administratora Bezpieczeństwa Informacji przedstawia **Załącznik** do niniejszej instrukcji.

ROZDZIAŁ II

§2

Niniejsza instrukcja określa zasady pracy z każdym systemem informatycznym służącym do przetwarzania danych osobowych



POLITYKA BEZPIECZEŃSTWA INFORMACJI STAROSTWA POWIATOWEGO W LĘBORKU

będącym fragmentem systemu informatycznego w **Starostwie Powiatowym w Lęborku**.

§3

Niniejsza instrukcja reguluje następujące zagadnienia:

- 1) zasady eksploatacji systemów informatycznych
- 2) bezpieczeństwo systemów informatycznych
- 3) zasady dostępu do systemu informatycznego
- 4) procedury rozpoczęcia i zakończenia pracy w systemie informatycznym
- 5) zasady tworzenia i przechowywania kopii awaryjnych
- 6) zabezpieczenie antywirusowe systemu informatycznego
- 7) zasady postępowania z nośnikami informacji
- 8) zasady komunikacji w sieciach komputerowych
- 9) zasady monitorowania, przeglądu i konserwacji systemów informatycznych
- 10) zasady dokonywania zmian w systemach informatycznych
- 11) odpowiedzialność i obowiązki użytkowników systemu informatycznego

§4

Stopień poziomu zabezpieczeń informacji przetwarzanych w systemie informatycznym określa Administrator Bezpieczeństwa Informacji.

ROZDZIAŁ III

§5

Wszystkie osoby zatrudnione przy przetwarzaniu danych osobowych w systemie informatycznym w **Starostwie Powiatowym w Lęborku** bez względu na zajmowane stanowisko i miejsce pracy oraz charakter stosunku pracy są zobowiązane do postępowania zgodnie z zasadami określonymi w niniejszej instrukcji.

§6

Za tworzenie, wdrażanie, administrację i interpretację polityki bezpieczeństwa informacji, standardów, zaleceń i procedur w całym



POLITYKA BEZPIECZEŃSTWA INFORMACJI STAROSTWA POWIATOWEGO W LĘBORKU

systemie informatycznym w **Starostwie Powiatowym w Lęborku** odpowiedzialny jest Starosta Lęborski.

§7

Polecenia osób wyznaczonych przez **Administradora Bezpieczeństwa Informacji** do realizacji zadań w zakresie ochrony informacji i bezpieczeństwa systemu informatycznego muszą być bezwzględnie wykonywane przez wszystkich użytkowników systemu.

§8

System informatyczny w **Starostwie Powiatowym w Lęborku** może być używany tylko na potrzeby działania Starostwa.

§9

Systemy sieciowe stosowane w systemie informatycznym w **Starostwie Powiatowym w Lęborku** muszą wykorzystywać oprogramowanie ograniczające dostęp do plików dla każdego użytkownika osobno, rejestrujące aktywność każdego użytkownika i przyznające Administratorowi Systemu Informatycznego specjalne uprawnienia.

§10

1. Wszystkie stacje robocze pracujące w systemie informatycznym w **Starostwie Powiatowym w Lęborku** muszą być zgodne ze sprzętową oraz programową konfiguracją zalecaną przez Administratora Bezpieczeństwa Informacji.
2. Zabrania się podłączania do systemu informatycznego w **Starostwie Powiatowym w Lęborku** komputerów z takim typem lub wersją systemu operacyjnego, którą użytkownik uprzywilejowany nie jest w stanie administrować.

§11

1. Stacje robocze działające w systemie informatycznym w **Starostwie Powiatowym w Lęborku** muszą mieć możliwość blokowania dostępu do tego systemu oraz możliwość zastosowania zabezpieczonego hasłem wygaszacza ekranu automatycznie uruchamianego po określonym czasie braku aktywności użytkownika.



POLITYKA BEZPIECZEŃSTWA INFORMACJI STAROSTWA POWIATOWEGO W LĘBORKU

2. Powyższe zasady odnoszą się również do komputerów przenośnych zawierających dane z systemu informatycznego w **Starostwie Powiatowym w Lęborku**, jak również do wykorzystywanych w tym systemie urządzeń sieciowych.

§12

W pomieszczeniach, gdzie przebywają osoby postronne, monitory stanowisk dostępu do danych z systemu informatycznego w **Starostwie Powiatowym w Lęborku** powinny być ustawione w sposób uniemożliwiający tym osobom wgląd w dane.

§13

Możliwość wielokrotnego logowania, rozumiana jako logowanie przez jednego użytkownika na kilku komputerach równocześnie z wykorzystaniem tego samego identyfikatora, powinna zostać ograniczona do uzasadnionego rodzaju wykonywanych zadań minimum.

§14

1. Zasady określone w niniejszej instrukcji odnoszą się również do przetwarzania danych osobowych w komputerach przenośnych, w których za bezpieczeństwo danych w całości odpowiada użytkownik urządzenia.
2. Dane osobowe w komputerach przenośnych mogą być przetwarzane wyłącznie za pisemną zgodą Administratora Bezpieczeństwa Informacji.
3. Przetwarzanie danych osobowych w komputerach przenośnych jest dopuszczalna wyłącznie, gdy dostęp do systemu operacyjnego urządzenia jest zabezpieczony hasłem.
4. Użytkownik komputera przenośnego, w którym przetwarzane są dane osobowe obowiązany jest zachować szczególną ostrożność podczas transportu urządzenia i nie zezwalać na jego użytkowanie osobom nieupoważnionym do dostępu do danych osobowych.
5. Każda utrata komputera przenośnego, w którym przetwarzane są dane osobowe musi być natychmiast zgłaszana Administratorowi Bezpieczeństwa Informacji.



POLITYKA BEZPIECZEŃSTWA INFORMACJI STAROSTWA POWIATOWEGO W LĘBORKU

ROZDZIAŁ IV

§15

1. Zabrania się testowania i podejmowania prób poznania metod zabezpieczenia systemu informatycznego w **Starostwie Powiatowym w Lęborku** dopóki nie otrzymają specjalnej, wcześniejszej zgody na piśmie podpisanej przez lokalnego Administratora Bezpieczeństwa Informacji.
2. Niedopuszczalne są próby obejścia zabezpieczeń ustalonych przez Administratora Bezpieczeństwa Informacji.
3. Przypadki związane z nieuprawnionym dostępem do systemu informatycznego w **Starostwie Powiatowym w Lęborku**, łamaniem haseł, deszyfracją plików, kopiowaniem fałszywego oprogramowania lub innymi, podobnymi nieautoryzowanymi próbami pokonywania zabezpieczeń będą uważane za bezprawne i ciężkie naruszenie obowiązków pracowniczych.

ROZDZIAŁ V

§16

1. Wszystkie pomieszczenia, w których przetwarzane są dane z systemu informatycznego w **Starostwie Powiatowym w Lęborku** powinny posiadać drzwi zabezpieczone zamkiem oraz systemy przeciwpożarowe i oznaczone drogi ewakuacji.
2. Przebywanie w pomieszczeniach, o których mowa w ust. 1 osób nieuprawnionych do dostępu do danego systemu informatycznego jest możliwe tylko w obecności użytkownika uprawnionego do korzystania ze sprzętu informatycznego znajdującego się w danym pomieszczeniu.
3. Pomieszczenia, o których mowa w ust. 1 powinny być zamykane na czas nieobecności w nich użytkowników uprawnionych do korzystania ze sprzętu informatycznego znajdującego się w danym pomieszczeniu, w sposób uniemożliwiający dostęp do nich osób trzecich.



POLITYKA BEZPIECZEŃSTWA INFORMACJI STAROSTWA POWIATOWEGO W LĘBORKU

§17

1. Pomieszczenia, w których znajdują się newralgiczne elementy sieci komputerowych, a w szczególności serwery sieciowe, serwery aplikacji, serwery baz danych, serwery komunikacyjne, aktywne urządzenia sieciowe, modemy powinny być zabezpieczone w sposób uniemożliwiający dostęp nieupoważnionych.
2. Pomieszczenia przewidziane na miejsca dla newralgicznych elementów sieci komputerowych powinny w szczególności:
 - 1) znajdować się w budynkach objętych całodobową ochroną,
 - 2) znajdować się w części budynku, gdzie ruch interesantów jest ograniczony,
 - 3) być oddzielone trwałymi wewnętrznymi ścianami od innych pomieszczeń,
 - 4) być zaopatrzone w co najmniej dwa zamki o skomplikowanym mechanizmie otwierania,
 - 5) posiadać aparaturę klimatyzacyjną oraz systemy przeciwpożarowe i oznaczone drogi ewakuacji,
 - 6) posiadać okna odpowiednio zabezpieczone przed dostaniem się z zewnątrz.

Administrator Bezpieczeństwa Informacji może zastosować inne co najmniej tak samo skuteczne metody zabezpieczeń.

3. Zasady i sposób przechowywania kluczy do pomieszczeń, w których znajdują się newralgiczne elementy sieci komputerowych, określa kierownik jednostki organizacyjnej.

ROZDZIAŁ VI

§18

Sprzęt komputerowy używany w systemie informatycznym w **Starostwie Powiatowym w Lęborku** powinien być fizycznie chroniony przed kradzieżą, zniszczeniem lub niewłaściwym użytkowaniem. Bezpośrednio odpowiedzialny za to jest użytkownik tego sprzętu.



POLITYKA BEZPIECZEŃSTWA INFORMACJI STAROSTWA POWIATOWEGO W LĘBORKU

§19

Użytkownicy nie mogą sami demontować komputerów oraz dokonywać jakiegokolwiek zmiany komponentów sprzętu komputerowego. Wykonują to tylko administratorzy (ABI, ASI) lub inne uprawnione osoby.

§20

Sprzęt komputerowy używany w systemie informatycznym w **Starostwie Powiatowym w Lęborku** nie może być przenoszony bez zgody ABI.

§21

1. Każde urządzenie używane w systemie informatycznym w **Starostwie Powiatowym w Lęborku** musi być oznaczone w celu jego identyfikacji.
2. Inwentaryzacji i oznaczenia sprzętu dokonuje ABI, który okresowo kontroluje stan poszczególnych stanowisk komputerowych.
3. Za brak elementów w powierzonym sprzęcie odpowiada pracownik odpowiedzialny za dany sprzęt komputerowy.

ROZDZIAŁ VII

§22

1. Oprogramowanie używane w systemie informatycznym w **Starostwie Powiatowym w Lęborku** musi być chronione przed jakąkolwiek niekontrolowaną modyfikacją, nieautoryzowanym usunięciem oraz kopiowaniem.
2. Przed jakimkolwiek zainstalowaniem nowego oprogramowania należy sprawdzić jego działanie pod kątem bezpieczeństwa całego systemu.

§23

1. W systemie informatycznym w **Starostwie Powiatowym w Lęborku** może być używane wyłącznie oprogramowanie licencjonowane przez posiadacza praw autorskich.
2. Oprogramowanie może być używane tylko zgodnie z prawami licencji.



POLITYKA BEZPIECZEŃSTWA INFORMACJI STAROSTWA POWIATOWEGO W LĘBORKU

§24

Narzędzia związane z bezpieczeństwem systemów mogą być wykorzystane w systemie informatycznym w **Starostwie Powiatowym w Lęborku** tylko jeśli pochodzą od zaufanego dostawcy.

ROZDZIAŁ VIII

§25

Należy zainstalować odpowiednią ochronę przeciwpożarową dla wszystkich elementów systemu informatycznego, które tego wymagają.

§26

1. Każdy komputer powinien być podłączony do wydzielonych gniazd z zasilaniem prądowym.
2. Serwery i krytyczne stacje robocze powinny być chronione zasilaniem awaryjnym (UPS).

ROZDZIAŁ IX

§27

Prawo dostępu do poszczególnych systemów informatycznych mogą mieć wyłącznie osoby, które posiadają pisemne upoważnienie, o którym mowa w Instrukcji Ochrony Danych Osobowych.

§28

1. Żądanie przyznania jak i zmiany praw dostępu do systemu informatycznego musi być udokumentowane w formie pisemnej i zaakceptowane przez Administratora danego systemu informatycznego oraz kierownika danej komórki organizacyjnej.
2. Dla celów archiwizacji wszelkich zdarzeń dotyczących systemu, powyższe dokumenty powinny być przechowywane przez okres przynajmniej 3 lat.



POLITYKA BEZPIECZEŃSTWA INFORMACJI STAROSTWA POWIATOWEGO W LĘBORKU

§29

1. Z wnioskiem o przyznanie dostępu lub zmianę praw dostępu do systemu informatycznego występuje kierownik odpowiedniej komórki organizacyjnej do ABI.
2. Dostęp fizyczny oraz zakres uprawnień przydziela ABI.

§30

Natychmiast po utracie praw dostępu, będącej wynikiem zmiany stanowiska pracy lub zwolnienia z pracy, kierownik odpowiedniej komórki organizacyjnej występuje do ABI o zmianę uprawnień użytkownika lub zlikwidowanie dostępu.

§31

Dział Kadr winien poinformować Administratora Bezpieczeństwa Informacji w przypadku złożenia przez osobę dopuszczoną do przetwarzania danych osobowych w systemie informatycznym w **Starostwie Powiatowym w Lęborku** deklaracji o zamiarze zmiany stanowiska pracy.

§32

Prawo dostępu przyznane użytkownikom, którzy nie są pracownikami **Starostwa Powiatowego w Lęborku** mają charakter czasowy i mogą być przyznawane na okres odpowiadający wykonywanemu zadaniu.

§33

Specjalne prawa dostępu muszą być ściśle ograniczone do osób, które bezpośrednio odpowiadają za administrację poszczególnych systemów informatycznych i ich bezpieczeństwo.

§34

1. Użytkownikiem uprzywilejowanym, jeśli zachodzą takie potrzeby, może być jedynie ABI oraz najwyżej dwie osoby przez niego uprawnione.



POLITYKA BEZPIECZEŃSTWA INFORMACJI STAROSTWA POWIATOWEGO W LĘBORKU

§35

1. Administrator Bezpieczeństwa Informacji może w uzasadnionych przypadkach zastrzec prawo do korzystania z systemu informatycznego każdemu użytkownikowi.
2. W przypadku zastrzeżenia, o którym mowa w ust. 1 natychmiast cofane są wszelkie prawa dostępu do systemu informatycznego dla tego użytkownika, a w uzasadnionych przypadkach następuje

wymiana identyfikatorów i haseł dostępu dla wszystkich lub określonych grup użytkowników.

ROZDZIAŁ X

§36

Dostęp do systemu informatycznego w **Starostwie Powiatowym w Lęborku** musi być zabezpieczony co najmniej przez system identyfikatora i hasła użytkownika.

§37

Identyfikator użytkownika nadawany jest przez Administratora Bezpieczeństwa Informacji.

§38

1. Hasła dostępu do systemu komputerowego tworzone są przez użytkownika i stanowią tajemnicę **Starostwa Powiatowego w Lęborku** znaną wyłącznie temu użytkownikowi.
2. Użytkownik ponosi pełną odpowiedzialność za utworzenie hasła i jego przechowywanie.

§39

1. Hasła nie mogą być przechowywane w formie jawnej w żadnej postaci: elektronicznej lub tradycyjnej (pliki tekstowe, zapisy w skryptach logowania, makrach zdefiniowane jako klawisze funkcyjne terminali, inne dowolne zapisy tradycyjne), szczególnie w miejscach, gdzie może dojść do nieautoryzowanego dostępu ze strony osób trzecich.



POLITYKA BEZPIECZEŃSTWA INFORMACJI STAROSTWA POWIATOWEGO W LĘBORKU

2. Hasła nie mogą być zapisane i pozostawiane w miejscach gdzie osoby nieuprawnione mogą je odczytać.

§40

Wszystkie hasła muszą być natychmiast zmienione jeśli istnieje podejrzenie, że zostały odkryte lub wiadomo, że znajdują się w posiadaniu osoby innej niż autoryzowani użytkownicy.

§41

Hasła dostępów do systemów informatycznych powinny być zmieniane zgodnie z ustaleniami ABI. Zmiana powinna być wymuszana w sposób automatyczny przez odpowiednie oprogramowanie.

§42

1. ABI może przy użyciu specjalnego oprogramowania kontrolować bezpieczeństwo hasła wybranego przez użytkownika i w przypadkach stwierdzenia wadliwości, zmienić je na bezpieczne.
2. ABI może zmieniać hasło użytkownika, lecz nie może znać haseł wybranych przez tegoż użytkownika.

ROZDZIAŁ XI

§43

Wszyscy użytkownicy systemu informatycznego w **Starostwie Powiatowym w Lęborku** muszą być sprawdzeni przez ABI zanim będą mogli używać zasobów wielodostępnych systemów informatycznych. Sprawdzeniu ulega identyfikator użytkownika (ID) i hasło indywidualne dla każdego użytkownika.

§44

ABI obowiązany jest tak go sformatować, by próby dostępu do tego systemu były limitowane zarówno w ujęciu ilościowym jak i czasowym.

§45

1. Systemy kontroli dostępu do systemów informatycznych funkcjonujących w ramach systemu informatycznego w **Starostwie**



POLITYKA BEZPIECZEŃSTWA INFORMACJI STAROSTWA POWIATOWEGO W LĘBORKU

Powiatowym w Lęborku powinny zawierać: system haseł dostępu, identyfikatory użytkowników i zapisu w systemie oraz odpowiednią kontrolę antywirusową.

3. System kontroli dostępu ze strony zewnętrznej (Internet, WAN, łącza publicznej sieci telekomunikacyjnej) do systemu informatycznego w **Starostwie Powiatowym w Lęborku** powinien posiadać: odpowiedni system ochrony firewall dla usług połączeniowych udostępnionych przez serwery sieci w **Starostwie Powiatowym w Lęborku**, serwer autentykacyjny dla użytkowników logujących się zdalnie do systemu, system kontroli połączeń dial-up, mechanizmy szyfrowania i identyfikacji użytkowników przesyłających dane do sieci wewnętrznej w **Starostwie Powiatowym w Lęborku**.
3. Jeżeli podsystem kontroli dostępu do systemu informatycznego lub łączności nie działa prawidłowo, musi on domyślnie blokować prawa dostępu użytkowników. Jednocześnie do czasu naprawy uszkodzeń systemu, dane których dotyczą problemy, muszą pozostać niedostępne.

§46

1. Użytkownicy nie mogą mieć możliwości logowania się do systemu informatycznego lub sieci komputerowej w sposób anonimowy.
2. Jeśli użytkownicy korzystają z cech systemu pozwalających na zmianę swych uprawnień w systemie w trakcie pracy, muszą zawsze logować się z wykorzystaniem identyfikatora (ID), który umożliwia jednoznaczne oznaczenie użytkownika.

§47

1. Proces logowania się do systemu informatycznego w **Starostwie Powiatowym w Lęborku** musi przebiegać przez wyświetlanie przez system zachęty do logowania (zapytanie o nazwę użytkownika i hasło).
2. Do chwili zakończenia autoryzacji w systemie nie mogą być wyświetlane żadne informacje opisujące organizację, konfigurację sieci i inne informacje wewnętrzne.

§48

1. Użytkownicy są odpowiedzialni za administrowanie programem wygaszacza ekranu mającym zabezpieczyć dostęp do komputera



POLITYKA BEZPIECZEŃSTWA INFORMACJI STAROSTWA POWIATOWEGO W ŁĘBORKU

w momencie nieobecności na stanowisku pracy. Zaleca się stosowanie wygaszaczy ekranu zabezpieczających hasłem.

2. Użytkownicy stacji roboczych odpowiadają również za ustawienie hasła na poziomie aplikacji i oprogramowania systemowego.

§49

1. Przed przystąpieniem do pracy w systemie informatycznym w **Starostwie Powiatowym w Łęborku**, każdy użytkownik powinien upewnić się, że spełnione są podstawowe warunki bezpieczeństwa wymagane przy przetwarzaniu danych w systemie informatycznym w **Starostwie Powiatowym w Łęborku**, a w szczególności:

- 1) jeżeli w pomieszczeniu przebywają osoby postronne, monitor stanowiska dostępu do danych z systemu informatycznego ustawiony jest w sposób uniemożliwiający tym osobom wgląd w dane,
 - 2) na danej stacji roboczej zainstalowane jest i sprawnie działa oprogramowanie antywirusowe lub inny sposób realizowana jest ochrona antywirusowa.
 - 3) na danej stacji roboczej zainstalowane jest i sprawnie działa zabezpieczony hasłem wygaszacz ekranu automatycznie uruchamiany po określonym czasie braku aktywności użytkownika.
2. Użytkownik może rozpocząć logowanie się do systemu informatycznego i przystąpić do przetwarzania danych tylko wtedy, gdy spełnione są warunki określone w ust. 1.

§50

Po zakończeniu pracy w systemie informatycznym użytkownik obowiązany jest wylogować się z tego systemu.

§51

Wychodząc z pomieszczenia w którym przetwarzane są dane z systemu informatycznego należy sprawdzić czy zamknięte są okna i wejście do pomieszczenia.

§52

Ze względu na bezpieczeństwo wprowadza się obowiązek sporządzania kopii awaryjnych oprogramowania systemowego, aplikacji i danych.



POLITYKA BEZPIECZEŃSTWA INFORMACJI STAROSTWA POWIATOWEGO W LĘBORKU

§53

Kopie awaryjne mogą być użyte jedynie dla odbudowy systemu uszkodzonego wskutek ataku wirusa, awarii twardego dysku lub innych problemów.

§54

Kopie awaryjne oprogramowania systemowego powinny być sporządzane nie rzadziej niż raz na trzy miesiące oraz po każdej modyfikacji.

§55

1. Kopie awaryjne powinny być przechowywane w szafach ognioodpornych lub powinny być zastosowane środki bezpieczeństwa o podobnej skuteczności.
2. Pomieszczenia, w których przechowywane są kopie awaryjne muszą być zabezpieczone przez dostępem osób nieupoważnionych.

§56

1. Kopie awaryjne danych z poszczególnych systemów informatycznych należy usunąć po ustaniu ich użyteczności.
2. Decyzje o usunięciu kopii awaryjnych z systemu informatycznego podejmuje Administrator Bezpieczeństwa Informacji.

§57

1. Dla zapewnienia nieprzerwanego działania (z dostępem do Internetu) systemu informatycznego w **Starostwie Powiatowym w Lęborku**, użytkownicy stacji roboczych muszą mieć zainstalowane na swoich komputerach oprogramowanie antywirusowe. Oprogramowanie to musi być zainstalowane na serwerach sieciowych.
2. Oprogramowanie antywirusowe musi być zainstalowane tak, aby użytkownik nie był w stanie pominąć etapu skanowania.



§58

1. Każde oprogramowanie pochodzące od osób trzecich lub innych działów nie może być użyte bez wcześniejszego sprawdzenia przy pomocy odpowiedniego oprogramowania antywirusowego.
2. Zewnętrzne dostarczenie dyskietki lub inne media z danymi nie mogą być użyte bez wcześniejszego sprawdzenia przy pomocy odpowiedniego oprogramowania antywirusowego.
3. Skanowanie antywirusowe musi odbyć się zanim program zostanie po raz pierwszy uruchomiony.

§59

W przypadku podejrzenia wykrycia wirusa komputerowego użytkownik natychmiast powiadamia o tym ABI.

ROZDZIAŁ XII

§60

Użytkownicy nie mogą kopiować oprogramowania, informacji o wysokim stopniu ważności oraz informacji wrażliwych należących do **Starostwa Powiatowego w Lęborku** na jakiegokolwiek nośniki informacji (dyskietki, taśmy magnetyczne itd.), przenosić tego oprogramowania na inne komputery lub przekazywać stronom trzecim. Uprawnionym do tego jest jedynie ABI.

§61

1. Wszystkie komputerowe nośniki informacji używane w systemie informatycznym w **Starostwie Powiatowym w Lęborku** winny być odpowiednio oznaczone i zarejestrowane w dziennikach ewidencji.
2. Rejestr wydanych komputerowych nośników informacji prowadzony jest przez ABI.
3. Niedopuszczalne jest stosowanie w systemie informatycznym w **Starostwie Powiatowym w Lęborku** dyskietek, CD-ROM i innych komputerowych nośników informacji bez oznaczeń autoryzujących.
4. Za pobrany komputerowy nośnik informacji oraz bezpieczeństwo zapisanych na nim danych odpowiada użytkownik, który pobrał dany nośnik i posiada go na swoim stanie.



POLITYKA BEZPIECZEŃSTWA INFORMACJI STAROSTWA POWIATOWEGO W LĘBORKU

§62

Autoryzowane do używania z systemu informatycznego w **Starostwie Powiatowym w Lęborku** nośniki informacji powinny być po zakończeniu pracy przechowywane w sposób zapewniający bezpieczeństwo zapisanych na nim danych.

§63

1. W przypadku uszkodzenia lub zużycia dyskietki, płyty CD-ROM lub inne komputerowe nośniki winny być zdawane ABI.
2. ABI dokonuje zniszczenia uszkodzonego lub zużytego komputerowego nośnika informacji w sposób uniemożliwiający odtworzenie zapisanych na nim danych.

ROZDZIAŁ XIII

§64

1. Drukarki nie mogą być pozostawione bez kontroli jeśli są lub wkrótce będą drukowane na nich dane osobowe z systemu informatycznego w **Starostwie Powiatowym w Lęborku**, o ile dostęp osób postronnych do pomieszczeń drukarek nie jest odpowiednio ograniczony
2. Drukowanie na takich drukarkach jest dopuszczalne o ile otoczenie drukarki jest chronione przed fizycznym dostępem osób nieuprawnionych.

§65

1. Za przechowywanie wydruku zawierającego dane z systemu informatycznego w **Starostwie Powiatowym w Lęborku** odpowiada wykonawca.
2. Wykonawca odpowiada za przechowywanie wydruku zawierającego dane z systemu informatycznego w **Starostwie Powiatowym w Lęborku** może przekazać wydruk oraz odpowiedzialność za jego przechowanie innej osobie tylko wtedy, gdy jest ona autoryzowana do dostępu informacji zawartych na wydruku.



POLITYKA BEZPIECZEŃSTWA INFORMACJI STAROSTWA POWIATOWEGO W LĘBORKU

§66

Wydruki zawierające dane z systemu informatycznego w **Starostwie Powiatowym w Lęborku** po zakończeniu pracy powinny być przechowywane w zamkniętych szafach.

§67

1. Wydruki, notatki, kserokopie dokumentów itp. nie wykorzystane a zawierające dane z systemu informatycznego w **Starostwie Powiatowym w Lęborku** muszą być bezwzględnie niszczone w sposób uniemożliwiający odtworzenie ich treści.
2. Za wykonanie czynności, o której mowa w ust.1 odpowiedzialna jest osoba, która w chwili ustania użyteczności danego dokumentu odpowiedzialna jest za jego przechowanie.

§68

Zabrania się przesyłania danych z systemu informatycznego osobom nieautoryzowanym do dostępu do danych z tego systemu informatycznego.

§69

Wszystkie połączenia zewnętrzne do systemu informatycznego w **Starostwie Powiatowym w Lęborku** muszą być bezwzględnie monitorowane.

§70

Zabrania się korzystania z jakichkolwiek modemów podłączanych do komputerów działających w systemie informatycznym w **Starostwie Powiatowym w Lęborku** bez zgody Administratora Bezpieczeństwa Informacji.

§71

1. Wprowadza się okresową weryfikację uprawnień poszczególnych użytkowników aplikacji. Odpowiedzialny za to jest Administrator Bezpieczeństwa Informacji.



POLITYKA BEZPIECZEŃSTWA INFORMACJI STAROSTWA POWIATOWEGO W LĘBORKU

2. Wprowadza się obowiązek prowadzenia historii pracy systemu (dziennik pracy), w którym notuje się wszystkie sytuacje awaryjne oraz sposoby ich usuwania i wszelkich modyfikacji. Za prowadzenie dziennika pracy systemu informatycznego odpowiedzialny jest ABI.

§72

1. Każdy system wielodostępny powinien zawierać odpowiednie, automatyczne narzędzia pozwalające ABI na weryfikację stanu bezpieczeństwa systemu.
2. Poszczególne systemy informatyczne muszą w sposób bezpieczny prowadzić zapis wszystkich znaczących zdarzeń systemowych mających wpływ na bezpieczeństwo przetwarzanych w nich danych osobowych a w szczególności:
 - 1) zmian identyfikatora użytkownika w czasie sesji,
 - 2) prób odgadywania haseł,
 - 3) prób wykorzystania uprawnień, do których użytkownik nie uzyskał autoryzacji,
 - 4) modyfikacji oprogramowania aplikacyjnego,
 - 5) modyfikacji oprogramowania systemowego,
 - 6) zmian uprawnień użytkowników,
 - 7) prób ingerencji w systemowe rejestry zdarzeń.

§73

1. Rejestry zdarzeń systemowych związanych z bezpieczeństwem systemów informatycznych muszą być przechowywane przez okres co najmniej 1 roku.
2. Podczas tego okresu muszą być zabezpieczone w taki sposób aby nie była możliwa ich modyfikacja oraz aby były one dostępne jedynie dla autoryzowanych pracowników.
3. Rejestry zdarzeń systemowych są istotne w przypadku usuwania błędów, rekonstrukcji po włamaniu do systemu, badania i tym podobnych wysiłków.

§74

1. ABI powinien codziennie kontrolować zbiory systemowe dla prawidłowego funkcjonowania systemu.
2. Raz na kwartał ABI przeprowadza kontrolę możliwości zdalnego dostępu (logowania) do poszczególnych systemów.



POLITYKA BEZPIECZEŃSTWA INFORMACJI STAROSTWA POWIATOWEGO W LĘBORKU

3. Co kwartał należy przeprowadzać weryfikację całego oprogramowania użytkowego eksploatowanego na wszystkich komputerach podłączonych do systemu informatycznego pod kątem spełnienia wymogów bezpieczeństwa. Czynności te winny być dokumentowane w dzienniku ABI.

§75

Administrator Bezpieczeństwa Informacji co najmniej raz na kwartał winien przeprowadzić weryfikację usług sieciowych dostępnych w systemach informatycznych oraz blokować usługi niewykorzystywane.

§76

ABI jest odpowiedzialny za uaktualnianie systemów operacyjnych i aplikacji.

§77

Wszystkie zmiany dotyczące sieci komputerowych w **Starostwie Powiatowym w Lęborku** powinny być:

- 1) udokumentowane w takim porządku w jakim zostały przeprowadzone,
- 2) zaakceptowane przez Administratora Bezpieczeństwa Informacji.

§78

1. Zmiany w systemie informatycznym w **Starostwie Powiatowym w Lęborku** mogą być dokonywane wyłącznie przez ABI lub upoważnioną przez niego osobę.
2. Nie można zestawiać nowych połączeń między komputerami w systemie informatycznym w **Starostwie Powiatowym w Lęborku**, dopóki nie zostanie udzielone zezwolenie przez ABI.
3. Celem takiego postępowania jest ochrona przed nieoczekiwanymi przerwami w dostarczaniu usług, nieautoryzowanym dostępem do informacji i innymi problemami.
4. Proces ten odnosi się nie tylko do pracowników ale również do personelu dostawców sprzętu i oprogramowania.



ROZDZIAŁ XIV

§79

ABI jest odpowiedzialny za prawidłowe działanie podległego mu systemu informatycznego.

§80

1. Administrator Bezpieczeństwa Informacji działa w zakresie polityki bezpieczeństwa danych w **Starostwie Powiatowym w Lęborku**.
2. ABI odpowiedzialny jest za określenie właściwych uprawnień użytkowników, monitorowanie zapisów związanych z bezpieczeństwem dotyczącym administrowanych przez nich systemach.
3. Odpowiedzialny jest również za przekazywanie osobom wyznaczonym do ochrony wszelkich informacji dotyczących podejrzanej działalności związanej z bezpieczeństwem komputerów i sieci komputerowych.

ROZDZIAŁ XV

§81

Użytkownicy odpowiedzialni są za wypełnianie wszystkich postanowień dotyczących bezpieczeństwa informacji w systemie informatycznym w **Starostwie Powiatowym w Lęborku**.

§82

Kierownicy komórek organizacyjnych odpowiedzialni są za bieżące przestrzeganie zasad ustalonych w instrukcjach ochrony danych osobowych oraz zasad użytkowania urządzeń i systemów informatycznych w **Starostwie Powiatowym w Lęborku**.



POLITYKA BEZPIECZEŃSTWA INFORMACJI STAROSTWA POWIATOWEGO W LĘBORKU

ROZDZIAŁ XVI

§83

Nieprzestrzeganie postanowień niniejszej instrukcji oraz brak nadzoru nad bezpieczeństwem informacji stanowi ciężkie naruszenie obowiązków pracowniczych i może być przyczyną odpowiedzialności dyscyplinarnej określonej przepisami Kodeksu Pracy.

§84

Jeżeli skutkiem działania użytkownika jest ujawnienie informacji osobie nieupoważnionej, sprawca może być pociągnięty do odpowiedzialności karnej określonej przepisami Kodeksu Karnego.

§85

Jeżeli skutkiem działania użytkownika jest szkoda, sprawca ponosi odpowiedzialność materialną na warunkach określonych w przepisach Kodeksu Pracy oraz Kodeksu Cywilnego.

