ZARZĄDZENIE NR 65/2017

STAROSTY RACIBORSKIEGO

z dnia 22 maja 2017 r.

w sprawie zasad ochrony danych osobowych przetwarzanych w Starostwie Powiatowym w Raciborzu

Działając na podstawie art. 35 ust. 2 ustawy z dnia 5 czerwca 1998 r. o samorządzie powiatowym (t.j. Dz. U. 2016 r., poz. 814 z późn. zm.) i art. 36 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. 2016 r., poz. 922), § 3 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych .

zarządzam co następuje:

§ 1. Wprowadzam do stosowania w Starostwie Powiatowym w Raciborzu:

1) "Politykę bezpieczeństwa" stanowiącą załącznik nr 1 do Zarządzenia.

2) "Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych" stanowiącą załącznik nr 2 do Zarządzenia.

§ 2. Przestrzeganie zasad ochrony danych osobowych przetwarzanych w Starostwie Powiatowym w Raciborzu szczegółowo określonych w załącznikach, o których mowa w § 1 nadzoruje Administrator Bezpieczeństwa Informacji powołany odrębnym zarządzeniem.

§ 3. Wykonanie niniejszego zarządzenia powierzam wszystkim pracownikom Starostwa Powiatowego w Raciborzu, a nadzór - kierownikom komórek organizacyjnych Starostwa.

§ 4. Traci moc: Zarządzenie Nr 14/2012 Starosty Raciborskiego z dnia 31 grudnia 2012 r. w sprawie zasad ochrony danych osobowych przetwarzanych w Starostwie Powiatowym w Raciborzu.

§ 5. Upoważnienia do przetwarzania danych osobowych i dostępu do systemów informatycznych nadane na podstawie dotychczas obowiązujących przepisów zachowują swoją moc.

§ 6. Aktualizacja załączników do dokumentów, o których mowa w § 1 pkt 1 i 2, nie powoduje konieczności zmiany niniejszego Zarządzenia.

§ 7. Zarządzenie wchodzi w życie z dniem podpisania i podlega publikacji w Bazie Rejestrów Urzędowych na stronie internetowej www.bip.powiatraciborski.pl, oraz w Intranecie Starostwa Powiatowego w Raciborzu.

STAROSTA

Ryszard Winiarski

Załącznik Nr 1 do Zarządzenia Nr 65/2017

Starosty Raciborskiego

z dnia 22 maja 2017 r.

POLITYKA BEZPIECZEŃSTWA

§ 1. Celem Polityki Bezpieczeństwa jest wprowadzenie i przestrzeganie w Starostwie Powiatowym w Raciborzu zasad przetwarzania danych osobowych oraz stosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych, określonych w ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2016 poz. 922) oraz w przepisach wykonawczych.

§ 2. Dane osobowe przetwarza się w Starostwie w celu realizacji zadań ustawowych. Przetwarzanie i ochrona danych osobowych podlegają przepisom Ustawy.

§ 3. Zasady bezpieczeństwa i ochrony danych osobowych przetwarzanych w Starostwie dotyczą wszystkich danych, niezależnie od formy ich przetwarzania w zbiorach danych lub poza nimi.

§ 4. Definicje

Starostwo	Starostwo Powiatowe w Raciborzu.
Ustawa	Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2016 r., poz. 922).
GIODO	Generalny Inspektor Ochrony Danych Osobowych - organ do spraw ochrony danych osobowych powołany przez Sejm Rzeczypospolitej Polskiej za zgodą Senatu.
Administrator Danych	Starosta Raciborski jako organ samorządu terytorialnego decydujący o celach i środkach przetwarzania danych osobowych w Starostwie Powiatowym w Raciborzu zgodnie z art.7 ust. 4 Ustawy.
Administrator Bezpieczeństwa Informacji	Pracownik odpowiedzialny za nadzór nad bezpieczeństwem informacji przetwarzanych w Starostwie powołany przez Administratora Danych zgodnie z art. 36a ust. 1 Ustawy.
Dysponent	Kierownik komórki organizacyjnej odpowiadający za przetwarzanie danych w aplikacji lub zbiorze danych osobowych.
Dane osobowe	Wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej zgodnie z art. 6 Ustawy.
Przetwarzanie danych	Operacje wykonywane na danych osobowych takie jak zbieranie, przeglądanie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie zgodnie z art. 7 ust. 2 Ustawy.
Zbiór danych osobowych	Każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.
Baza danych osobowych	Zbiór danych osobowych przetwarzany w systemie informatycznym.
Poufność danych	Zapewnienie, że dane nie są udostępniane lub ujawniane nieupoważnionym osobom lub podmiotom.
Integralność danych	Zapewnienie, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany.
Dostępność danych	Zapewnienie, że dane są osiągalne i możliwe do wykorzystania na żądanie w założonym czasie, przez upoważnione osoby lub podmioty.
Rozliczalność	Zapewnienie, że działania osoby lub podmiotu mogą być przypisane tylko tej osobie lub podmiotowi.
Autentyczność	Zapewnienie, że tożsamość osoby lub podmiotu jest taka, jak deklarowana.
Niezaprzeczalność	Brak możliwości wyparcia się przez osobę lub podmiot swego uczestnictwa w procesie przetwarzania danych.
System Informatyczny Starostwa	Zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych stosowanych w celu przetwarzania danych wStarostwie.
Administrator Systemu Informatycznego	Pracownik zgodnie z zakresem czynności odpowiedzialny za ciągłość pracy, bezpieczeństwo i rozwój Systemu Informatycznego w Starostwie.
Aplikacja	Pogram komputerowy, będący częścią Systemu Informatycznego służący do przetwarzania danych w określonym dla niego obszarze.
Administrator aplikacji	Użytkownik posiadający uprawnienia do zarządzania aplikacją, odpowiedzialny za ciągłość pracy i rozwój aplikacji.
Użytkownik	Pracownik posiadający upoważnienie do przetwarzania danych w Systemie Informatycznym Starostwa.
Identyfikator użytkownika	Ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę, która jest użytkownikiem systemu informatycznego.
Identyfikacja użytkownika	Użycie identyfikatora użytkownika w systemie informatycznym w celu weryfikacji jego tożsamości.
Uwierzytelnianie	Weryfikowanie przez mechanizmy systemu informatycznego tożsamości użytkownika na podstawie jego identyfikatora.
Autoryzacja	Weryfikowanie, czy dany użytkownik ma prawo dostępu do informacji, do których usiłuje uzyskać dostęp.
Active Directory	Usługa systemu informatycznego służąca do uwierzytelniania i autoryzacji użytkowników.
Incydent bezpieczeństwa	Pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem

	informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań i zagrażają bezpieczeństwu informacji.
Komórka organizacyjna	Wyodrębniony element struktury Starostwa, w szczególności: wydział, referat, biuro oraz samodzielne stanowisko pracy.

§ 5. Zadania i czynności

1. **Administrator Danych** – realizuje zadania w zakresie ochrony danych osobowych, a w szczególności:

1) Podejmuje decyzje o celach i środkach przetwarzania danych osobowych z uwzględnieniem przede wszystkim zmian w obowiązujących przepisach prawa, zmian w organizacji Starostwa oraz technik zabezpieczenia danych osobowych.
2) Dokłada wszelkich starań aby dane osobowe w Starostwie przetwarzane były zgodnie z prawem, zbierane dla oznaczonych, zgodnych z prawem celów, merytorycznie poprawne i adekwatne w stosunku do celów w jakich są przetwarzane, przechowywane nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.
3) Upoważnia poszczególnych pracowników do przetwarzania danych osobowych w określonym indywidualnie zakresie, odpowiadającym zakresowi ich obowiązków.
4) Powołuje Administratora Bezpieczeństwa Informacji i wyznacza Administratora Systemu Informatycznego.
5) Zleca Kierownikowi Referatu Administracyjnego, do którego obowiązków należą sprawy związane z zaopatrzeniem, by we współpracy z Administratorem Bezpieczeństwa Informacji oraz Administratorem Systemu Informatycznego zapewnił użytkownikom odpowiednie stanowiska pracy umożliwiające bezpieczne przetwarzanie danych.
6) Zatwierdza korespondencję z GIODO w tym dotyczącą rejestracji i aktualizacji zbiorów danych osobowych.
7) Podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia procedur bezpiecznego przetwarzania danych osobowych.

2. **Administrator Bezpieczeństwa Informacji** - realizuje zadania w zakresie zapewnienia przestrzegania przepisów o ochronie danych osobowych, a w szczególności:

1) Opracowuje i aktualizuje dokumentację z zakresu bezpieczeństwa danych osobowych.
2) Sprawdza zgodność przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowuje w tym zakresie sprawozdania dla Administratora Danych.
3) Zapewnia zapoznanie osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych.
4) Prowadzi nadzór nad ciągłym procesem szkoleń w zakresie ochrony danych osobowych pracowników Starostwa.
5) Prowadzi rejestr zbiorów danych osobowych przetwarzanych przez Administratora Danych.
6) Prowadzi ewidencję dokumentów z zakresu ochrony danych osobowych.
7) Nadzoruje powierzanie przetwarzania danych osobowych podmiotom zewnętrznym.
8) Akceptuje dokumenty dotyczące ochrony danych osobowych przygotowywane przez komórki organizacyjne Starostwa w tym zwłaszcza:
   a) wnioski o udzielenie upoważnienia do przetwarzania danych osobowych,
   b) wnioski o powierzenie przetwarzania danych osobowych podmiotom zewnętrznym,
   c) upoważnienia do przetwarzania danych osobowych,
   d) umowy powierzenia przetwarzania danych osobowych podmiotom zewnętrznym.

9) Przygotowuje wspólnie z dysponentami zbiorów danych osobowych wnioski zgłoszeń rejestracyjnych i aktualizacyjnych tych zbiorów do Generalnego Inspektora Ochrony Danych Osobowych.

10) Decyduje o ograniczeniu lub pozbawieniu uprawnień do przetwarzania zbiorów danych osobowych użytkownikom, którzy powodują zagrożenie bezpieczeństwa ochrony danych osobowych.

11) Nadzoruje usuwanie nieprawidłowości stwierdzonych w czasie prowadzonych sprawdzeń i dostosowanie ochrony danych osobowych do stanu zgodnego z przepisami.

12) Prowadzi bieżące sprawdzenia stosowania zasad przetwarzania danych osobowych przez pracowników Starostwa zakresie:

a) dostępu do danych osobowych (kontrola zgodności dokumentów upoważniających do przetwarzania danych osobowych z wykonywanymi czynnościami),

b) zabezpieczenia fizycznego (serwerownie, pomieszczenia biurowe, w których przechowywane są dane osobowe, szafy i inne meble biurowe, w których przechowywane są dane osobowe, zasada "czyste biurko"),

c) zabezpieczeń programowych i sprzętowych (ochrona antywirusowa, ochrona przed dostępem z sieci zewnętrznej, identyfikatory, hasła, ustawienie monitorów).

3. **Administrator Systemu Informatycznego** - realizuje zadania w zakresie zarządzania i bieżącego nadzoru nad Systemem Informatycznym Starostwa, a w szczególności:

1) Zarządza Systemem Informatycznym Starostwa , posługując się hasłem dostępu z pozycji administratora.

2) Na podstawie upoważnienia wydanego przez Administratora Danych przydziela każdemu użytkownikowi identyfikator oraz hasło dostępu do Systemu Informatycznego Starostwa oraz dokonuje ewentualnych modyfikacji uprawnień, a także blokuje i usuwa konta użytkowników zgodnie z zasadami określonymi w instrukcji zarządzania systemem informatycznym.

3) Prowadzi w systemie elektronicznym ewidencję użytkowników upoważnionych do przetwarzania danych w Systemie Informatycznym Starostwa, która zawiera:

- nazwisko i imię użytkownika,
- identyfikator użytkownika,
- stanowisko użytkownika,
- komórkę organizacyjną Starostwa, w której użytkownik jest zatrudniony, odbywa staż, praktykę lub wykonuje czynności określone w innej umowie,
- wykaz aplikacji, do których użytkownik ma upoważnienie i zakres uprawnień użytkownika w tym zakresie,
- datę przyznania uprawnień,
- datę utraty ważności upoważnienia.

4) Przeciwdziała dostępowi osób niepowołanych do Systemu Informatycznego Starostwa, w tym w szczególności do aplikacji, w których przetwarzane są dane osobowe.

5) Nadzoruje działanie mechanizmów uwierzytelniania i autoryzacji użytkowników w Systemie Informatycznym Starostwa.

6) W sytuacji stwierdzenia naruszenia zasad bezpieczeństwa przetwarzania danych osobowych w Systemie Informatycznym Starostwa, informuje Administratora Bezpieczeństwa Informacji i współdziała z nim przy usuwaniu skutków naruszenia.

7) Prowadzi dokumentację naruszeń bezpieczeństwa (incydentów) w Systemie Informatycznym Starostwa.

8) Sprawuje nadzór nad wykonywaniem napraw, konserwacji oraz likwidacji urządzeń komputerowych, nad wykonywaniem kopii zapasowych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii Systemu Informatycznego Starostwa.

9) Podejmuje działania służące zapewnieniu niezawodności zasilania komputerów, innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych oraz zapewnieniu bezpiecznej wymiany danych w sieci wewnętrznej i bezpiecznej teletransmisji.

4. **Dysponent** (kierownik komórki organizacyjnej) - realizuje zadania w zakresie nadzoru nad aplikacją lub zbiorem danych osobowych, za które, zgodnie z wykazem (Załącznik nr 2 do Polityki Bezpieczeństwa) odpowiada komórka organizacyjna Starostwa, a w szczególności:

1) Zgłasza do Administratora Bezpieczeństwa Informacji zmiany dotyczące zakresu przetwarzanych w bazie danych osobowych.

2) Opiniuje wnioski o udzielenie upoważnienia użytkownikowi do przetwarzania danych osobowych w zbiorze danych i decyduje o poziomie uprawnień do przetwarzania danych w tym zbiorze.

3) Opiniuje wnioski o udzielenie upoważnienia użytkownikowi do przetwarzania danych w aplikacji i decyduje o poziomie uprawnień do przetwarzania danych w tej aplikacji, w tym uprawnieniu do administrowania aplikacją.

4) Zarządza kopiami bazy danych i aplikacji:

   a) zleca Administratorowi Systemu Informatycznego wysłanie bazy danych do naprawy w serwisie zewnętrznym,

   b) zleca Administratorowi Systemu Informatycznego przywrócenie bazy danych z kopii bezpieczeństwa.

5) Wyznacza administratorów aplikacji.

5. **Administrator aplikacji** - realizuje zadania w zakresie zarządzania aplikacją na podstawie uprawnień nadanych mu przez dysponenta aplikacji, a w szczególności:

1) Nadaje uprawnienia użytkownikom do modułów i funkcji aplikacji zgodnie z ich upoważnieniem.

2) Zgłasza do Administratora Bezpieczeństwa Informacji uwagi dotyczące przetwarzania w aplikacji danych osobowych.

3) Zgłasza do Administratora Systemu Informatycznego problemy techniczne występujące w trakcie działania aplikacji.

4) Zgłasza do Administratora Systemu Informatycznego konieczność zainstalowania nowej wersji aplikacji wraz z instrukcją obsługi dla użytkowników.

5) W sytuacji stwierdzenia naruszenia zabezpieczeń aplikacji informuje Administratora Systemu Informatycznego i współdziała z nim przy usuwaniu skutków naruszenia.

6. **Użytkownik** - obsługuje aplikacje do przetwarzania baz danych osobowych:

1) Wyłącznie w zakresie zgodnym z upoważnieniem otrzymanym od Administratora Danych.

2) Zgłasza do administratora aplikacji uwagi dotyczące przetwarzania w aplikacji danych osobowych.

3) Zgłasza do Administratora Systemu Informatycznego problemy techniczne występujące w trakcie działania aplikacji.

§ 6. Dostęp do danych osobowych

1. Do przetwarzania danych osobowych, dla których administratorem jest Starosta Raciborski dostęp może mieć wyłącznie osoba spełniająca następujące warunki:

1) Posiada upoważnienie wydane przez Administratora Danych.

2) Przed przystąpieniem do wykonywania czynności związanych z przetwarzaniem danych osobowych zapoznała się z obowiązującymi w Starostwie przepisami w zakresie ochrony danych osobowych i zobowiązała się do ich przestrzegania.

3) Została przeszkolona przez Administratora Bezpieczeństwa Informacji w zakresie przepisów Ustawy, lub posiada inny dokument stwierdzający odbycie takiego przeszkolenia.

2. Upoważnienie, o którym mowa w ust. 1 pkt 1 wydawane jest:

1) Pracownikom Starostwa zatrudnionym na podstawie umowy o pracę – na wniosek bezpośredniego przełożonego,

2) Osobom nie będącym pracownikami Starostwa, w szczególności odbywającym staż, praktykę lub wykonującym czynności określone w innej umowie – na wniosek kierownika komórki organizacyjnej Starostwa sprawującego nadzór nad realizacją powierzonych zadań.

3) Wniosek, o którym mowa w ust. 2 opiniowany jest przez dysponentów zbiorów danych osobowych i aplikacji służących do ich przetwarzania.

3. Zobowiązanie, o którym mowa w ust. 1 pkt 2 udokumentowane jest oświadczeniem przechowywanym w aktach osobowych pracownika Starostwa lub jako załącznik do Rejestru Upoważnień – dla osób nie będących pracownikami Starostwa.

§ 7. Zbiory danych osobowych

1. Wykaz zbiorów danych osobowych przetwarzanych w Starostwie wraz ze wskazaniem aplikacji stosowanych do ich przetwarzania, opisem struktury bazy danych i sposobem przepływu danych między bazami, znajduje się w załączniku nr 1 do Polityki Bezpieczeństwa.

2. Wykaz aplikacji stosowanych w Starostwie do przetwarzania danych osobowych, znajduje się w załączniku nr 3 do Polityki Bezpieczeństwa.

3. Załączniki nr 1 i 2 do Polityki Bezpieczeństwa są aktualizowane na bieżąco przez Administratora Bezpieczeństwa Informacji.

§ 8. Rejestracja zbiorów danych osobowych

1. Kierownicy komórek organizacyjnych Starostwa zobowiązani są do zgłoszenia Administratorowi Bezpieczeństwa Informacji, w formie pisemnej, zamiaru utworzenia nowego zbioru danych osobowych lub uzyskania dostępu do zbioru danych osobowych w skutek powierzenia przez inny podmiot.

2. Dysponenci zbiorów danych osobowych zobowiązani są do zgłoszenia Administratorowi Bezpieczeństwa Informacji, w formie pisemnej, zamiar dokonania zmian w zakresie informacji przetwarzanych w podlegającym im zbiorach danych.

3. Administrator Bezpieczeństwa Informacji aktualizuje "Wykaz zbiorów danych osobowych dla których administratorem jest Starosta Raciborski" (Załącznik nr 1 do Polityki Bezpieczeństwa) i decyduje o konieczności zgłoszenia nowego zbioru danych osobowych GIODO, lub umieszczenia zbioru w jawnym wykazie Administratora Danych.

4. Administrator Systemu Informatycznego nadaje uprawnienia użytkownikom do przetwarzania danych w nowej bazie na podstawie ich upoważnień.

5. Administrator Systemu Informatycznego aktualizuje procedury wykonywania kopii systemu o nową bazę danych.

6. O rozpoczęciu zbierania informacji w nowym zbiorze danych osobowych decyduje Dysponent który:

1) Sprawdza czy użytkownicy posiadają aktualne upoważnienia z odpowiednim poziomem uprawnień.

2) Sprawdza czy dostęp do zbioru danych posiadają tylko upoważnieni użytkownicy.

3) Sprawdza czy zastosowane zostały zasady zabezpieczenia danych zgodnie z §12 i 13 Polityki Bezpieczeństwa.

§ 9. Zasady przetwarzania danych osobowych.

1. Osoba, która dokonuje operacji przetwarzania danych osobowych zobowiązana jest do ścisłego przestrzegania obowiązujących przepisów z zakresu ochrony danych osobowych, ze świadomością odpowiedzialności karnej, którą określa Rozdział 8 Ustawy, a w szczególności do:

1) Przetwarzania danych osobowych tylko w zakresie posiadanego upoważnienia, zgodnie z art. 49 Ustawy.

2) Nie udostępniania i nie umożliwiania dostępu do danych osobowych osobom nieupoważnionym, zgodnie z art. 51 Ustawy.

3) Prawidłowego zabezpieczania danych osobowych przed zabraniem, uszkodzeniem lub zniszczeniem, zgodnie z art. 52 Ustawy.

4) Informowania osób, których dane dotyczą o ich prawach wynikających z ustawy, zgodnie z art. 54 ustawy.

5) Niezwłocznego informowania Administratora Systemu Informatycznego o wszelkich zauważonych incydentach stwarzających zagrożenie dla bezpieczeństwa przetwarzania danych osobowych w Systemie Informatycznym Starostwa.

6) Niezwłocznego informowania Administratora Bezpieczeństwa Informacji o wszelkich zauważonych nieprawidłowościach mających wpływ na bezpieczeństwo przetwarzania danych osobowych.

7) Niezwłocznego informowania Administratora Bezpieczeństwa Informacji o zamierzonych i odbywających się czynnościach kontrolnych przeprowadzanych przez GIODO i inne upoważnione podmioty, zgodnie z art. 54a Ustawy.

§ 10. Powierzenie przetwarzania danych osobowych

1. Powierzenie zbioru danych osobowych innemu podmiotowi jest dopuszczalne tylko w drodze umowy zawartej na piśmie na wniosek tego podmiotu.

2. Wniosek, o którym mowa w ust. 1 powinien zawierać:

1) Oznaczenie wnioskodawcy.

2) Określenie celu przetwarzania powierzonych danych.

3) Określenie zakresu przetwarzania powierzonych danych.

4) Określenie czasu, po którym zostanie zakończone przetwarzanie powierzonych danych.

3. Podmiot, o którym mowa w ust. 1, może przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie.

4. Podmiot, któremu przekazano dane osobowe musi zastosować odpowiednie do zagrożeń środki techniczne i organizacyjne w celu zapewnienia ochrony danych, zgodnie z art. 39-39a Ustawy.

5. Nadzór nad powierzaniem przetwarzania danych osobowych podmiotom zewnętrznym sprawuje Administrator Bezpieczeństwa Informacji.

§ 11. Miejsca przetwarzania danych osobowych

1. Lokalizacja zbiorów danych osobowych przetwarzanych w Starostwie:

1) Zbiory kartotekowe:

a) pomieszczenia w budynkach Starostwa Powiatowego w Raciborzu:

- Plac Okrzei 4

- Plac Okrzei 4a

- ul. Opolska 5

2) Bazy informatyczne w budynkach Starostwa Powiatowego w Raciborzu:

a) serwerownia w budynku B, Plac Okrzei 4 - I piętro, pok. nr 116,

b) serwerownia w budynku B, Plac Okrzei 4 - II piętro, pok. nr 212,

c) serwerownia w budynku A, Plac Okrzei 4a - parter, pok. nr 4a,

d) kancelaria w budynku B, Plac Okrzei 4 - parter, pok. nr 21,

e) Administrator Systemu Informatycznego w budynku Plac Okrzei 4 - I piętro, pok. 114.

3) Zbiory informatyczne, dla których zawarto umowy powierzenia przetwarzania danych - lokalizacja określona w umowie powierzenia przetwarzania.

2. Przetwarzanie danych osobowych ma miejsce wyłącznie w pomieszczeniach Starostwa i pomieszczeniach podmiotów, z którymi zawarto umowy powierzenia przetwarzania danych.

3. Przebywanie w pomieszczeniach, o których mowa w ust.1 i 2 osób nieuprawnionych do przetwarzania danych osobowych, jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu tych danych.

4. Pomieszczenia, w których przetwarzane są dane osobowe powinny być zamykane i chronione na czas nieobecności w nich osób upoważnionych do przetwarzania danych osobowych, w sposób uniemożliwiający dostęp do nich osób trzecich.

5. Pomieszczenia, w których przechowywane są bazy informatyczne lub kopie baz danych oraz pomieszczenie Administratora Systemu Informatycznego podlegają szczególnej ochronie i powinny być wyposażone w instalację kontroli dostępu i instalację alarmową.

§ 12. Zasady zabezpieczenia danych osobowych przetwarzanych w sposób tradycyjny

1. Dokumenty zawierające dane osobowe przechowywane są w pomieszczeniach biurowych, w meblach zamykanych na klucz.

2. Pomieszczenia biurowe, o których mowa w ust. 1 są:

1) Przed rozpoczęciem pracy - sprawdzane, czy nie ma śladów włamania lub uszkodzenia. Takiemu samemu sprawdzeniu podlegają meble biurowe, w których przechowywane są dokumenty zawierające dane osobowe.

2) W trakcie godzin pracy - zamykane na czas nieobecności osoby zatrudnionej przy przetwarzaniu danych osobowych.

3) Po zakończeniu pracy – sprawdzane, czy nie pozostały niezabezpieczone dokumenty zawierające dane osobowe, czy meble biurowe i szafy zostały zamknięte, czy dokumenty w pojemniku z makulaturą zostały zniszczone w stopniu uniemożliwiającym identyfikację danych osobowych.

3. Osoby nieupoważnione przebywają w pomieszczeniach biurowych tylko w obecności osoby zatrudnionej przy przetwarzaniu danych.

4. Dostęp do zbioru danych osobowych posiada tylko osoba upoważniona.

5. Zasady postępowania z kluczami od pomieszczeń i mebli biurowych określają odrębne przepisy.

6. Nadzór nad prawidłowym zabezpieczeniem pomieszczeń biurowych i mebli sprawuje Kierownik Referatu Administracyjnego.

§ 13. Zabezpieczenie danych przetwarzanych w systemie informatycznym.

1. W Starostwie z uwagi na fakt, że urządzenia systemu teleinformatycznego służącego do przetwarzania danych osobowych połączone są z siecią publiczną, stosuje się wysoki poziom bezpieczeństwa teleinformatycznego.

2. Bezpieczeństwo teleinformatyczne na poziomie wysokim zapewnia się przez:

1) Środki prawne - spełnienie wymogów określonych w Ustawie, a w szczególności:

a) został powołany Administrator Bezpieczeństwa Informacji nadzorujący przestrzeganie zasad ochrony przetwarzanych danych osobowych,

b) został wyznaczony Administrator Systemu Informatycznego nadzorujący przestrzeganie zasad bezpieczeństwa w systemie informatycznym.

c) do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez Administratora Danych,

d) prowadzona jest ewidencja osób upoważnionych do przetwarzania danych,

e) została opracowana i wdrożona polityka bezpieczeństwa,

f) została opracowana i wdrożona instrukcja zarządzania systemem informatycznym.

2) Środki ochrony fizycznej danych:

a) bazy danych osobowych przechowywane są w pomieszczeniach zabezpieczonych drzwiami zwykłymi wyposażonymi w minimum dwa zamki klasy B,

b) bazy danych osobowych przechowywane są w pomieszczeniach, w których okna zabezpieczone są za pomocą rolet antywłamaniowych,

c) pomieszczenia, w których przechowywane są bazy danych osobowych oraz pomieszczenia podlegającej szczególnej ochronie (§11 ust. 5), wyposażone są w system alarmowy przeciwwłamaniowy,

d) pomieszczenia, w których przechowywane są bazy danych osobowych oraz pomieszczenia podlegającej szczególnej ochronie (§11 ust. 5), objęte są systemem kontroli dostępu,

e) dostęp do pomieszczeń, w których przechowywane są bazy danych osobowych jest w czasie nieobecności zatrudnionych tam pracowników nadzorowany przez służbę ochrony,

f) kopie zapasowe/archiwalne baz danych osobowych przechowywane są w zamkniętej niemetalowej szafie – w zamkniętej kasecie posiadającej certyfikat producenta w zakresie odporności mechanicznej, wodnej i termicznej,

g) pomieszczenia, w których przechowywane są bazy danych osobowych zabezpieczone są przed skutkami pożaru za pomocą systemu przeciwpożarowego i/lub wolnostojącej gaśnicy,

h) dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.

3) Środki sprzętowe infrastruktury informatycznej i telekomunikacyjnej:

a) dostęp do bazy danych osobowych, która przetwarzana jest na wydzielonej stacji komputerowej/ komputerze przenośnym zabezpieczony został przed nieautoryzowanym uruchomieniem za pomocą hasła BIOS,

b) zastosowano urządzenia typu UPS, chroniące system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania,

c) dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła,

d) dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem karty procesorowej oraz kodu PIN lub tokena (dla komputerów spełniających warunki techniczne),

e) dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem technologii biometrycznej (dla komputerów spełniających warunki techniczne),

f) zastosowano środki uniemożliwiające wykonywanie nieautoryzowanych kopii danych osobowych przetwarzanych przy użyciu systemów informatycznych,

g) zastosowano system rejestracji dostępu do bazy danych osobowych,

h) zastosowano środki kryptograficznej ochrony danych dla danych osobowych przekazywanych drogą teletransmisji,

i) dostęp do środków teletransmisji zabezpieczono za pomocą mechanizmów uwierzytelnienia,

j) zastosowano macierz dyskową w celu ochrony danych osobowych przed skutkami awarii pamięci dyskowej,

k) zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity,

l) do ochrony dostępu do sieci komputerowej użyto sprzętowego systemu Firewall, IPS, AVG, - z aktualnymi licencjami producenta.

4) Środki ochrony w ramach narzędzi programowych i baz danych:

a) dostęp do Systemu Informatycznego Starostwa mają użytkownicy posiadający identyfikator i hasło dostępu nadane przez Administratora Systemu Informatycznego na podstawie upoważnienia wydanego przez Administratora Danych,

b) wykorzystano środki pozwalające na rejestrację zmian wykonywanych na poszczególnych elementach bazy danych osobowych,

c) zastosowano środki umożliwiające określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanej bazy danych osobowych,

d) dostęp do bazy danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła,

e) zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym baz danych osobowych dla poszczególnych użytkowników systemu informatycznego,

f) zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do Systemu Informatycznego Starostwa i aplikacji obsługujących bazy danych osobowych,

g) zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe,

h) zastosowano mechanizm automatycznej blokady dostępu do stanowiska komputerowego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.

5) Środki organizacyjne:

a) osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych,

b) przeszkolono osoby zatrudnione przy przetwarzaniu danych osobowych w zakresie zabezpieczeń systemu informatycznego,

c) osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy,

d) monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane,

e) kopie zapasowe baz danych osobowych przechowywane są w innym pomieszczeniu niż to, w którym znajduje się serwer, na którym dane osobowe przetwarzane są na bieżąco,

f) użycie komputerów przenośnych służących do przetwarzania danych osobowych poza terenem Starostwa jest możliwe tylko po uzyskaniu zgody Administratora Danych.

§ 14. Postępowanie w sytuacji naruszenia zasad ochrony danych osobowych

1. W razie stwierdzenia przez osobę zatrudnioną przy przetwarzaniu danych naruszenia zasad ich ochrony zobowiązana jest ona do:

1) Natychmiastowego powiadomienia o zdarzeniu swojego bezpośredniego przełożonego oraz Administratora Bezpieczeństwa Informacji.

2) Zabezpieczenia miejsce zdarzenia.

3) Fizycznego odłączenia urządzenia i segmentów sieci , które mogły umożliwić dostęp do zbiorów danych osobom nieupoważnionym.

2. W razie naruszenia ochrony zabezpieczenia danych osobowych przetwarzanych w systemie informatycznym Administrator Bezpieczeństwa Informacji wspólnie z Administratorem Systemu Informatycznego podejmują działania:

1) Wylogowania użytkownika podejrzanego o naruszenie zabezpieczenia ochrony danych.

2) Zmiany hasła na koncie użytkownika, poprzez które uzyskano nielegalny dostęp w celu uniknięcia ponownego włamania.

3) Zapisania wszelkich informacji związanych z danym zdarzeniem a szczególnie czas uzyskania informacji o naruszeniu zabezpieczenia danych osobowych lub czas samodzielnego wykrycia tego faktu.

4) Wygenerowania i wydrukowania (jeżeli zasoby systemu na to pozwalają) wszystkich możliwych dokumentów i raportów, które mogą pomóc w ustaleniu okoliczności zdarzenia. Należy opatrzyć je datą i podpisem.

5) Sprawdzenia:

a) stanu urządzeń wykorzystywanych do przetwarzania danych osobowych,

b) zawartości zbioru danych,

c) sposobu działania programu,

d) jakości komunikacji w sieci telekomunikacyjnej.

6) Wykluczenia możliwości obecności wirusów komputerowych.

7) Przystąpienia do zidentyfikowania rodzaju zaistniałego zdarzenia, zwłaszcza do określenia skali szkód i sposobu dostępu do danych osoby niepowołanej.

3. Administrator Bezpieczeństwa Informacji sporządza protokół ze stwierdzonego naruszenia ochrony danych osobowych zawierający w szczególności:

1) rodzaj zaistniałego zdarzenia,

2) dokładny czas uzyskania informacji o naruszeniu zabezpieczenia danych osobowych,

3) określenie sposobu naruszenia zabezpieczenia ochrony danych osobowych,

4) określenie ewentualnych szkód lub zniszczeń,

5) określenie przyczyny naruszenia danych osobowych.

4. Protokół sporządza się w terminie 14 dni od daty zaistnienia zdarzenia i przekazuje Administratorowi Danych.

§ 15. Załączniki do Polityki Bezpieczeństwa.

1. Wykaz zbiorów danych osobowych dla których administratorem jest Starosta Raciborski.

2. Wykaz dysponentów zbiorów danych osobowych.

3. Wykaz aplikacji do przetwarzania danych osobowych.

4. Wniosek o wydanie upoważnienia do przetwarzania danych osobowych i dostęp do Systemu Informatycznego Starostwa.

5. Upoważnienie do przetwarzania danych osobowych i dostęp do Systemu Informatycznego Starostwa.

6. Rejestr upoważnień do przetwarzania danych osobowych i dostępu do Systemu Informatycznego Starostwa.

7. Oświadczenie użytkownika o zapoznaniu się obowiązującymi w Starostwie przepisami w zakresie ochrony danych osobowych.

8. Poświadczenie szkolenia z zakresu ochrony danych osobowych.

Administrator
Bezpieczeństwa Informacji

Włodzimierz Gralak

STAROSTA

Ryszard Winiarski

WYKAZ ZBIORÓW DANYCH OSOBOWYCH
DLA KTÓRYCH ADMINISTRATOREM JEST STAROSTA
RACIBORSKI

Lp.	Nazwa zbioru danych osobowych Lokalizacje zbioru Opis struktury zbioru Uwagi	Forma przetwarzania zbioru danych osobowych		Program stosowany do przetwarzania danych Rodzaj bazy danych	Komórka organizacyjna odpowiedzialna za przetwarzanie danych osobowych w zbiorze danych	Zgłoszenie do GIODO Data Numer	Dysponent zbioru danych
		Informatyczna	Tradycyjna				
1.	**Nazwa zbioru danych** **Lokalizacje** ZBIÓR KARTOTEKOWY: BAZA INFORMATYCZNA : **Zakres danych przetwarzanych w zbiorze TRADYCYJNYM** **Zakres danych przetwarzanych w bazie INFORMATYCZNEJ**	TAK/NIE	TAK/NIE				Kierownik Referatu ...

Aktualny WYKAZ ZBIORÓW DANYCH OSOBOWYCH DLA KTÓRYCH ADMINISTRATOREM JEST STAROSTA RACIBORSKI znajduje się systemie elektronicznym Administratora Bezpieczeństwa Informacji.

Załącznik Nr 2
do Polityki Bezpieczeństwa

WYKAZ DYSPONENTÓW ZBIORÓW DANYCH OSOBOWYCH

Lp.	Nazwa zbioru danych	Dysponent	Stanowisko
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			
21			
22			
23			
24			
25			

Aktualny WYKAZ DYSPONENTÓW ZBIORÓW DANYCH OSOBOWYCH DLA KTÓRYCH ADMINISTRATOREM JEST STAROSTA RACIBORSKI znajduje się systemie elektronicznym Administratora Bezpieczeństwa Informacji

Załącznik Nr 3
do Polityki Bezpieczeństwa

WYKAZ APLIKACJI DO PRZETWARZANIA DANYCH OSOBOWYCH

Lp.	Nazwa aplikacji Wykaz modułów	Dysponent (Komórka organizacyjna)	Administrator aplikacji/modułu (Osoba, stanowisko)	Wymagany identyfikator i hasło użytkownika	Wymagane upoważnienie do przetwarzania
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					

Aktualny WYKAZ APLIKACJI DO PRZETWARZANIA DANYCH OSOBOWYCH
znajduje się systemie elektronicznym Administratora Bezpieczeństwa Informacji

WNIOSEK O WYDANIE UPOWAŻNIENIA
DO PRZETWARZANIA DANYCH OSOBOWYCH I DOSTĘP DO SYSTEMU INFORMATYCZNEGO

Aktualizacja upoważnienia nr
Wydanie upoważnienia do: - przetwarzania danych osobowych **X**
Wydanie upoważnienia do: - dostępu do systemu informatycznego **X**

Imię i nazwisko pracownika:
Komórka organizacyjna :
Stanowisko:

.....
Podpis wnioskującego

Dysponenci (Komórki organizacyjne):

Przetwarzanie danych osobowych
Pracownik

Lp.	Uzasadnienie potrzeby posiadania dostępu do zbioru danych osbowych Wypełnia bezpośredni przełożony								Opinia w sprawie celowości uzyskania dostępu do zbioru danych osobowych Wypełnia kierownik komórki organizacyjnej Starostwa odpowiedzialny za przetwarzanie danych osobowych w zbiorze danych			
	Nazwa zbioru danych osobowych	Rodzaj dostępu						Uzasadnienie	Komórka organizacyjna odpowiedzialna za przetwarzanie danych osobowych w zbiorze danych	Zgłoszenie do GIODO	Opinia	Podpis
		Oglądanie	Wprowadzanie	Edycja	Usuwanie	Wydruki	Administrator					
1.												
2.												
3.												
4.												
5.												
6.												
7.												

Dostęp do systemu informatycznego

Pracownik

Lp.	Uzasadnienie potrzeby posiadania dostępu Wypełnia bezpośredni przełożony								Opinia w sprawie celowości nadania hasła Wypełnia kierownik komórki organizacyjnej Starostwa/Dysponent programu		
	Wykaz programów, do których konieczne jest uzyskanie zgody na dostęp	Rodzaj dostępu						Uzasadnienie	Dysponent programu	Opinia	Podpis dysponenta
		Oglądanie	Wprowadzanie	Edycja	Usuwanie	Wydruki	Administrator				
1.											
2.											
3.											
4.											
5.											
6.											
7.											
8.											

U P O W A Ż N I E N I E Nr

z dnia

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tj. Dz. U. z 2016 r. poz. 922) w związku z § 6 ust. 1 pkt 1 Polityki Bezpieczeństwa, stanowiącej Załącznik nr 1 do Zarządzenia nr . . . . . Starosty Raciborskiego z dnia . . . . . oraz § 2 ust. 2 Instrukcji Zarządzania Systemem Informatycznym stanowiącej Załącznik nr 2 do ww. Zarządzenia

Aktualizacja upoważnienia nr:

Stanowisko:

Komórka organizacyjna:

Pan (i)

otrzymuje upoważnienie

I. do wykonywania operacji przetwarzania w zbiorach danych osobowych	O	W	E	U	W	A

O-oglądanie, W-wprowadzanie, E-edycja, U-usuwanie, W-wydruki, A-administracja

II. do wykonywania operacji przetwarzania w systemach informatycznych:	O	W	E	U	W	A

O-oglądanie, W-wprowadzanie, E-edycja, U-usuwanie, W-wydruki, A-administracja

Niniejsze upoważnienie ważne jest w czasie zatrudnienia w Starostwie Powiatowym w Raciborzu.
Upoważnienie aktualizowane utraciło ważność.
Upoważnienie nie może być przeniesione na inne osoby

. . . . . .
STAROSTA RACIBORSKI

Powyższe upoważnienie przyjmuję do wiadomości i ścisłego przestrzegania

Racibórz.....
/data i podpis upoważnionego/

Załącznik Nr 6
do Polityki Bezpieczeństwa

REJESTR UPOWAŻNIEŃ DO PRZETWARZANIA DANYCH OSOBOWYCH I DOSTĘPU DO SYSTEMÓW INFORMATYCZNYCH

UPOWAŻNIENIA AKTUALNE NA DZIEŃ:

Lp	Imię i nazwisko	Stanowisko Komórka organizacyjna Wydano upoważnienie do:	Numer upoważnienia	Data wydania	Data cofnięcia	Podstawa cofnięcia	Uwagi
1	2	3	4	5	6	7	8

Aktualny REJESTR UPOWAŻNIEŃ DO PRZETWARZANIA DANYCH OSOBOWYCH I DOSTĘPU DO SYSTEMÓW INFORMATYCZNYCH znajduje się systemie elektronicznym Administratora Bezpieczeństwa Informacji

Pracownik
Stanowisko
Komórka organizacyjna

Oświadczam, że zapoznałem się z obowiązującymi w Starostwie Powiatowym w Raciborzu zasadami ochrony danych osobowych określonych w Zarządzeniu . . . . . Starosty Raciborskiego z dnia . . . . . i zobowiązuję się do ich przestrzegania.

Oświadczam, że jestem świadomy odpowiedzialności karnej wynikającej z art. 49-54a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2016 r. poz. 922 z późn. zm.), a także art. 266 ustawy z dnia 6 czerwca 1997 r. Kodeks karny (t.j. Dz. U. z 2016. poz. 1137 z późn. zm.)

Racibórz, dn..... .....
czytelny podpis

Załącznik Nr 8
do Polityki Bezpieczeństwa

Pracownik
Stanowisko
Komórka organizacyjna

ZAŚWIADCZENIE

o szkoleniu z zakresu ochrony danych osobowych

Zaświadczam, że Pani . . . . . w dniu . . . . została przeszkolona z przepisów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tj. Dz. U. z 2016 r. poz.922 z późn. zm.), wraz z aktami wykonawczymi do niej i zapoznała się z przepisami o ochronie danych osobowych obowiązującymi w Starostwie Powiatowym w Raciborzu.

Prowadzący szkolenie

Data i podpis osoby szkolonej

Załącznik Nr 2 do Zarządzenia Nr 65/2017

Starosty Raciborskiego

z dnia 22 maja 2017 r.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

§ 1. Postanowienia Ogólne.

1. Instrukcja określa zasady oraz tryb postępowania przy przetwarzaniu danych w Systemie Informatycznym Starostwa, a w szczególności zapewnienie bezpieczeństwa przetwarzania danych osobowych.

2. Instrukcja opracowana została zgodnie z §3 ust.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 (Dz. U. Nr 100 poz. 1024)

3. Procedury i zasady zawarte w instrukcji powinny być bezwzględnie przestrzegane przez wszystkich użytkowników Systemu Informatycznego Starostwa w zakresie ich obowiązków i odpowiedzialności.

4. Przestrzeganie zasad i procedur zawartych w instrukcji ma na celu maksymalne zmniejszenie ryzyka utraty poufności i integralności danych przetwarzanych w Systemie Informatycznym Starostwa w zakresie zidentyfikowanych zagrożeń:

1) Włamania do Systemu Informatycznego Starostwa i pozyskania danych przez osoby nieuprawnione.

2) Pozyskania danych przez osoby nieuprawnione na skutek bezpośredniego dostępu do komputera.

3) Pozyskania danych osobowych przez osoby nieuprawnione w trakcie przesyłania ich siecią publiczną (INTERNET).

4) Dokonywania modyfikacji danych przez osoby nieuprawnione.

§ 2. Zarządzanie uprawnieniami do przetwarzania danych i rejestrowanie tych uprawnień w systemie informatycznym.

1. Zarządzanie uprawnieniami do przetwarzania danych w Systemie Informatycznym Starostwa obejmuje:

1) Przyznanie uprawnień.

2) Zmianę uprawnień.

3) Cofnięcie uprawnień.

4) Kontrolę wykorzystywania uprawnień w przyznanym zakresie.

2. Uprawnienia do przetwarzania danych nadawane są przez Starostę w formie upoważnienia, na podstawie wniosku kierownika komórki organizacyjnej zaakceptowanego przez dysponentów programów. Wzór wniosku stanowi załącznik nr 4 do Polityki Bezpieczeństwa. Wzór upoważnienia stanowi załącznik nr 5 do Polityki Bezpieczeństwa.

3. Rejestracja użytkownika w Systemie Informatycznym Starostwa polega na przydziale identyfikatorów i haseł dostępu do programów, zgodnie z zakresem upoważnienia.

4. Za przydział identyfikatora i hasła w usłudze Active Directory Systemu Informatycznego Starostwa odpowiedzialny jest Administrator Systemu Informatycznego.

5. Za przydział identyfikatorów i haseł dostępu do programów, zgodnie z zakresem upoważnienia odpowiedzialni są administratorzy tych programów.

6. Użytkownik jest wyrejestrowywany z Systemu Informatycznego Starostwa w każdym przypadku utraty przez niego uprawnień, szczególnie w sytuacji:

1) Ustania zatrudnienia w Starostwie.

2) Zmiany zakresu obowiązków.

3) Naruszenia zasad bezpieczeństwa przetwarzania danych.

7. Za wyrejestrowanie użytkownika z Systemu Informatycznego Starostwa odpowiedzialny jest Administrator Systemu.

8. Administrator Systemu Informatycznego otrzymuje informację o utracie uprawnień przez użytkownika na podstawie:

1) Karty obiegowej pracownika (o ustaniu zatrudnienia).

2) Informacji dysponenta programu.

3) Informacji Administratora Bezpieczeństwa Informacji o naruszeniu zasad bezpieczeństwa.

9. Uprawnienia dostępu do Systemu Informatycznego lub programu mogą być także odebrane lub zablokowane przez Administratora Systemu Informatycznego w razie stwierdzenia naruszenia zasad bezpieczeństwa przetwarzania danych.

10. Administrator Systemu Informatycznego prowadzi rejestr identyfikatorów użytkowników przechowywany w bazie usługi Active Directory.

11. Administrator Systemu Informatycznego sprawuje nadzór na wykorzystywaniem uprawnień użytkowników zgodnie z przyznanym zakresem.

12. Hasło Administratora Systemu Informatycznego jest zdeponowane u Kierownika Referatu Administracyjnego.

13. W przypadku awaryjnego użycia hasła Administratora Systemu Informatycznego, Kierownik Referatu Administracyjnego sporządza notatkę służbową do wiadomości Starosty i Administratora Systemu Informatycznego, który niezwłocznie dokonuje zmiany tego hasła.

§ 3. Metody i środki uwierzytelniania użytkowników.

1. Dostęp do Systemu Informatycznego Starostwa możliwy jest jedynie po uwierzytelnieniu użytkownika.

2. Uwierzytelnienie użytkownika odbywa się w usłudze Active Directory, która weryfikuje podany identyfikator i hasło ze wzorcem przechowywanym w jej bazie.

3. Uwierzytelnienie użytkownika jest możliwe na każdym stanowisku komputerowym w Systemie Informatycznym Starostwa.

4. Indywidualny identyfikator i hasło użytkownika muszą spełniać następujące zasady.

1) Identyfikator:

a) musi zapewniać rozliczalność, autentyczność i niezaprzeczalność użytkownika w Systemie Informatycznym Starostwa - być unikalnym i niepowtarzalnym dla każdego użytkownika,

b) nie może być wykorzystany ponownie i przyznany innemu użytkownikowi,

c) nie może być zmieniony bez wiedzy użytkownika,

d) użytkownik jest odpowiedzialny za wszystkie czynności wykonane przy użyciu jego identyfikatora,

2) Hasło:

a) jest znane wyłącznie osobie, do której należy związany z nim identyfikator,

b) pierwsze hasło użytkownika nadaje Administrator Systemu Informatycznego. Użytkownik po pierwszym zalogowaniu zmienia hasło wg zasad nadawania haseł.

c) hasło musi składać się z co najmniej 8 znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne,

d) hasło musi być zmieniane przez użytkownika co 30 dni,

e) hasło nie może zostać powtórzone w cyklu kolejnych 4 zmian.

5. Administrator Systemu Informatycznego przekazuje użytkownikowi nadany identyfikator i hasło w sposób zapewniający zachowanie poufności.

6. Po uwierzytelnieniu w Systemie Informatycznym Starostwa użytkownik nie może udostępniać innym osobom swojego stanowiska pracy.

7. Zabronione jest:

1) Przechowywanie identyfikatorów i haseł w sposób umożliwiający utratę poufności w szczególności zapisywanie i pozostawianie identyfikatorów i haseł w miejscach ogólnie dostępnych.

2) Przekazywanie lub udostępnianie identyfikatorów i haseł innym osobom.

3) Posługiwanie się identyfikatorem i hasłem innego użytkownika w ramach pełnionego zastępstwa.

8. W przypadku podejrzenia utraty poufności hasła należy je niezwłocznie zmienić, oraz powiadomić o tym fakcie Administratora Systemu Informatycznego.

9. W przypadku automatycznego wygaśnięcia, zablokowania lub zapomnienia hasła użytkownik zgłasza Administratorowi Systemu Informatycznego konieczność wprowadzenia nowego hasła. Użytkownik po otrzymaniu nowego hasła, zmienia je podczas pierwszego logowania.

§ 4. Zasady rozpoczęcia, zawieszenia i zakończenia pracy w systemie.

1. **Rozpoczęcie pracy na stanowisku komputerowym.**

1) Stanowisko komputerowe przekazywane użytkownikowi jest zabezpieczone identyfikatorem i hasłem Administratora Systemu Informatycznego.

2) Użytkownik otrzymuje od Administratora Systemu Informatycznego identyfikator i pierwsze hasło logowania.

3) W czasie pierwszego logowania użytkownik zmienia hasło zgodnie z zasadami określonymi w § 3 niniejszej Instrukcji.

4) Użytkownik loguje się do Systemu Informatycznego Starostwa na stanowisku komputerowym używając swojego identyfikatora i hasła.

5) W przypadku stwierdzenia, że logowanie jest niemożliwe z użyciem aktualnie obowiązującego hasła, użytkownik zawiadamia Administratora Systemu Informatycznego.

6) Podczas logowania należy zwracać szczególną uwagę na systemowe komunikaty informujące o konieczności zmiany hasła i stosować się do ich treści, a w razie wątpliwości poinformować Administratora Systemu Informatycznego.

7) Praca jednego użytkownika na kilku stanowiskach komputerowych równocześnie, z wykorzystaniem tego samego identyfikatora, jest dozwolona w uzasadnionych przypadkach wynikających z zakresu wykonywanych obowiązków.

8) W przypadku zauważenia przez użytkownika nietypowego zachowania w trakcie uruchamiania i pracy na stanowisku komputerowym (np.: pojawienie się nowych lub nietypowych komunikatów lub znacznego spowolnienie działania programów), użytkownik powinien natychmiast powiadomić o tym Administratora Systemu Informatycznego.

9) Monitor stanowiska komputerowego powinien być ustawiony w taki sposób, aby uniemożliwić wgląd w dane przebywającym w pomieszczeniu osobom nieupoważnionym.

10) Stanowisko komputerowe powinno zostać ustawione w taki sposób, aby osoby postronne miały utrudniony dostęp do portów zewnętrznych stacji roboczej (gniazda USB, napędy CD/DVD).

2. **Zawieszenie pracy na stanowisku komputerowym.**

1) Użytkownik, opuszczający czasowo stanowisko pracy, wylogowuje się, przez użycie karty do logowania lub kombinację klawiszy Windows+L.

2) W przypadku, gdy użytkownik planuje przerwać pracę na dłuższy okres lub zakończyć pracę - zobowiązany jest do wyłączenia stanowiska komputerowego oraz sprawdzenia, czy nie zostały niezabezpieczone przed nieuprawnionym dostępem nośniki (PENDRIVE, płyty CD/DVD) i wydruki zawierające dane osobowe.

3) Ekran stanowiska komputerowego wygasza się automatycznie po 15-tu minutach bezczynności użytkownika. Wznowienie pracy na stanowisku komputerowym jest możliwe po wprowadzeniu hasła użytkownika.

3. **Zakończenie pracy na stanowisku komputerowym.**

1) Użytkownik kończący pracę, przed wyłączeniem stanowiska komputerowego zamyka wszystkie używane programy.

2) Jeżeli stanowisko komputerowe nie wyłącza się automatycznie, należy wyłączyć go odpowiednim przyciskiem na obudowie oraz powiadomić o tym Administratora Systemu Informatycznego.

3) Należy zabezpieczyć przed nieuprawnionym dostępem używane w czasie pracy nośniki (PENDRIVE, płyty CD/DVD) i wydruki zawierające dane osobowe.

§ 5. Zasady pracy w systemie.

1. **Podczas pracy na stanowisku komputerowym niedozwolone jest:**

1) Uruchamianie i obsługa programów, do których użytkownik nie posiada upoważnienia.

2) Podejmowanie prób omijania mechanizmów zabezpieczeń i kontroli.

3) Testowanie zabezpieczeń pod kątem możliwości ich złamania.

4) Skanowanie urządzeń sieciowych, serwerów oraz stacji komputerowych pod kątem badania świadczonych usług.

5) Wyłączanie programów uruchamianych automatycznie przy starcie systemu.

6) Odinstalowywanie programów.

7) Podłączanie i użytkowanie prywatnego sprzętu, w tym używanie prywatnych nośników danych.

8) Podejmowanie jakichkolwiek prób ingerencji w sprzęt komputerowy, poza czynnościami związanymi z codzienną eksploatacją.

9) Przechowywanie w zasobie sieciowym udostępnionym użytkownikowi, dokumentów nie związanych z zakresem czynności (gier, filmów, obrazów, dźwięków).

10) Przenoszenie i przełączanie stanowisk komputerowych między stanowiskami pracy bez wiedzy Administratora Systemu Informatycznego.

11) Dopuszczanie do pracy na stanowisku komputerowym osób postronnych.

12) Kopiowanie i przechowywanie na stanowisku komputerowym lub nośnikach zewnętrznych baz danych osobowych, za wyjątkiem czynności udostępniania danych osobowych podmiotom uprawnionym.

2. **Zasady korzystania z sieci publicznej.**

1) Stanowiska komputerowe użytkowników Systemu Informatycznego Starostwa mają stały dostęp do sieci publicznej (INTERNET).

2) Ze względu na wymóg stosowania wysokiego poziomu bezpieczeństwa teleinformatycznego, wszystkie połączenia z siecią publiczną są rejestrowane i zapisywane w bazie danych urządzenia monitorującego pracę sieci Starostwa.

3) Użytkownicy Systemu Informatycznego Starostwa korzystają z dostępu do sieci publicznej zgodnie ze swoim zakresem czynności.

4) Strony WWW mogące być źródłem ataków lub szkodliwego oprogramowania są niedostępne dla użytkowników Systemu Informatycznego Starostwa.

5) Administrator Systemu Informatycznego blokuje kategorie stron WWW kierując się zapisami Polityki Bezpieczeństwa i niniejszej Instrukcji, a także własną wiedzą z zakresu bezpieczeństwa teleinformatycznego. Wykaz kategorii stron WWW znajduje się w Załączniku nr 5 do Instrukcji Zarządzania Systemem Informatycznym.

6) Użytkownicy Systemu Informatycznego Starostwa nie mają dostępu między innymi do: portali społecznościowych, komunikatorów internetowych, prywatnych serwisów bankowych, portali multimedialnych, zakupów i aukcji internetowych. W uzasadnionych przypadkach, niezbędnych do realizacji czynności służbowych, kierownik komórki organizacyjnej może wnioskować o nadanie użytkownikowi dodatkowych uprawnień dostępu do sieci publicznej.

7) O zablokowaniu dostępu do strony WWW niezbędnej do wykonywania czynności służbowych, użytkownik informuje Administratora Systemu Informatycznego, podając pełny adres zablokowanej strony. Jeżeli dostęp został zablokowany przypadkowo, to po pozytywnej weryfikacji zawartości strony WWW, Administrator Systemu Informatycznego odblokowuje ją. W przypadkach wątpliwych, o odblokowaniu strony WWW decyduje bezpośredni przełożony użytkownika. Administrator Systemu Informatycznego może odmówić odblokowania strony WWW, jeżeli w wyniku tego obniżyłby się poziom bezpieczeństwa Systemu Informatycznego Starostwa.

8) Zdalny dostęp do Systemu Informatycznego Starostwa z sieci publicznej, a w szczególności do programów służących do przetwarzania danych osobowych jest możliwy jedynie przy zastosowaniu technicznych zabezpieczeń zapewniających rozliczalność, autentyczność i niezaprzeczalność osób, a także integralność i poufność przetwarzanych danych. Dostęp realizowany jest przy wykorzystaniu szyfrowanych protokołów transmisji danych.

9) Dostęp do Systemu Informatycznego Starostwa z sieci publicznej jest możliwy dla osób i podmiotów do tego uprawnionych, i dotyczy to następujących sytuacji:

a) Świadczenia serwisu zdalnego

- dostęp w ramach zawartych umów dotyczących serwisu oprogramowania zainstalowanego w Starostwie - na czas trwania umowy. Zasady dostępu do danych osobowych precyzuje zawarta dodatkowo umowa powierzenia przetwarzania danych osobowych pomiędzy Administratorem Danych w Starostwie a podmiotem, który świadczy usługi serwisowe,
- dostęp jest możliwy wyłącznie na czas wykonywania prac serwisowych i jest blokowany po ich zakończeniu,
- dostęp polegający na zdalnej kontroli pulpitu użytkownika jest możliwy tylko za pomocą licencjonowanych narzędzi programowych zapewniających szyfrowanie transmisji i uruchamiany jest każdorazowo przez Administratora Systemu Informatycznego na czas serwisu.

b) Wykonywania czynności kontrolnych, konserwacyjnych, diagnostycznych oraz naprawczych przez Administratora Systemu Informatycznego.

c) Udostępniania internetowego serwisu mapowego (GEOPORTAL)

- w trybie publicznym - bez możliwości przetwarzania danych osobowych,
- dla klientów Wydziału Geodezji - bez możliwości przetwarzania danych osobowych. Z zapewnieniem rozliczalności, autentyczności i niezaprzeczalności.
- dla służb i jednostek Powiatu Raciborskiego na podstawie umów powierzenia przetwarzania danych osobowych - możliwość przetwarzania danych osobowych. Z zapewnieniem rozliczalności, autentyczności i niezaprzeczalności. Dostęp wyłącznie z potwierdzonej lokalizacji.

10) Administratorzy aplikacji znajdujących się w innej lokalizacji niż System Informatyczny Starostwa (np. w sieci publicznej), zobowiązani są do przekazania wszystkich identyfikatorów użytkowników tej aplikacji Administratorowi Systemu Informatycznego Starostwa.

11) Aplikacje do przetwarzania baz danych osobowych znajdujących się w innej lokalizacji niż sieć Systemu Informatycznego Starostwa, mogą być obsługiwane wyłącznie z sieci systemu informatycznego o poziomie bezpieczeństwa teleinformatycznego nie niższym niż w Starostwie.

12) Administrator Systemu Informatycznego może ograniczyć lub zablokować dostęp do sieci publicznej użytkownikowi nie przestrzegającemu zasad Polityki Bezpieczeństwa i niniejszej Instrukcji.

13) W przypadku wykrycia zagrożenia bezpieczeństwa Systemu Informatycznego Starostwa spowodowanego nieprawidłowym korzystaniem z sieci publicznej przez pracownika, Administrator Systemu Informatycznego zgłasza zagrożenie bezpośredniemu przełożonemu pracownika, blokuje dostęp do sieci publicznej oraz informuje pracownika o ograniczeniu lub zablokowaniu dostępu do sieci publicznej.

3. **Zasady używania urządzeń mobilnych.**

1) Użytkownicy urządzeń mobilnych odpowiadają za ich ochronę fizyczną w czasie wykorzystywania poza terenem Starostwa.

2) Utratę urządzenia należy niezwłocznie zgłosić Kierownikowi Referatu Administracyjnego.

3) Urządzenie nie może być udostępniane osobom nieuprawnionym.

4) Administrator Systemu Informatycznego przekazuje użytkownikowi urządzenia mobilnego hasło dostępu do zaszyfrowanego dysku twardego. Użytkownik nie ma uprawnień do zmiany tego hasła.

5) Znajdujące się na dysku twardym urządzenia mobilnego pliki zawierające dane osobowe, należy zaszyfrować i opatrzyć hasłem dostępu.

6) Podłączanie urządzeń mobilnych, nie będących własnością Starostwa, do Systemu Informatycznego Starostwa jest możliwe jedynie za zgodą Administratora Systemu Informatycznego.

4. **Zasady postępowania z wydrukami komputerowymi.**

1) Wytwarzanie, powielanie, niszczenie wydruków komputerowych zawierających dane osobowe może być wykonywane jedynie przez osoby posiadające upoważnienie do przetwarzania tych danych.

2) Wydruki komputerowe zawierające dane osobowe należy przechowywać w miejscu uniemożliwiającym bezpośredni dostęp osobom nieupoważnionym.

3) Niewykorzystane wydruki komputerowe, zawierające dane osobowe, należy zniszczyć w taki sposób aby identyfikacja tych danych była niemożliwa.

4) Wydruki komputerowe znalezione na terenie Starostwa w miejscach ogólnie dostępnych (np. klatki schodowe, korytarze, kosze na śmieci, pojemniki na makulaturę, niszczarki dokumentów), powinny zostać zabezpieczone i przekazane Kierownikowi Referatu Administracyjnego.

5. **Zasady korzystania z sieci bezprzewodowej.**

1) W Systemie Informatycznym Starostwa są wykorzystywane urządzenia mobilne pracujące w sieci bezprzewodowej (WLAN).

2) Poziom bezpieczeństwa teleinformatycznego w sieci WLAN jest taki sam jak w sieci przewodowej (LAN).

3) Do sieci WLAN mogą uzyskać dostęp wyłącznie urządzenia Systemu Informatycznego Starostwa.

4) Połączenia z sieci WLAN do LAN obsługiwane są przy wykorzystaniu bezpiecznych, szyfrowanych protokołów transmisji.

5) Na terenie Starostwa funkcjonuje ogólnodostępna sieć bezprzewodowa (HOTSPOT), zapewniająca połączenie z siecią publiczną dla:

   a) klientów Starostwa,

   b) uczestników szkoleń, konferencji, narad itp. spotkań organizowanych na terenie Starostwa,

   c) uczestników komisji i sesji Rady Powiatu Raciborskiego.

6) Sieć HOTSPOT nie wchodzi w skład Systemu Informatycznego Starostwa.

7) Nie ma możliwości dostępu do sieci LAN i WLAN z sieci HOTSPOT.

6. **Zasady korzystania z poczty elektronicznej.**

1) Urzędowa poczta elektroniczna Starostwa znajduje się w domenie internetowej powiatraciborski.pl.

2) Poczta elektroniczna służy do komunikacji wewnętrznej w Starostwie oraz komunikacji pomiędzy Starostwem a klientami zewnętrznymi, w zakresie wykonywania czynności służbowych.

4) Potrzebę utworzenia nowego adresu poczty elektronicznej (konta pocztowego), kierownik komórki organizacyjnej Starostwa zgłasza Administratorowi Systemu Informatycznego. Wzór wniosku stanowi Załącznik nr 1 do Instrukcji Zarządzania Systemem Informatycznym. Po pozytywnym zweryfikowaniu warunków technicznych, Administrator Systemu Informatycznego zakłada na serwerze poczty nowe konto.

5) Dysponentami kont pocztowych dla komórek organizacyjnych Starostwa i imiennych kont pocztowych zatrudnionych w nich pracowników, są kierownicy tych komórek.

6) Do kont pocztowych komórek organizacyjnych Starostwa upoważnionymi mogą być pracownicy po pozytywnym zaopiniowaniu przez dysponenta.

7) Hasło do kont pocztowych komórek organizacyjnych Starostwa przechowuje Administrator Systemu Informatycznego.

8) Do imiennych kont pocztowych pracowników upoważnionymi mogą być inne osoby wyłącznie w zastępstwie, na czas nieobecności pracownika.

9) Każde konto pocztowe domeny powiatraciborski.pl posiada użytkownika upoważnionego do jego obsługi.

10) Użytkownik konta pocztowego:

   a) odpowiada za treść wysyłanych z tego konta wiadomości,

   b) odpowiada za treść otrzymywanych wiadomości:

      - powinien zwracać szczególną uwagę na wiadomości nieznanego pochodzenia mogące stwarzać zagrożenie bezpieczeństwa,

- powinien przekazywać do właściwego adresata wiadomości przeznaczone dla innej komórki organizacyjnej lub osoby,
- powinien przekazywać do Kierownika Referatu Administracyjnego wiadomości zagrożenia bezpieczeństwa,

c) zmienia hasło do konta pocztowego nie rzadziej niż raz na kwartał.

11) Administrator Systemu Informatycznego konfiguruje na stanowisku komputerowym użytkownika konto pocztowe, w programie do obsługi poczty elektronicznej.

12) Użytkownik konta pocztowego nie może w programie do obsługi poczty zmieniać konfiguracji konta, usuwać i dodawać inne konta pocztowe.

13) W przypadku wykrycia zagrożenia bezpieczeństwa Systemu Informatycznego Starostwa ze strony konta poczty elektronicznej, Administrator Systemu Informatycznego:

a) blokuje dostęp do zagrożonego konta,

b) informuje dysponenta konta o zaistniałym incydencie,

c) zabezpiecza wiadomości poczty elektronicznej dla zagrożonego konta na stanowiskach komputerowych użytkowników i na serwerze pocztowym ,

d) zabezpiecza logi systemów operacyjnych na zagrożonych stanowiskach komputerowych,

e) zabezpiecza logi połączeń z siecią publiczną dla zagrożonych stanowisk komputerowych,

f) analizuje incydent i wprowadza zabezpieczenia minimalizujące jego powtórne wystąpienie,

g) informuje Kierownika Referatu Administracyjnego - jeżeli incydent spowodowany został przez zamierzone działanie osób trzecich.

14) Użytkownicy Systemu Informatycznego Starostwa nie mają praw dostępu do portali poczty elektronicznej w sieci publicznej. W uzasadnionych przypadkach, niezbędnych do realizacji czynności służbowych, kierownik komórki organizacyjnej może wnioskować o nadanie użytkownikowi dodatkowych uprawnień dostępu do sieci publicznej.

15) Przekazywanie za pomocą poczty elektronicznej wiadomości zawierających dane osobowe jest możliwe w przypadku gdy:

a) odbiorcy wiadomości są upoważnieni do ich przetwarzania przez Administratora Danych w Starostwie,

b) odbiorcy wiadomości są upoważnieni do ich przetwarzania w związku z realizacją umowy powierzenia przetwarzania danych,

c) dane osobowe zostały zaszyfrowane, a klucz (hasło) jest przekazywany w inny, bezpieczny sposób.

16) Administrator Systemu Informatycznego prowadzi rejestr kont pocztowych domeny powiatraciborski.pl i użytkowników upoważnionych do ich obsługi. Załącznik nr 2 do Instrukcji Zarządzania Systemem Informatycznym.

17) Obsługa kont pocztowych domeny powiatraciborski.pl odbywa się przez szyfrowane połączenie do strony http s://webmail.powiatraciborski.pl

§ 6. Zasady tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania.

1. Kopie zapasowe zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania wykonywane są w celu zachowania ciągłości działania Systemu Informatycznego w Starostwie.

2. Za wykonywanie, przechowywanie i testowanie poprawności kopii zapasowych odpowiada Administrator Systemu Informatycznego.

3. Kopie zapasowe zbiorów danych i danych użytkowników

1) przetwarzanych na serwerach baz danych i zasobach sieciowych udostępnionych użytkownikom - wykonywane są przez Administratora Systemu Informatycznego według ustalonego harmonogramu jako kopie codzienne, tygodniowe i miesięczne. Załącznik nr 3 do Instrukcji Zarządzania Systemem Informatycznym.

2) przetwarzanych na stanowiskach komputerowych użytkowników - wykonują użytkownicy przez przekopiowanie do zasobu sieciowego.

4. Kopie zapasowe oprogramowania systemowego

1) zainstalowanego na serwerach - przechowywane są w formie nośników instalacyjnych wraz z aktualizacjami. Administrator Systemu Informatycznego po każdej istotnej zmianie w systemie wykonuje kopię jako obraz całego systemu.

2) zainstalowanego na stanowiskach komputerowych - przechowywane są w formie nośników instalacyjnych wraz z aktualizacjami. Administrator Systemu Informatycznego przed przekazaniem stanowiska użytkownikowi wykonuje kopię jako obraz całego systemu.

5. Kopie zapasowe wykonane na nośnikach zewnętrznych przechowywane są w zamkniętej niemetalowej szafie, w kasecie posiadającej certyfikat producenta w zakresie odporności mechanicznej, wodnej i termicznej, w kancelarii Starostwa (budynek B, Plac Okrzei 4 - parter, pok. nr 21)

6. W celu zweryfikowania poprawności wykonania kopii zapasowych Administrator Systemu Informatycznego wykonuje testy odtwarzania danych z kopii zgodnie harmonogramem. Załącznik nr 4 do Instrukcji Zarządzania Systemem Informatycznym.

7. Administrator Systemu Informatycznego prowadzi dokumentację dotyczącą wykonywania, przechowywania i testowania kopii zapasowych.

§ 7. Zasady wykorzystywania nośników informacji zawierających dane osobowe.

1. Jako elektroniczne nośniki informacji do przetwarzania danych osobowych w Starostwie wykorzystane są:

1) Pamięci masowe (dyski twarde) serwerów baz danych, serwerów plików i serwerów kopii zapasowych.

2) Sieciowe macierze dyskowe.

3) Pamięci masowe zewnętrze do przechowywania kopii zapasowych.

4) Płyty CD lub DVD.

2. Jako elektroniczne nośniki do przetwarzania danych osobowych nie mogą być wykorzystywane urządzenia przenośne typu PENDRIVE.

3. Płyty CD lub DVD mogą być wykorzystywane do przekazywania udostępnianych danych osobowych uprawnionym podmiotom lub osobom po zaszyfrowaniu i opatrzeniu hasłem.

4. Wszystkie nośniki zawierające kopie zapasowe są ewidencjonowane i jednoznacznie oznaczone.

5. Czas użytkowania nośników informacji przeznaczonych na kopie zapasowe, określa Administrator Systemu Informatycznego na podstawie analizy sprawności danego nośnika.

6. Nie wykorzystywane lub uszkodzone nośniki informacji zawierające dane osobowe, komórki organizacyjne Starostwa przekazują do Administratora Systemu Informatycznego.

7. Nośniki informacji przeznaczone do likwidacji są pozbawione zapisanych danych w sposób uniemożliwiający ich odzyskanie a następnie niszczone mechanicznie.

8. W urządzeniach wycofywanych z użytkowania w Starostwie, a przeznaczonych do wykorzystania przez inne podmioty, nośniki informacji są pozbawiane zapisów w sposób trwały, uniemożliwiający ich późniejsze odczytanie lub odtworzenie , za pomocą specjalistycznego oprogramowania.

9. Naprawa urządzeń z nośnikami informacji zawierającymi dane osobowe jest wykonywana w siedzibie Starostwa w asyście Administratora Systemu Informatycznego, a jeżeli urządzenie musi być naprawione w serwisie zewnętrznym - przekazywane jest bez nośników informacji.

10. Administrator Systemu Informatycznego prowadzi dokumentację dotyczącą likwidacji wycofanych z użytkowania nośników informacji która zawiera:

a) pochodzenie nośnika,

b) opis zawartości nośnika,

c) powód likwidacji,

d) metodę likwidacji,

e) datę likwidacji.

§ 8. Zabezpieczenia systemu informatycznego

1. W celu zabezpieczenia Systemu Informatycznego Starostwa przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu, zastosowano następujące środki bezpieczeństwa:

1) Mechanizm wymuszający okresową zmianę haseł dostępu.

2) Mechanizm uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.

3) Mechanizmy pozwalające na określenie odpowiednich praw dostępu do zasobów serwerów, w tym zbiorów danych osobowych dla poszczególnych użytkowników Systemu Informatycznego Starostwa.

4) Mechanizm automatycznego wygaszania ekranów na stanowiskach komputerowych po upływie 15 min bezczynności.

5) Mechanizm wymuszający ponowne zalogowanie do systemu po wznowieniu pracy na stanowisku komputerowym.

6) Mechanizm wymuszający naciśnięcie sekwencji klawiszy ctrl+alt+del przed zalogowaniem na stanowisku komputerowym.

7) Centralnie zarządzany system antywirusowy pozwalający monitorować stan oprogramowania antywirusowego na stanowiskach komputerowych.

8) Regularne skanowanie stanowisk komputerowych programem antywirusowym zgodnie z harmonogramem.

9) Na serwerach i stanowiskach komputerowych użytkowników zainstalowane są wyłącznie programy spełniające wymogi legalności.

10) Monitorowanie stanowisk komputerowych użytkowników pod kątem legalności oprogramowania.

11) Mechanizm wymuszający skanowanie zewnętrznych nośników informacji na obecność wirusów i innego szkodliwego oprogramowania przed ich użyciem na stanowisku komputerowym.

12) Mechanizmy monitorujące aktywność użytkowników w sieci publicznej.

13) Zablokowanie dostępu do kategorii stron internetowych, które mogą wpływać na obniżenie poziomu bezpieczeństwa przetwarzania danych w Systemie Informatycznym Starostwa.

2. Zabezpieczenie infrastruktury informatycznej i telekomunikacyjnej w Starostwie realizowane jest przez:

1) Kontrolę dostępu do pomieszczeń serwerowni.

2) Zabezpieczenia przed skutkami awarii zasilania (UPS) dla serwerów i pozostałych kluczowych elementów systemu.

3) Autonomiczne klimatyzatory w pomieszczeniach serwerowni.

3. System Informatyczny Starostwa jest chroniony przed zagrożeniami pochodzącymi z sieci publicznej przez wdrożenie fizycznych i logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem.

4. Zabezpieczenie Systemu Informatycznego Starostwa przed zagrożeniami pochodzącymi z sieci publiczne realizowane jest przez:

1) Blokowanie nieuprawnionego dostępu do sieci Starostwa z sieci publicznej.

2) Ustalenie reguł zdalnego serwisu użytkowanych w Starostwie programów.

3) Ograniczenie kategorii dostępnych stron WWW.

4) Kontrolę antywirusową odwiedzanych stron WWW.

5) Ewidencję wszystkich połączeń z siecią publiczną.

6) Kontrolę antywirusową treści informacji przekazywanych do i z sieci publicznej.

7) Zastosowanie mechanizmów alarmujących o naruszeniu bezpieczeństwa sieci.

8) Generowanie okresowych raportów o wykorzystaniu dostępu do sieci publicznej.

§ 9. Ochrona systemu przed szkodliwym oprogramowaniem.

1. W celu zabezpieczenia Systemu Informatycznego Starostwa przed szkodliwym oprogramowaniem jest wdrożony i stosowany system antywirusowy.

2. Ochrona antywirusowa obejmuje wszystkie stanowiska komputerowe oraz serwery działające w Systemie Informatycznym Starostwa.

3. Oprogramowanie antywirusowe zapewnia:

1) Automatyczne usuwanie wirusów, zaś w przypadku gdy ich usunięcie jest niemożliwe, przekazywanie zainfekowanych obiektów do kwarantanny.

2) Skanowanie wszystkich stanowisk komputerowych nie rzadziej niż raz w miesiącu.

3) Sporządzanie raportów i powiadamianie użytkowników i Administratora Systemu Informatycznego o wykryciu szkodliwego oprogramowania.

4) Zarządzanie przez zdalną konsolę administracyjną ustawieniami systemu antywirusowego na stanowiskach komputerowych użytkowników.

5) Automatyczną aktualizację definicji baz wirusów na stanowiskach komputerowych użytkowników.

4. Za wdrożenie i prawidłowe działanie systemu antywirusowego, oraz obsługę incydentów bezpieczeństwa związanych z działaniem szkodliwego oprogramowania odpowiada Administrator Systemu Informatycznego.

5. Po wykryciu działania szkodliwego oprogramowania na stanowisku komputerowym użytkownika Administrator Systemu Informatycznego:

1) Blokuje dostęp do zagrożonego stanowiska komputerowego.

2) Informuje kierownika komórki organizacyjnej użytkownika o zaistniałym incydencie.

3) Zabezpiecza logi systemu operacyjnego na zainfekowanym stanowisku komputerowym.

4) Zabezpiecza logi połączeń z siecią publiczną zainfekowanego stanowiska komputerowego.

5) Przywraca stanowisko komputerowe do stanu z przed incydentu.

6) Analizuje incydent i wprowadza zabezpieczenia minimalizujące jego powtórne wystąpienie.

7) Informuje Kierownika Referatu Administracyjnego - jeżeli incydent spowodowany został przez zamierzone działanie osób trzecich.

6. Administrator Systemu Informatycznego rejestruje wszystkie przypadki obniżenia poziomu bezpieczeństwa spowodowane przez działanie szkodliwego oprogramowania w dzienniku administratora.

7. Opis incydentu bezpieczeństwa spowodowanego przez szkodliwe oprogramowanie zawiera:

1) Identyfikator stanowiska komputerowego (numer IP i numer inwentarzowy), na którym wykryte zostało szkodliwe oprogramowanie.

2) Dokładaną datę i czas wykrycia.

3) Rodzaj wykrytego wirusa lub innego oprogramowania;

4) Podjętej akcji naprawczej mającej na celu przywrócenie właściwego poziomu bezpieczeństwa.

8. **Zasady postępowania w celu ochrony przed szkodliwym oprogramowaniem.**

1) Użytkownicy zgłaszają Administratorowi Systemu Informatycznego wszelkie nieprawidłowości w działaniu stanowiska komputerowego, mogące wskazywać na zainfekowanie szkodliwym oprogramowaniem (uruchamianie się nieznanych wcześniej programów, pojawianie się nieznanych komunikatów, spowolnienie działania systemu).

2) Wiadomości poczty elektronicznej od nieznanego nadawcy o treści mogącej wskazywać na próbę wyłudzenia informacji są usuwane bez próby otwierania załączników i linków .

3) Przenośne nośniki informacji są skanowane programem antywirusowym przed każdym użyciem.

4) Niedozwolone jest wyłączanie, blokowanie, odinstalowywanie z miana parametrów oprogramowania chroniącego stanowisko komputerowe przed szkodliwym oprogramowaniem.

§ 10. Przeglądy, konserwacja, naprawy i utylizacja.

1. Przeglądy, konserwacja, naprawy oraz utylizacja sprzętu komputerowego przeprowadzane są w sposób uniemożliwiający dostęp do danych osobowych osobom nieuprawnionym.

2. Wszelkie prace konserwacyjne i naprawy sprzętu komputerowego oraz uaktualnienia całości lub części Systemu Informatycznego Starostwa, które wykonuje podmiot zewnętrzny, odbywają się zgodnie z zapisami umowy pomiędzy tym podmiotem i Starostwem, zawierającej regulacje dotyczące ochrony danych osobowych.

4. Naprawy wykonywane w trybie awaryjnym przez inne osoby lub podmioty, wykonywane są pod nadzorem Administratora Systemu Informatycznego.

3. Nośniki zawierające dane osobowe, które uległy uszkodzeniu, przekazywane są do naprawy jedynie w przypadku konieczności odzyskania z nich danych.

5. Za przeglądy, konserwacje, naprawy i utylizację sprzętu komputerowego odpowiada Administrator Systemu Informatycznego.

6. Administrator Systemu Informatycznego opisuje w swoim dzienniku wykonane czynności.

§ 11. Załączniki do Instrukcji.

1. Zgłoszenie nowego konta poczty elektronicznej.
2. Wykaz użytkowników poczty elektronicznej.
3. Harmonogram wykonywania kopii danych i programów.
4. Harmonogram odtworzeń testowych kopii danych.
5. Wykaz kategorii stron internetowych.

Administrator
Bezpieczeństwa Informacji

Włodzimierz Gralak

STAROSTA

Ryszard Winiarski

Załącznik Nr 1
do Instrukcji Zarządzania
Systemem Informatycznym

ZGŁOSZENIE NOWEGO KONTA POCZTY ELEKTRONICZNEJ

Komórka organizacyjna: . . . . . .

Nazwa konta: . . . . . @powiatraciborski.pl

Wielkość skrzynki: . . . . . MB

. . . . . .

Data i podpis

Załącznik Nr 2
do Instrukcji Zarządzania
Systemem Informatycznym

WYKAZ UŻYTKOWNIKÓW POCZTY ELEKTRONICZNEJ

Lp.	Nazwa konta pocztowego	Uprawnieni użytkownicy
1.		
2.		
3		
4.		
5.		
6.		
7.		
8.		
9.		
10.		
11.		
12.		
13.		
14.		
15.		
16.		
17.		
18.		
19.		
20.		

Aktualny WYKAZ UŻYTKOWNIKÓW POCZTY ELEKTRONICZNEJ
znajduje się systemie elektronicznym Administratora Bezpieczeństwa Informacji

Racibórz, dnia 01.03.2017

Kopia na dysk zewnętrzny, sieciowy oraz Rdx za miesiąc Marzec

DATA			PODPIS	Stan kopii : ew. opis
1	Marzec	Środa		
2	Marzec	Czwartek		
3	Marzec	Piątek		
4	Marzec	Sobota		
5	Marzec	Niedziela		
6	Marzec	Poniedziałek		
7	Marzec	Wtorek		
8	Marzec	Środa		
9	Marzec	Czwartek		
10	Marzec	Piątek		
11	Marzec	Sobota		
12	Marzec	Niedziela		
13	Marzec	Poniedziałek		
14	Marzec	Wtorek		
15	Marzec	Środa		
16	Marzec	Czwartek		
17	Marzec	Piątek		
18	Marzec	Sobota		
19	Marzec	Niedziela		
20	Marzec	Poniedziałek		
21	Marzec	Wtorek		
22	Marzec	Środa		
23	Marzec	Czwartek		
24	Marzec	Piątek		
25	Marzec	Sobota		
26	Marzec	Niedziela		
27	Marzec	Poniedziałek		
28	Marzec	Wtorek		
29	Marzec	Środa		
30	Marzec	Czwartek		
31	Marzec	Piątek		
		Data\Podpis:		

Stan kopii : poprawna ✓
niepoprawna X

Harmonogram odtworzeń testowych kopii danych w roku 2017

Lp.	Nazwa programu	Dysp.	Administrator aplikacji	Opis	Harmonogram kopii	Harmonogram weryfikacji przez próbne odtworzenie danych			
						I kw 2017	II kw 2017	III kw 2017	IV kw 2017
1	BIULETYN INFORMACJI PUBLICZNEJ	TO	Karolina Kunicka	Kopia wykonywana przez INTRACOM - zgodnie z umową na obsługę BIP	codziennie. Kopia przekazywana do starostwa na nośnikach zewnętrznych (płyta DVD) 1x w miesiącu.				
2	STRONA INTERNETOWA POWIATRACIBORSKI.PL	TO	Karolina Kunicka	Kopia wykonywana przez INTRACOM - zgodnie z umową.	codziennie				
3	EDYTOR AKTÓW PRAWNYCH XML	TO	Ewa Mekeresz	Baza aktów prawnych XML na serwerze Starostwa	codziennie		13.06.2017		13.12.2017
4	BESTI@ - ZARZĄDZANIE BUDŻETEM	TF	Gabriela Gieda	Baza MSSQL dokumentów budżetowych na serwerze starostwa.	codziennie	23.03.2017		13.09.2017	
5	URZĄD (Efekt)	TF	Gabriela Gieda	Archiwalne systemy finansowo-księgowe i kadrowo-płacowe	Z uwagi na zakończenie użytkoania systemu, kopia jest przechowywana na nośnikach zewnętrznych (płyty DVD)				
6	URZĄD NT (Sygnity)	TF	Gabriela Gieda	Archiwalne systemy finansowo-księgowe	Z uwagi na zakończenie użytkoania systemu, kopia jest przechowywana na nośnikach zewnętrznych (płyty DVD)				
7	ŚRODKI TRWAŁE - EST (Arisco)	TF	Aniela Pełechata	Baza na serwerze starostwa	codziennie		13.06.2017		
8	WYPOSAŻENIE - KEW (Arisco)	TF	Aniela Pełechata	Baza na serwerze starostwa	codziennie				
9	STOWARZYSZENIA - RESTO (Arisco)	TO	Ewa Kwiatkowska	Baza na serwerze starostwa	codziennie				13.12.2017
10	ESTIMA - REJESTR	SA	Andrzej Skora	Baza na serwerze starostwa	codziennie		13.06.2017		
11	PŁATNIK ZUS	TF	Urszula Solich	Baza MSSQL na serwerze starostwa	codziennie			13.09.2017	
12	POCZTA ELEKTRONICZNA E-mail	TO	Mariusz Szramek	Na stanowiskach użytkowników.	Nie podlega archiwizacji.				
13	BAZA DANYCH NA SERWERZE STAROSTWA POWIATOWEGO	**	Włodzimierz Gralak	Baza dokumentów użytkowników w ramach wydziałów i referatów, na serwerze starostwa	codziennie		13.06.2017		13.12.2017
14	RATUSZ - REKORD	TF	Gabriela Gieda	System finansowo-księgowy. Baza na serwerze starostwa	codziennie. Kopia skonfigurowana i zweryfikowana przez producenta oprogramowania REKORD SA	23.03.2017			
15	R2PŁATNIKPro	TO	Alina Rutkowska	System kadrowo-płacowy. Baza MSSQL na serwerze starostwa	codziennie	23.03.2017		13.09.2017	
16	CEPIK - Centralna Ewidencja Pojzadów i Kierowców	SK	Grażyna Kowalska	Baza na serwerze MSW. Kopia systemu skonfigurowana i weryfikowana przez obsługę zewnętrzną HP-Polska , zgodnie z umową z MSW.	codziennie				
17	TRANSPORT DROGOWY	SK	Rajmund Ignacy	Baza na serwerze starostwa	codziennie	23.03.2017		13.09.2017	
18	GEODEZJA-SYGNITY	SG	Piotr Blochel	Baza na serwerze starostwa. Kopia systemu skonfigurowana i weryfikowana przez SYGNITY SA, zgodnie z umową.	codziennie				
	GEODEZJA-GEOBID	SG	Piotr Blochel	Baza i aplikacje na serwerze starostwa. Kopia systemu wykonywana tygodniowo Vmvware Data Protection.	codziennie		13.06.2017		13.12.2017
19	POWIAT - aplikacje użytkowe	OR	Włodzimierz Gralak	Dodatkowe programy z zakresu FK. Baza na serwerze starostwa.	codziennie	23.03.2017			13.12.2017
20	NORMA 3 - kosztorysowanie	SI	Zygfryd Kostka	Baza kosztorysów na serwerze starostwa w zasobie Referatu Inwestycji i Remontów.	codziennie			13.09.2017	
21	ELEKTRONICZNY OBIEG DOKUMENTÓW "Mdok"	TO	Andrzej Chwalczyk	Baza na serwerze starostwa. Kopia systemu weryfikowana przez COIG SA, zgodnie z umową.	codziennie				
22	OPTIest - System Ewidencji Majątku	OR	Andrzej Chwalczyk	Baza na serwerze starostwa	codziennie		13.06.2017		13.12.2017
23	DGA BPM - Narzędzie wspomagające ZSZ	TJ	Dominika Świerk-Bara	Baza na serwerze starostwa	codziennie			13.09.2017	
24	RISK MANAGER	TK	Katarzyna Borek	Baza na serwerze starostwa	codziennie		13.06.2017		13.12.2017
25	ZPU - zezwolenia na kierowanie pojazdami uprzywilejowanymi	SK	Cecylia Maindok	Baza na serwerze starostwa.	codziennie	23.03.2017		13.09.2017	
26	INTRANET - wewnętrzny portal Starostwa Powiatowego w Raciborzu	OR	Włodzimierz Gralak	Baza na serwerze starostwa.	codziennie			13.09.2017	

Uwagi

Załącznik Nr 5
do Instrukcji Zarządzania
Systemem Informatycznym

Kategorie stron internetowych (WWW)

1. Violence, Hate & Racism **Przemoc, Nienawiść i Rasizm** Witryny, które przedstawiają ekstremalną szkodę fizyczną ludziom lub mieniu, lub które opowiadają się lub dostarczają wskazówek, jak powodować takie szkody. Obejmuje również witryny, które przemawiają lub przedstawiają wrogość, opowiadają się za agresją lub ośmieszają każdą osobę lub grupę na podstawie rasy, religii, płci, narodowości, pochodzenia etnicznego lub innych nieumyślnych cech.
2. Intimate Apparel/Swimsuits **Stroje kąpielowe / stroje kąpielowe** Witryny zawierające zdjęcia lub oferujące sprzedaż strój kąpielowy lub kamizelkę intymną lub inne rodzaje odzieży sugestywnej. Nie obejmuje witryn sprzedających bielizna jako podsekcji innych oferowanych produktów.
3. Nudism **Nudyzm** Witryny zawierające nago lub półnagie obrazy ludzkiego ciała. Te przedstawienia niekoniecznie są intencją seksualną, ale mogą zawierać witryny zawierające nagie obrazy lub galerie zdjęć o charakterze artystycznym. Do tej kategorii należą również nagrania nudystów lub naturystów zawierające zdjęcia nagich osób.
4. Pornography **Pornografia** Witryny, które zawierają materiał pornograficzny w celu wywołania seksualnego lub żarliwego zainteresowania
5. Weapons **Bronie** Witryny sprzedające, przeglądające lub opisujące broń, takie jak pistolety, noże lub urządzenia sztuk walki i ich akcesoria, lub dostarczające informacji na temat ich użytkowania lub innych modyfikacji. Nie obejmuje witryn promujących zbieranie broni lub grup, które popierają lub sprzeciwiają się użyciu broni.
6. Adult/Mature Content **Dorosłe / Starsze treści** Witryny zawierające materiały o charakterze dorosłym, które niekoniecznie zawierają nadmierną przemoc, treści seksualne lub nagość. Miejsca te zawierają bardzo lubieżną lub wulgarną treść i miejsca, które nie są odpowiednie dla dzieci.

7. Cult/Occult

Kult / okultyzm

Witryny, które promują lub oferują metody, środki instruktażowe lub inne zasoby, które mają wpływać na rzeczywiste wydarzenia lub wpływać na nich poprzez użycie zaklęć, przekleństw, mocy magicznych lub nadprzyrodzonych istot.

8. Drugs/Illegal Drugs

Narkotyki / Narkotyki Nielegalne

Witryny narkotyków, które promują, oferują, sprzedają, dostarczają, zachęcają lub w inny sposób popierają rekreacyjne lub niezgodne z prawem używanie, uprawę, wytwarzanie lub dystrybucję narkotyków, farmaceutyków, odurzających roślin lub chemikaliów i związanych z nimi elementów. Ponadto strony, które dyskutują lub promują używanie i nadużywanie leków regulowanych oraz urządzeń związanych z lekami regulowanymi, a także miejscami, które dostarczają informacji o zatwierdzonych lekach i ich zastosowaniach medycznych oraz promują stosowanie substancji chemicznych, które nie są regulowane przez FDA .

9. Illegal Skills/Questionable Skills

Nieprawidłowe umiejętności / wątpliwe umiejętności

Witryny, które przemawiają lub udzielają porad na temat czynów nielegalnych, takich jak kradzieże usług, unikają egzekwowania prawa, oszustw, technik włamań i plagiatu. Obejmuje również witryny, które dostarczają lub sprzedają wątpliwe materiały edukacyjne, takie jak dokumenty okresowe.

10. Sex Education

Edukacja seksualna

Witryny dostarczające graficznej informacji na temat reprodukcji, rozwoju seksualnego, bezpiecznych praktyk seksualnych, seksualności, kontroli urodzin i rozwoju seksualnego. Obejmuje również witryny, które oferują wskazówki dotyczące lepszego seksu, a także produktów wykorzystywanych do poprawy seksualności.

11. Gambling

Hazard

Witryny, w których użytkownik może postawić zakład lub wziąć udział w puli zakładów (w tym loteriach) online. Zawiera również witryny, które dostarczają informacji, pomocy, zaleceń lub szkoleń dotyczących zakładów lub uczestniczących w grach losowych. Nie obejmuje witryn, które sprzedają produkty lub maszyny związane z hazardem lub witryny kasyna hotelu lub offline (o ile te witryny nie spełniają jednego z powyższych wymagań).

12. Alcohol/Tobacco

Alkohol / Tytoń

Witryny, które promują lub oferują wyroby alkoholowe / tytoniowe lub udostępniają sposoby ich tworzenia. Obejmuje również witryny, w których uwielbiam, tout lub zachęcasz do spożywania alkoholu / tytoniu. Nie obejmuje to witryn, które sprzedają alkohol lub tytoń jako podzbiór innych produktów.

13.Chat/Instant Messaging

Czat / Wiadomości błyskawiczne

Witryny obsługujące czat lub komunikator internetowy lub pliki do pobrania klienta.

14. Arts/Entertainment

Sztuka i rozrywka

Witryny promujące i dostarczające informacje o filmach, wideo, telewizji, muzyce i przewodnikach programowych, książkach, komiksach, kinach, galeriach, artystach czy opiniach na temat rozrywki.

15. Business/Economy

Biznes / gospodarka

Witryny poświęcone firmom biznesowym, informacje biznesowe, ekonomia, marketing, zarządzanie przedsiębiorstwem i przedsiębiorczość. Nie obejmuje to witryn, które wykonują usługi zdefiniowane w innej kategorii (takie jak firmy z branży informatycznej lub firmy sprzedające usługi turystyczne).

16. Abortion/Advocacy Groups

aborcyjne / propagujące

Witryny, które dostarczają informacji lub argumentów na rzecz lub przeciw aborcji, opisują procedury aborcyjne, oferują pomoc w uzyskiwaniu lub unikaniu aborcji lub udzielaniu informacji o skutkach lub braku ich aborcji.

17. Education

Edukacja

Witryny oferujące informacje edukacyjne, kształcenie na odległość i informacje lub programy szkolnictwa handlowego. Obejmuje również witryny sponsorowane przez szkoły, placówki edukacyjne i wydziałowe lub grupy absolwentów.

19. Cultural Institutions

Instytucje kultury

Witryny sponsorowane przez instytucje kultury lub dostarczają informacji o muzeach, galeriach, teatrach (nie kinowych). Obejmuje takie grupy, jak 4-H i harcerstwo z Ameryki.

20. Online Banking

Bankowość online

Witryny dostarczające lub reklamujące usługi bankowe (online lub offline) lub inne rodzaje informacji finansowych, takie jak pożyczki. Nie obejmuje witryn, które oferują informacje o rynku, usługi brokerskie lub handlowe.

21. Online Brokerage/Trading

Online Brokerage / Trading

Witryny, które świadczą lub reklamują papiery wartościowe i zarządzanie aktywami inwestycyjnymi (online lub offline). Obejmuje również witryny ubezpieczeniowe, a także witryny, które oferują strategie inwestycyjne finansowe, cytaty i nowości.

22.Games

Gry

Witryny dostarczające informacje na temat gier lub pobierania gier wideo, gier komputerowych, gier elektronicznych, porad i porad na temat gier lub pobierania kody. Obejmuje również witryny poświęcone sprzedaży gier planszowych, a także czasopism i czasopism poświęconych grze. Obejmuje witryny, które obsługują lub organizują zamachy online i prezenty.

23. Government

Rząd

Witryny sponsorowane lub dostarczające informacji o rządach, agencjach rządowych i usługach rządowych, takich jak opodatkowanie i usługi ratownicze. Obejmuje również witryny, które dyskutują lub wyjaśniają prawa różnych podmiotów rządowych.

24. Military

Wojskowy

Witryny promujące lub dostarczające informacje o oddziałach wojskowych lub uzbrojonych.

25. Political & Advocacy Groups

Grupy polityczne i rzecznictwa

Witryny sponsorowane lub dostarczające informacji o partiach politycznych, specjalnych grupach interesów lub każdej organizacji promującej zmiany lub reformy w polityce publicznej, opinii publicznej, praktyce społecznej lub działalności gospodarczej.

26. Health

Zdrowie

Witryny, które udzielają porad i informacji o ogólnym zdrowiu, takich jak kondycja i samopoczucie, zdrowie osobiste lub usługi medyczne, leki, alternatywne i bezpłatne terapie, informacje medyczne o dolegliwościach, stomatologii, optometrii, psychiatrii ogólnej, samopomocy i organizacjach wspierających Choroba lub stan.

27. Information Technology/Computers

Informatyka / Komputery

Witryny, które sponsorują lub dostarczają informacji na temat komputerów, technologii, internetu oraz organizacji i firm związanych z technologią.

28. Hacking/Proxy Avoidance Systems

Systemy zapobiegania włamaniom / proxy

Witryny dostarczające informacje o nielegalnym lub wątpliwym dostępie do sprzętu lub oprogramowania komunikacyjnego lub udostępniają informacje o pomijaniu funkcji serwera proxy lub uzyskiwanie dostępu do adresów URL w jakikolwiek sposób, który pomija serwer proxy.

29. Search Engines & Portals

Wyszukiwarki i portale

Witryny obsługujące wyszukiwanie w internecie, indeksy i katalogi.

30. Email

E-mail

Witryny oferujące usługi poczty elektronicznej w sieci Web, takie jak e-maile, e-kartki i usługi mailingowe.

31. Web Communications

Komunikacja internetowa

Witryny umożliwiające lub oferujące komunikację internetową za pośrednictwem poczty e-mail, czatu, komunikacji błyskawicznej lub forum.

32. Job Search

Poszukiwania pracy

Witryny, które pomagają w znalezieniu zatrudnienia i narzędzi do znalezienia potencjalnych pracodawców.

33. News/Media

Media informacyjne

Witryny, które głównie publikują informacje lub komentarze dotyczące bieżących wydarzeń lub współczesnych wydarzeń dnia. Zawiera również stacje radiowe i czasopisma. Nie obejmuje witryn, które mogą być oceniane w innych kategoriach.

34. Personals & Dating

Randki i Randki

Witryny promujące relacje międzyludzkie.

35. Usenet News Groups

Grupy dyskusyjne Usenet

Witryny oferujące dostęp do grup dyskusyjnych Usenetu lub innych systemów komunikacyjnych lub biuletynów.

36. Reference

Odniesienie

Witryny zawierające dane osobowe, zawodowe lub edukacyjne, w tym słowniki internetowe, mapy, spis powszechny, almanachy, katalogi biblioteczne, miejsca związane z genealogią oraz informacje naukowe.

37. Religion

Religia

Witryny promujące i dostarczające informacji o konwencjonalnych lub niekonwencjonalnych przedmiotach religijnych lub quasi-religijnych, a także kościołach, synagogach i innych domach kultu. Nie obejmuje witryn zawierających czary (Cult / Occult) lub przekonań ateistycznych.

38. Shopping

Zakupy

Witryny dostarczające lub reklamujące sposoby uzyskiwania towarów lub usług. Nie obejmuje witryn, które można sklasyfikować w innych kategoriach, takich jak pojazdy czy broń.

39. Internet Auctions

Aukcje internetowe

Witryny wspierające oferowanie i zakup towarów między osobami. Nie obejmuje ogłoszeń klasyfikowanych.

40. Real Estate

Nieruchomość

Witryny informujące o wynajmie, kupnie lub sprzedaży nieruchomości lub nieruchomości.

41. Society and Lifestyle

Społeczeństwo i styl życia

Witryny dostarczające informacji o kwestiach związanych z codziennym życiem. Nie obejmuje witryn, które można sklasyfikować w innych kategoriach, takich jak sztuka i rozrywka, zdrowie i sport / rekreacja.

43. Restaurants and Dining

Restauracje i jadalnia

Witryny, które przeglądają, dyskutują, reklamują i promują jedzenie, gastronomię, usługi gastronomiczne, gotowanie i przepisy kulinarne.

44. Sports/Recreation

Sport / Rekreacja

Witryny promujące lub dostarczające informacje na temat widowisk sportowych, rekreacyjnych lub hobby. Obejmuje witryny, które dyskutują lub promują camping, ogrodnictwo i kolekcje.

45. Travel

Podróżować

Witryny promujące lub oferujące możliwość planowania podróży, w tym znajdowanie i rezerwowanie podróży, wypożyczanie samochodów, opisy podróży lub promocji hoteli lub kasyna.

46. Vehicles

Pojazdy

Witryny dostarczające informacje lub promujące pojazdy, łodzie lub samoloty. Obejmują one witryny obsługujące zakup online pojazdów lub części samochodowych.

47. Humor/Jokes

Humor / żarty

Witryny skupiające się na humorze, komedii, żartach i zabawie. Mogą zawierać witryny zawierające humor lub dowcipy o dorosłej lub dojrzałej naturze. Witryny zawierające treść dla dorosłych lub dojrzałych mogą również mieć rating kategorii treści dla dorosłych / starszych.

48. Multimedia

Multimedia

Witryny, które sprzedają, dostarczają lub przesyłają treści muzyczne lub wideo w dowolnym formacie, w tym witryny, które udostępniają takie materiały do pobrania.

49. Freeware/Software Downloads

Darmowe / Pobieranie oprogramowania

Witryny dedykowane do elektronicznego pobierania pakietów oprogramowania, bez względu na to czy są płatne czy nie.

50. Pay to Surf

Zapłać na Surf

Witryny, które płacą użytkownikom w formie gotówki lub nagród za kliknięcie lub przeczytanie konkretnych linków, adresów e-mail lub stron internetowych.

53. For Kids

Dla dzieci

Witryny zaprojektowane specjalnie dla dzieci.

54. Advertisements

Reklamy

Witryny oferujące reklamy internetowe lub banery zawsze będą dozwolone. Nie obejmują one serwerów reklamowych zawierających reklamy dla dorosłych.

55. Web Hosting

Hosting

Witryny organizacji, które udostępniają domeny na najwyższym poziomie, a także społeczności internetowe lub usługi hostingowe.

57. Internet Watch Foundation CAIC

Fundacja Watch Internetowa CAIC

Witryny rozpatrywane przez Internet Watch Foundation zawierają potencjalnie niebezpieczną treść internetową, w tym treści związane z wykorzystywaniem seksualnym dzieci, prowadzoną na całym świecie, pornograficznie niegrzeczne treści dla dorosłych w Wielkiej Brytanii i obrazy niemeograficzne dotyczące wykorzystywania seksualnego w Wielkiej Brytanii.

58. Social Networking

Sieć społecznościowa

Społeczności użytkowników i witryny umożliwiające użytkownikom wzajemną interakcję, publikowanie wiadomości, zdjęć lub komunikowanie się z innymi grupami. Nie obejmuje blogów ani stron osobistych.

59. Malware

Szkodliwe oprogramowanie

Witryny obsługujące oprogramowanie, które jest ukryte w systemie użytkownika w celu zbierania informacji i monitorowania aktywności użytkownika. Ponadto witryny zakaźne destrukcyjnymi lub złośliwymi programami, takimi jak wirusy, trojany lub robaki, które są specjalnie zaprojektowane do uszkodzenia, zakłócenia, ataku lub manipulowania systemami komputerowymi bez zgody użytkownika.

- kategorie zablokowane dla wszystkich użytkowników
- kategorie odblokowane dla wszystkich użytkowników
- kategorie odblokowane dla użytkowników posiadających uprawnienia dodatkowe
- kategorie odblokowane po potwierdzeniu wykorzystania do celów służbowych