Zarządzenie numer 2/2022

Starosty Ząbkowickiego

z dnia 15 LUTEGO 2022 roku

w sprawie zmiany Polityki Bezpieczeństwa Informacji Starostwa Powiatowego w Ząbkowicach Śląskich oraz załącznika numer 11 do Polityki Bezpieczeństwa Informacji.

Na podstawie art. 24 ust. 1 i 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L. 119.1 z 04.05.2016) oraz Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych – zarządzam, co następuje

§1

We wprowadzonej zarządzeniem numer 36/2019 z dnia 2 września 2019 roku Polityce Bezpieczeństwa Informacji Starostwa Powiatowego w Ząbkowicach Śląskich zmienia się zapisy w Polityce Bezpieczeństwa Informacji oraz załącznik numer 11 niniejszego dokumentu.

§2

Zmienione dokumenty stanowią załącznik do wydanego zarządzenia i stanowią dokumentację wewnętrzną Starostwa Powiatowego w Ząbkowicach Śląskich.

§3

W pozostałym zakresie Polityka Bezpieczeństwa Informacji Starostwa Powiatowego w Ząbkowicach Śląskich przyjęta zarządzeniem numer 36/2019 z dnia 2 września 2019 roku pozostaje w mocy.

§4

Zarządzenie wchodzi w życie z dniem podjęcia.

STAROSTA ZĄBKOWICKI
Roman Fester

RADCA PRAWNY
Agnieszka Jurek

Załącznik do Zarządzenia Nr 2/2022
Starosty Ząbkowickiego
z dnia 15 lutego 2022 roku

Polityka Bezpieczeństwa Informacji

w Starostwie Powiatowym w Ząbkowicach Śląskich

Opracował: Inspektor Ochrony Danych

Luty 2022

Spis treści:

I. Cele Polityki

§ 1

Informacja jest newralgicznym zasobem każdej organizacji, instytucji, w tym Starostwa Powiatowego w Ząbkowicach Śląskich.

§ 2

Celem niniejszej polityki jest:

1. zapewnienie bezpieczeństwa danych osobowych przetwarzanych w Starostwie przed naruszeniem ochrony danych osobowych, prowadzącym do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;
2. zapewnienie bezpieczeństwa systemom teleinformatycznym wykorzystywanym w Starostwie przed udostępnieniem i wykorzystywaniem w sposób naruszający zasady bezpieczeństwa przetwarzania i dostępu do informacji;
3. prawidłowe zabezpieczenie dokumentacji przed nieuprawnionym do niej dostępem, naruszeniem integralności bądź zniszczeniem aktywów związanych z przetwarzaniem informacji;
4. zagwarantowanie dostępności informacji oraz zdolności do nieprzerwanego świadczenia usług naszym klientom poprzez wdrożenie mechanizmów zarządzania ciągłością działania.

§ 3

Poprzez bezpieczeństwo rozumie się zapewnienie danym:

1. poufności – właściwość polegająca na tym, że informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom, podmiotom lub procesom;
2. integralności - właściwość polegająca na zapewnieniu dokładności i kompletności informacji, dane nie mogą zostać zmienione lub zniszczone w sposób nieautoryzowany;
3. dostępności - właściwość zapewniająca, że informacja jest osiągalna i może być wykorzystana na żądanie upoważnionego podmiotu.

§ 4

„Polityka Bezpieczeństwa Informacji", zwana dalej PBI, została opracowana zgodnie z wymogami:

1. Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie

swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L. 119.1 z 04.05.2016);

2. Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2017 poz. 2247 t.j.);
3. polskich norm PN-EN ISO/IEC 27001 i PN-EN ISO/IEC 27002.

§ 5

1. Kierownictwo Starostwa wyraża pełne zaangażowanie dla zapewnienia bezpieczeństwa przetwarzanych informacji w Starostwie oraz wsparcie dla przedsięwzięć technicznych i organizacyjnych związanych z ochroną tych informacji.
2. Administrator Danych Osobowych – Starosta Ząbkowicki odpowiedzialny jest m. in. za:
   - zatwierdzanie Polityki Bezpieczeństwa Informacji
   - zapewnianie zasobów niezbędnych do właściwego zabezpieczenia danych osobowych przed ich udostępnieniem osobom nieupoważnionym, utratą, uszkodzeniem lub zniszczeniem.
3. Inspektor Ochrony Danych – osoba pełniąca funkcję na podstawie umowy zawartej przez Starostę Ząbkowickiego odpowiedzialna jest za nadzór nad przestrzeganiem przepisów o ochronie danych osobowych, m. in. za:
   - analizowanie zagrożeń i ryzyka, na które może być narażone przetwarzanie danych osobowych
   - nadzór nad ustaleniem i zastosowaniem środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych w systemie informacyjnym Starostwa, m.in.:
     - zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym/ nieuprawnionym
     - zapobieganie przetwarzaniu danych osobowych z naruszeniem przepisów o ochronie danych osobowych, ich zmianie, utracie, uszkodzeniu lub zniszczeniu
   - monitorowanie działania zabezpieczeń wdrożonych w celu ochrony danych osobowych
   - coroczną weryfikację zagrożeń i szans dotyczących systemu informacyjnego
   - coroczną weryfikację PBI i ocenę jej funkcjonowania na przeglądzie systemu zarządzania
   - przekazywanie informacji związanych z bezpieczeństwem danych osobowych na bieżąco Staroście Ząbkowickiemu
   - nadzór nad przestrzeganiem przez pracowników zasad wynikających z PBI
   - zapewnienie, by upoważnienia do przetwarzania danych pracowników zatrudnionych przy ich przetwarzaniu określały odpowiedzialność związaną z ochroną danych osobowych

- organizację szkoleń mających na celu zaznajomienie pracowników przetwarzających dane osobowe z przepisami dotyczącymi ich ochrony

4. Administrator Systemów Informatycznych – osoba upoważniona przez Starostę Ząbkowickiego do nadzoru nad ochroną elektronicznych zbiorów danych osobowych, odpowiedzialny jest m. in. za:
    - właściwe zabezpieczenie sprzętu, na którym przetwarzane są dane osobowe
    - nadzór nad wykorzystywanym w Starostwie oprogramowaniem i jego legalnością
    - podejmowanie działań zapobiegających dostępowi osób niepowołanych do systemu, w którym przetwarzane są dane osobowe
    - analizę ewentualnych naruszeń w systemie zabezpieczeń danych osobowych
    - sporządzanie raportów z naruszenia bezpieczeństwa systemu informatycznego i przekazywanie ich inspektorowi ochrony danych (wraz z informacją o podjętych działaniach). Wzór zawiera załącznik nr 9
    - nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych zawierających dane osobowe
    - definiowanie użytkowników i haseł dostępu
    - aktualizowanie oprogramowania antywirusowego, chyba, że aktualizacje te wykonywane są automatycznie
    - wykonywanie kopii awaryjnych, ich przechowywanie oraz okresowe sprawdzanie pod kątem ich dalszej przydatności
5. Pracownicy przetwarzający dane osobowe odpowiedzialni są m. in. za:
    - stosowanie polityki bezpieczeństwa informacji,
    - ochronę powierzonych im do przetwarzania, archiwizowania lub przechowywania danych przed dostępem osób nieupoważnionych, oraz zabezpieczenia przed zniszczeniem, utratą lub modyfikacją
    - utrzymywanie w tajemnicy powierzonych identyfikatorów, haseł itp.
    - zgłaszanie Inspektorowi Ochrony Danych ewentualnych naruszeń ochrony danych osobowych

§ 6

1. Wszyscy pracownicy Starostwa są zobowiązani do zapoznania się z PBI i potwierdzenie u Inspektora Ochrony Danych tego faktu poprzez stosowną informację w ewidencji osób zapoznanych z PBI.
2. Wzór oświadczenia zawiera załącznik nr 1.

II. Definicje

§ 7

Użyte w niniejszej Polityce określenia i zwroty oznaczają:

1) **RODO** – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych);
2) **Administrator Danych Osobowych (ADO)** – Starosta Ząbkowicki;
3) **Inspektor Ochrony Danych (IOD)** – osoba wyznaczona przez ADO w rozumieniu art. 37 RODO;
4) **Administrator Systemów Informatycznych (ASI)** - pracownik wyznaczony przez ADO, odpowiedzialny za wdrażanie i stosowanie zasad bezpieczeństwa w zakresie technicznych zabezpieczeń systemu informatycznego;
5) **Blokowanie konta** – administracyjne uniemożliwienie korzystania z konta w danym systemie teleinformatycznym;
6) **Dane osobowe** – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą") na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
7) **Dane uwierzytelniające** – informacje wprowadzone do systemu, potwierdzające tożsamość użytkownika (np. hasła dostępu);
8) **Dedykowana sieć elektryczna** – sieć elektryczna przeznaczona do zasilania urządzeń komputerowych, która zapewnia stabilne parametry zasilania, bez zakłóceń urządzeń komputerowych oraz ciągłość zasilania na czas zaniku napięcia w sieci zasilającej z wykorzystaniem urządzeń UPS;
9) **Gwarantowane źródła zasilania** – źródło zasilania zapewniające jakość zasilania niezależnie od stanu źródeł zewnętrznych;
10) **Hasło** – ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie teleinformatycznym;
11) **Identyfikator użytkownika** – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę w systemie teleinformatycznym;

12) **Incydent** – pojedyncze zdarzenie lub seria niepożądanych albo niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań i zagrażają bezpieczeństwu;
13) **Konto** – część systemu teleinformatycznego (dane, oprogramowanie, zasoby sieciowe), które są przypisane do identyfikatora użytkownika;
14) **Kopia archiwalna** – duplikat danych, przechowywanych z uwagi na przepisy prawa lub potrzeby dokumentowania działalności Starostwa; kopia archiwalna nie służy do odtworzenia;
15) **Kopia zapasowa** – duplikat danych, przechowywany na wymiennym nośniku danych służący do odtworzenia systemu, aplikacji, bazy danych, lub dokumentu;
16) **Logowanie** – proces uwierzytelniania użytkownika w systemie teleinformatycznym;
17) **Starosta** – Starosta Ząbkowicki;
18) **Nośnik informacji** – medium magnetyczne, optyczne lub papierowe, na którym zapisuje się i przechowuje informacje - forma utrwalenia dokumentu;
19) **Organ nadzorczy** – niezależny organ publiczny ustanowiony przez Państwo zgodnie z art. 51 RODO;
20) **Osoba trzecia** – osoba prawna lub fizyczna, organizacyjnie niezwiązana ze Starostwem,
21) **Pracownik** – osoba zatrudniona w Starostwie na podstawie umowy o pracę, umowy zlecenie oraz umowy o dzieło, a także stażysta;
22) **Profil dostępu** – zestaw uprawnień, funkcji i zasobów systemu informatycznego dostępnych poszczególnym użytkownikom systemu;
23) **Profil uprzywilejowany** – profil użytkownika posiadającego większe uprawnienia systemowe niż standardowy użytkownik np. administrator, użytkownik zaawansowany;
24) **Profil użytkownika** – plik zawierający informacje konfiguracyjne dotyczące konkretnego użytkownika, na przykład ustawienia pulpitu, stałe połączenia sieciowe i ustawienia aplikacji. Preferencje poszczególnych użytkowników są zapisywane w profilach, dzięki czemu przy każdym ich logowaniu system może odpowiednio skonfigurować środowisko pracy dla użytkownika;
25) **Programy zabezpieczające** - programy, których celem jest zabezpieczanie systemu przed szkodliwym oprogramowaniem, nieupoważnionym dostępem oraz wykrywanie, zwalczanie i usuwanie wykrytego szkodliwego oprogramowania;
26) **Przetwarzanie danych** – oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie,

ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

27) **Rejestr Oprogramowania (RO)** - rejestr oprogramowania dopuszczonego do funkcjonowania w Starostwie. Rejestr jest prowadzony przez ASI;
28) **Rejestr Systemów Teleinformatycznych (RST)** - rejestr systemów informatycznych użytkowanych w ramach infrastruktury teleinformatycznej Starostwa lub na podstawie zawartych umów. Rejestr jest prowadzony przez ASI;
29) **Spam** – niepożądana przesyłka poczty elektronicznej kierowana do niezdefiniowanego adresata;
30) **System informatyczny** - system informacyjny, w którym którykolwiek z jego procesów odbywa się w formie elektronicznej;
31) **System teleinformatyczny** - zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania, zapewniający przetwarzanie i przechowywanie, a także wysyłanie i odbieranie danych poprzez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci urządzenia końcowego w rozumieniu ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2017 r. poz. 1907, z późn. zm.);
32) **Szkodliwe oprogramowanie** - wszelkie aplikacje, skrypty i ingerencje mające szkodliwe, przestępcze lub złośliwe działanie w stosunku do użytkownika komputera;
33) **Środki do przetwarzania informacji** – system, usługa lub infrastruktura przetwarzająca informacje;
34) **Uprawnienia administracyjne** - najwyższy poziom dostępu do całości lub części systemu informatycznego w Starostwie umożliwiający pełną kontrolę nad wszystkim funkcjami systemu informatycznego;
35) **Starostwo** – Starostwo Powiatowe w Ząbkowicach Śląskich;
36) **Uwierzytelnianie** – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;
37) **Użytkownik** – osoba posiadająca upoważnienie nadane przez ADO lub osobę wyznaczoną przez niego do korzystania z systemu teleinformatycznego dostępnego w Starostwie w celu realizacji powierzonych zadań;
38) **WAN** – sieć rozległa, łącząca siedziby Starostwa;
39) **VLAN** (Wirtualna sieć lokalna) – logicznie wydzielona grupa urządzeń lub użytkowników, dobranych pod względem funkcji, przyporządkowania lub aplikacji, niezależnie od ich fizycznej lokalizacji w sieci lokalnej;
40) **Wymienny nośnik danych** – komputerowy nośnik danych nie zainstalowany w sposób trwały (np. płyta CD\DVD, pamięć typu flash np. USB, karta, przenośny dysk twardy, kamera cyfrowa, smartfon) lub wymontowany z urządzenia służącego do przetwarzania danych;

41) **Zabezpieczenie danych w systemie teleinformatycznym** – wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;
42) **Zagrożenie** – potencjalna przyczyna incydentu, który może spowodować stratę w systemie;
43) **Zapora sieciowa (firewall)** – urządzenie bądź system ochrony sieci teleinformatycznych przed nieuprawnionym dostępem z zewnątrz;
44) **Zasoby kluczowe** – zasoby niezbędne do realizowania celów statutowych Starostwa.

III. Przetwarzanie danych osobowych

§ 8

Zgodnie z art. 5 RODO dane osobowe muszą być:

1. przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą,
2. zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami,
3. adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w którym są przetwarzane (minimalizacja danych),
4. prawidłowe i w razie potrzeby uaktualniane,
5. przechowywane w formie umożliwiającej identyfikacje osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane,
6. przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem (integralność i poufność).

§ 9

Dla zapewnienia skutecznej ochrony przetwarzanych danych osobowych ADO zapewnia:

1. odpowiednie do zagrożeń i kategorii danych objętych ochroną, środki techniczne i rozwiązania organizacyjne,
2. szkolenia w zakresie przetwarzania danych osobowych i sposobów ich ochrony,
3. okresowe szacowanie ryzyka zagrożeń dla zbiorów danych,
4. kontrolę i nadzór nad przetwarzaniem danych osobowych,
5. monitorowanie zastosowanych środków ochrony.

§ 10

Wszystkie osoby przetwarzające dane osobowe zobowiązane są do:

1. posiadania upoważnienia do przetwarzania danych osobowych,
2. przetwarzania danych osobowych zgodnie z obowiązującymi przepisami,
3. postępowania zgodnie z ustaloną przez ADO Polityką Bezpieczeństwa Informacji.

§ 11

Osoby nieprzestrzegające przepisów w zakresie ochrony danych osobowych podlegają sankcjom przewidzianym w Regulaminie Pracy i w Prawie Cywilnym.

§ 12

Użytkownicy zobowiązani są do:

1. przetwarzania i ochrony danych osobowych zgodnie z przepisami;
2. ścisłego przestrzegania zakresu nadanego upoważnienia;
3. zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia;
4. zgłaszania bez zbędnej zwłoki, do IOD, incydentów związanych z naruszeniem bezpieczeństwa ochrony danych osobowych.

§ 13

6. Za przestrzeganie ochrony informacji przetwarzanych w systemach informatycznych Starostwa odpowiedzialni są kierownicy komórek organizacyjnych Starostwa.
7. Kierownik komórki organizacyjnej odpowiada za przestrzeganie przepisów o ochronie danych osobowych oraz przepisów wewnętrznych na poszczególnych stanowiskach, a w szczególności:
   a) kontroluje sposób zabezpieczenia danych osobowych przez pracowników,
   b) kontroluje sposób realizacji obowiązku udzielania informacji, o jakich mowa w przepisach o ochronie danych osobowych,
   c) zgłasza ADO rejestrację nowych czynności przetwarzania lub zmianę w obecnych czynnościach przetwarzania oraz przygotowuje wniosek w tej sprawie. Wzór wniosku stanowi załącznik nr 2.
   d) wnioskuje o nadanie, zmianę lub odebranie upoważnień do przetwarzania informacji oraz uprawnień użytkownika systemów informatycznych pracownikom. Wzór wniosku stanowi załącznik nr 11.
   e) zgłasza potrzeby w zakresie zabezpieczenia danych osobowych w Starostwie Powiatowym w Ząbkowicach Śląskich.
8. Każdy użytkownik systemu informatycznego odpowiada za ochronę informacji przetwarzanych w systemie zgodnie z indywidualnym zakresem obowiązków, nadanymi uprawnieniami i zakresem odpowiedzialności wynikającym z zajmowanego stanowiska.
9. Podmiotem doradczym w dziedzinie bezpieczeństwa informacji dla komórek organizacyjnych Starostwa jest Inspektor Ochrony Danych.

§ 14

Obszar przetwarzania danych osobowych

1. Przetwarzanie danych w Starostwie dopuszczalne jest wyłącznie na wyznaczonym do tego obszarze.

2. Za obszar przetwarzania danych osobowych uznaje się obszar, w którym wykonywana jest choćby jedna z czynności przetwarzania wymienionych art. 4 RODO.
3. Kierownicy komórek organizacyjnych Starostwa, zobowiązani są do niezwłocznego przekazywania do IOD informacji o lokalizacji miejsc przetwarzania danych osobowych.
4. Wzór Wykazu pomieszczeń, w których przetwarzane są dane osobowe stanowi załącznik nr 3.
5. W szczególnych przypadkach możliwe jest przetwarzanie danych osobowych poza wyznaczonym obszarem (np. na komputerach przenośnych), jednak wymaga to indywidualnej zgody ADO.
6. Użytkownik urządzenia mobilnego zobowiązany jest do przestrzegania zapisów niniejszej polityki.

§ 15

Rejestr czynności przetwarzania danych

1. W Starostwie prowadzony jest Rejestr Czynności Przetwarzania, w którym zamieszcza się co najmniej następujące informacje. Wzór rejestru stanowi - załącznik nr 4.
   1) imię i nazwisko lub nazwę oraz dane kontaktowe administratora i inspektora ochrony danych,
   2) cele przetwarzania,
   3) opis kategorii osób, których dane dotyczą oraz kategorii danych osobowych,
   4) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione,
   5) gdy ma to zastosowanie, przekazania danych do państwa trzeciego, w tym nazwa tego państwa,
   6) jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych,
   7) jeżeli jest to możliwe ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO.
2. Rejestr, o którym mowa w ust. 1 ma formę pisemną lub formę elektroniczną.

§ 16

Udostępnianie danych osobowych

1. Na wniosek osoby, której dane dotyczą, ADO jest obowiązany do potwierdzenia przetwarzania danych oraz udzielenia następujących informacji:
   a) cele przetwarzania,
   b) kategorie odnośnych danych osobowych,
   c) informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych,

d) w miarę możliwości planowany okres przechowywania danych osobowych,
e) informacje o prawie do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych oraz do wniesienia sprzeciwu wobec takiego przetwarzania,
f) informacje o prawie wniesienia skargi do organu nadzorczego,
g) jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o ich źródle,
h) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

2. Administrator dostarcza osobie, której dane dotyczą, kopię danych osobowych podlegających przetwarzaniu.
3. IOD prowadzi wykaz udostępnień danych osobowych osobom, których dotyczą. Wzór wykazu stanowi załącznik nr 5.
4. Administrator danych udostępnia posiadane dane osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.
5. Wzór wykazu udostępnień danych osobowych innym podmiotom, prowadzonego przez IOD, stanowi załącznik nr 6.
6. Powierzenie przetwarzania danych osobowych innemu podmiotowi może nastąpić wyłącznie w drodze umowy lub innego instrumentu prawnego, zawartej w formie pisemnej przez ADO, określającej przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, a także obowiązki i prawa administratora.
7. IOD prowadzi wykaz podmiotów, którym powierzono przetwarzanie danych osobowych. Wzór w/w wykazu stanowi załącznik nr 7.

§ 17

Zarządzanie ryzykiem oraz ocena skutków

1. Zarządzanie ryzykiem, obejmujące wybór, wdrożenie i utrzymanie zabezpieczeń składających się z technicznych i organizacyjnych środków ochrony danych oraz infrastruktury teleinformatycznej.
2. Przeprowadzenie analizy ryzyka w celu zabezpieczenia danych osobowych adekwatnie do zidentyfikowanych zagrożeń, a także konieczności przeprowadzenia oceny skutków powierzono zespołowi składającemu się z ASI oraz IOD.
3. Wyniki szacowania ryzyka zatwierdza ADO.

§ 18

Upoważnienia do przetwarzania danych osobowych

1. Wszystkie osoby przetwarzające dane osobowe zobowiązane są do:
   a) posiadania upoważnienia do przetwarzania danych osobowych;
   b) przetwarzania danych osobowych zgodnie z obowiązującymi przepisami;
   c) postępowania zgodnie z ustaloną przez ADO Polityką Bezpieczeństwa Informacji.
2. Kierownik komórki organizacyjnej występuje z wnioskiem o upoważnienie do przetwarzania danych osobowych dla podległego mu pracownika na formularzu, którego wzór stanowi załącznik nr 11. polityki.
3. IOD sprawdza przed wydaniem upoważnienia do przetwarzania danych osobowych czy użytkownik spełnia warunki dopuszczenia do przetwarzania danej grupy informacji, a w szczególności:
   a) czy użytkownik zapoznał się i podpisał oświadczenie o zapoznaniu się z Polityką Bezpieczeństwa Informacji – załącznik nr 1;
   b) czy użytkownik podpisał deklarację zachowania poufności - załącznik nr 15.
4. Jeżeli użytkownik i jego stanowisko pracy spełniają warunki dopuszczenia, IOD przygotowuje upoważnienie do przetwarzania danych osobowych, którego wzór stanowi załącznik nr 13 i po podpisaniu przez ADO rejestruje je w Ewidencji osób upoważnionych do przetwarzania danych osobowych – którego wzór stanowi załącznik nr 12, a następnie przekazuje wniosek do ASI.
5. Wykreślenie użytkownika z Ewidencji osób upoważnionych do przetwarzania danych osobowych następuje na pisemną informację przekazaną z kadr, w związku z wygaśnięciem stosunku pracy lub po ustaniu okresu zawartej umowy zlecenia, o dzieło lub dotyczącej realizowanego stażu.

IV. Zgłaszanie naruszenia ochrony danych osobowych

§ 19

1. Na naruszenie ochrony danych osobowych mogą wskazywać:
   1) uszkodzenia dokumentacji,
   2) nieuprawniony dostęp do systemów informatycznych lub pomieszczeń,
   3) naruszenie lub próba naruszenia integralności systemu informatycznego,
   4) zmiana lub utrata danych zapisanych na kopiach zapasowych, dokonana w sposób nieautoryzowany,
   5) zniszczenie lub próba zniszczenia w sposób nieuprawniony danych,
   6) inny stan pomieszczeń lub systemu informatycznego niż pozostawiony po zakończeniu pracy lub przerwie w pracy.
2. Przykładowe incydenty ujęte są w załączniku nr 8. Lista przykładowych incydentów nie stanowi zamkniętego katalogu incydentów.

§ 20

1. Osoba przetwarzająca dane osobowe w każdym przypadku stwierdzenia lub podejrzenia wystąpienia incydentu naruszenia zasad ochrony danych osobowych ma obowiązek:
   1) niezwłocznie powiadomić bezpośredniego przełożonego, a następnie IOD i ASI,
   2) powiadomienie powinno zostać przekazane w sposób gwarantujący szybkie dotarcie informacji: telefonicznie lub osobiście, a następnie potwierdzone pocztą elektroniczną lub pisemnie,
   3) powstrzymać się od wszelkich działań mogących utrudnić ustalenie okoliczności naruszenia,
   4) zabezpieczyć pomieszczenie lub jego część do czasu przybycia IOD lub ASI,
   5) podjąć inne działania stosownie do zaistniałej sytuacji, niezbędne do zapobieżenia dalszym zagrożeniom dla danych.
2. IOD po przyjęciu zgłoszenia, wspólnie z ASI, podejmuje niezwłoczne działania zabezpieczające, sprawdzające i wyjaśniające. Po wykonaniu tych czynności sporządza szczegółowy Protokół obsługi incydentu z przeprowadzonego postępowania, którego wzór stanowi załącznik nr 9 i przedstawia go ADO.
3. Każdy przypadek wystąpienia incydentu jest odnotowywany w Rejestrze incydentów – Wzór stanowi załącznik nr 10.
4. Przygotowany Protokół jest podstawą zgłoszenia przez ADO Organowi nadzorczemu, nie później niż w ciągu 72 godzin, faktu stwierdzenia naruszenia bezpieczeństwa ochrony danych osobowych,

chyba że jest mało prawdopodobne, by naruszenie to skutkowało naruszeniem praw lub wolności osób fizycznych.

5. Zgłoszenie do organu nadzorczego, zgodnie z art. 33 RODO musi co najmniej:
   1) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorię i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie,
   2) zawierać imię i nazwisko oraz dane kontaktowe IOD, od którego można uzyskać więcej informacji,
   3) opisywać konsekwencje naruszenia danych osobowych,
   4) opisywać środki zastosowane lub proponowane przez Administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

V. Zasady bezpieczeństwa

§ 21

Podstawowe zasady

Pracownicy zobowiązani są do bezwzględnego przestrzegania podstawowych zasad korzystania z urządzeń oraz nośników zawierających informacje chronione tj.:

1) nie ujawnianie haseł przypisanych do użytkownika,
2) nie spożywanie płynów i pożywienia oraz przechowywanie roślin w bezpośredniej bliskości urządzeń teleinformatycznych,
3) umiejscowienie lub zabezpieczenie filtrami ekranowymi monitorów w pomieszczeniach biurowych w taki sposób, aby maksymalnie ograniczyć oglądanie zawartości ekranu osobom nieuprawnionym,
4) nie podłączanie do sieci komputerowej prywatnych urządzeń komputerowych,
5) nie korzystanie w komputerach stacjonarnych, laptopach, serwerach oraz innych urządzeniach komputerowych pracujących w systemie informatycznym Starostwa z prywatnych nośników informacji,
6) natychmiastowe zgłoszenie swojemu bezpośredniemu przełożonemu, IOD lub ASI wszystkich zauważonych nieprawidłowości, zdarzeń, incydentów lub zagrożeń,
7) nie podłączanie do dedykowanej sieci elektrycznej jakichkolwiek innych urządzeń niż komputerowe (tj. drukarek, kopiarek lub innych urządzeń o znacznym poborze prądu), a tylko komputery, monitory i laptopy,

§ 22

Zasada „czystego biurka i ekranu"

Pracownicy Starostwa zobowiązani są do bezwzględnego przestrzegania zasady „czystego biurka i ekranu", która w szczególności obejmuje następujące wytyczne:

1) wszelkie dokumenty papierowe i nośniki komputerowe, kiedy nie są używane, przechowuje się w odpowiednich, zamykanych szafach lub innego rodzaju zabezpieczonych meblach, szczególnie poza godzinami pracy Starostwa,
2) nośniki informacji danych osobowych, jeśli nie są aktualnie wykorzystywane, zamykane są w meblach biurowych, szafkach metalowych lub sejfach, w zależności od ich ważności,
3) w przypadku opuszczenia stanowiska pracy komputer należy zabezpieczyć przed niepowołanym dostępem innych osób poprzez zablokowanie go lub wylogowanie się,
4) komputery nie mogą być pozostawione bez nadzoru w stanie zarejestrowania do systemów informatycznych,

5) pracownicy zobowiązani są do niezwłocznego odbioru swoich wydruków z urządzeń drukujących (szczególnie dotyczy to wydruków zawierających dane osobowe).

§ 23

Odpowiedzialność za sprzęt komputerowy

1. Odpowiedzialność za właściwe użytkowanie sprzętu służącego do przetwarzania informacji, w szczególności sprzętu komputerowego, spoczywa na jego użytkowniku.
2. Przesunięcie do użytkowania urządzeń komputerowych pomiędzy użytkownikami, w wyniku którego następuje zmiana osoby odpowiedzialnej za urządzenie, może nastąpić tylko za wiedzą i zgodą dysponenta urządzeń.
3. Wynoszenie urządzeń komputerowych poza Starostwo odbywa się jedynie na podstawie ważnych dokumentów przekazania za zgodą przełożonego oraz wiedzą Dysponenta urządzenia. Nie dotyczy to komputerów przenośnych i innych urządzeń mobilnych (np. telefonów komórkowych), za których bezpieczeństwo odpowiedzialne są pracownicy, którym te urządzenia przydzielono na podstawie osobnych protokołów przekazania.

§ 24

Dostęp do urządzeń drukujących i powielających

1. W przypadku drukowania lub oczekiwania na wydrukowanie informacji zawierającej dane osobowe, użytkownikowi nie wolno odchodzić od drukarki/skanera, na której dokonywany jest wydruk. Zasada ta nie obowiązuje, jeśli drukarka/skaner znajduje się w zabezpieczonym miejscu chronionym przed dostępem osób nieupoważnionych lub posiada system zapewniający odbiór wydruku tylko osobie uprawnionej (właściciel wydruku).
2. Użytkownik, który oczekuje na wydrukowanie informacji musi być upoważniony do jej przeglądania.
3. Wszystkie zbędne kopie informacji powstałe w trakcie ich przetwarzania, kopiowania lub drukowania muszą być trwale zniszczone.

§ 25

Po zakończeniu pracy

1. Po zakończonej pracy, przed opuszczeniem pomieszczenia, pracownicy zobowiązani są do sprawdzenia czy na drukarkach/skanerach, faksach lub kserokopiarkach nie pozostawiono nieodebranych wydruków, czy zostały wyłączone wszystkie urządzenia elektryczne (w szczególności, czy został wyłączony komputer), zamknięte okna oraz czy dokumenty papierowe lub nośniki z informacjami zostały umieszczone w zamkniętych szafach/biurkach,

2. Jeżeli pomieszczenie opuszczają wszyscy pracownicy, należy je zamknąć na klucz. Po zamknięciu nie wolno zostawiać klucza w drzwiach, a następnie przekazać do miejsca określonego w instrukcji.
3. Klucze do pomieszczeń podlegają ochronie zgodnie z Instrukcją dysponowania kluczami.

VI. Hasła dostępu

§ 26

Użytkownik ponosi odpowiedzialność za użycie zasobów informatycznych Starostwa przy wykorzystaniu jego hasła do momentu powiadomienia ASI o ujawnieniu hasła.

§ 27

1. Korzystanie z haseł ma na celu utrudnienie uzyskania nieautoryzowanego dostępu do zasobów informatycznych Starostwa. Zasady te obejmują wszystkie systemy informatyczne należące do Starostwa i/lub zarządzane przez Starostwo.
2. Wszyscy użytkownicy systemów informatycznych Starostwa muszą stosować hasła zgodnie z niniejszymi zasadami.
3. Hasło użytkownika jest jego własnością i zna je wyłącznie użytkownik.
4. Zabronione jest przekazywania hasła innym osobom. Bez względu na okoliczności, hasła nie wolno ujawniać. W szczególności nie należy go ujawniać przez telefon lub pocztę elektroniczną osobom, które mogą podawać się np. za pracowników pomocy technicznej.
5. Jeśli istnieje podejrzenie, że hasło zostało ujawnione, należy je natychmiast zmienić i powiadomić ASI.

§ 28

1. Użytkownik ma obowiązek stosować hasła trudne do odgadnięcia.
2. Zaleca się aby użytkownicy nie używali haseł takich samych lub podobnych do używanych przez nich poprzednio. Hasło musi być różne od ostatnio wykorzystywanych 5 haseł.
3. Hasła powinny być unikalne tj. inne niż używane w jakimkolwiek innym systemie/aplikacji oraz inne niż używane przez Użytkowników poza systemami Starostwa.
4. Użytkownik korzystający z zewnętrznych usług internetowych zabezpieczanych hasłem (np. serwisu bankowego, portalu administracyjnego) nie powinien używać w celu dostępu do nich takiego samego hasła, jak w przypadku dostępu do systemów Starostwa.
5. Haseł nie należy zapisywać i pozostawiać w miejscu, w którym mogłyby zostać ujawnione. W szczególności zabronione jest umieszczanie haseł w treści skryptów systemowych i programów.
6. Hasła nie powinny być wpisywane w obecności osób nieupoważnionych, jeśli mogą one zauważyć treść wpisywanego hasła.

7. Niedopuszczalne jest podglądanie haseł wprowadzanych do systemu przez innych użytkowników. Jeżeli użytkownik w pobliżu zaczyna wprowadzać hasło zaleca się aby odwrócić wzrok.

§ 29

Użytkownicy są zobowiązani do przestrzegania poniższych reguł odnośnie długości i złożoności hasła oraz okresu jego wymiany:

1) Hasło do systemu musi składać się z min. 8 znaków - zawiera małe i duże litery oraz cyfry lub znaki specjalne.
2) Zmiana hasła następuje nie rzadziej niż co 30 dni.
3) Jeżeli system nie wymusza zmiany haseł użytkownik zobowiązany jest samodzielnie zmieniać hasło nie rzadziej niż co 30 dni.

§ 30

Hasło nie powinno być:

1) słowem ze słownika w żadnym popularnym języku,
2) nazwiskiem, nazwą geograficzną, terminem technicznym lub określeniem potocznym,
3) związane z życiem zawodowym lub osobistym Użytkownika np. nie powinno być numerem rejestracyjnym samochodu, numerem telefonu, imieniem członka rodziny, częścią adresu, inicjałami itp.
4) sekwencją kolejnych znaków na klawiaturze np. 123456, qwerty,
5) sekwencją tych samych znaków np. 33333, aaaaa,
6) oparte na ciągu znaków ulegających zmianie w zależności od daty lub innego przewidywalnego czynnika,
7) dowolnym elementem spośród wymienionych powyżej z dodaną na końcu cyfrą lub liczbą.

§ 31

Użytkownicy powinni stosować łatwe do zapamiętania hasła, które są jednocześnie trudne do odgadnięcia, spełniające co najmniej jeden z niżej wymienionych warunków:

1) łącząc kilka słów razem,
2) zastępując w określonym słowie kilka małych liter dużymi,
3) zastępując poszczególne znaki w haśle wcześniejszymi lub dalszymi znakami w alfabecie lub na klawiaturze,
4) zastępując w określonym słowie litery numerami odzwierciedlającymi ich pozycję w alfabecie,
5) łącząc znaki przestankowe i cyfry ze słowami,

6) wykorzystując pierwsze litery słów piosenki, wiersza lub innego znanego powiedzenia,
7) celowo stosując słowo z błędem (nie popełnianym jednak często lub nietypowym).

VII. Zarządzanie hasłami

§ 32

1. Wszystkie systemy informatyczne Starostwa (o ile producent systemu przewidział taką możliwość) powinny umożliwiać ustalenie minimalnej długości hasła, okresu maksymalnej ważności hasła oraz mieć możliwość wymuszenia zmiany hasła przez użytkownika po upływie terminu jego ważności oraz przy pierwszym logowaniu.
2. Użytkownicy uprawnieni do pracy w systemach informatycznych Starostwa otrzymują profile dostępu.
3. ASI ustawia w systemie (jeżeli jest to możliwe) zasady wymuszenia zmiany hasła co 30 dni, długości i złożoności hasła.
4. Hasło użytkownika jest składowane w systemie przetwarzania w bezpieczny sposób.
5. Hasło użytkownika nie może być przesyłane przez sieć otwartym tekstem.
6. Hasło użytkownika nie jest pokazywane na ekranie lub wydrukach w postaci otwartego tekstu.
7. Oprogramowanie nie może przechowywać ani zapisywać hasła w postaci jawnego tekstu.

§ 33

1. W przypadku, gdy użytkownik musi posiadać dostęp do wielu systemów lub aplikacji, co stwarza konieczność przypisania mu wielu profili użytkownika, może on posługiwać się tym samym hasłem we wszystkich swoich profilach. Wyjątkiem są profile administracyjne, które powinny być zabezpieczone innym hasłem.
2. Systemy używane przez wielu użytkowników powinny mieć możliwość ustawienia unikatowych identyfikatorów użytkowników i haseł przyporządkowanych poszczególnym użytkownikom, a także posiadać mechanizmy ograniczające przywileje użytkowników.
3. Systemy wykorzystywane przez pojedynczych użytkowników zaleca się, aby posiadały mechanizmy kontrolujące ich uruchamianie oraz automatycznie blokujące dostęp w przypadku przerwy w korzystaniu z systemu.
4. Dla tych elementów systemów informatycznych Starostwa, których technologia uniemożliwia stosowanie indywidualnych profili dostępu, dopuszcza się stosowanie haseł grupowych, przy czym utworzenie hasła grupowego powinno być każdorazowo zatwierdzone przez IOD.
5. Przed przekazaniem do użytkowania systemów informatycznych konieczna jest zmiana wszystkich haseł domyślnych ustawionych przez dostawcę lub ich zablokowanie.

6. Jeśli oprogramowanie zapewnia takie możliwości, należy wymusić automatyczną zmianę hasła tymczasowego podczas pierwszego logowania do systemu.
7. Jeśli oprogramowanie zapewnia takie możliwości, należy uniemożliwić użytkownikom stosowanie łatwych do odgadnięcia haseł.
8. ASI oraz inni pracownicy Starostwa nie będą zapoznawać się z treścią informacji zawartych w innych profilach użytkowników, z wyjątkiem sytuacji, gdy jest to niezbędne do usunięcia awarii systemu.
9. W Starostwie może istnieć system stwarzający możliwość korzystania z innych metod uwierzytelniania, takich jak sprzętowe generatory haseł, hasła jednorazowe, karty elektroniczne.
10. Każdy użytkownik zarządza swoimi hasłami dla wszystkich identyfikatorów, których używa.

§ 34

Profile uprzywilejowane

1. Hasła dostępu do profili uprzywilejowanych powinny składać się z 12 znaków, zawierać małe i duże litery, cyfry oraz znaki specjalne.
2. Hasła dostępu do profili uprzywilejowanych powinny być przechowywane w bezpiecznym miejscu, w sposób zapewniający utrzymanie ich w tajemnicy. Powinny zostać stworzone procedury określające sytuacje, w których hasła dostępu do profili uprzywilejowanych będą udostępniane osobom innym, niż ich właściciele. Hasła przechowywane w bezpiecznym miejscu powinny być aktualizowane przy każdej ich zmianie. Hasła nieaktualne powinny być niszczone.
3. W przypadku konieczności udzielenia osobom trzecim dostępu do profilu uprzywilejowanego, hasło dostępu powinno być przed udzieleniem takiego dostępu zmienione na tymczasowe, a po wykorzystaniu przywrócone do stanu poprzedniego lub zmienione na nowe w ramach standardowej procedury.

VIII. Oprogramowanie

§ 35

Zakresy odpowiedzialności

Odpowiedzialność za zainstalowanie, odinstalowanie oraz obsługę techniczną oprogramowania ponosi ASI.

§ 36

Starostwo zapewnia, że:

1) wszystkie użytkowane w Starostwie programy, aplikacje oraz systemy operacyjne są legalne i posiadają odpowiednie licencje oraz zezwolenie na użytkowanie,
2) oprogramowanie jest zainstalowane maksymalnie na takiej liczbie stanowisk na jaką pozwala liczba licencji,
3) nośniki z oprogramowaniem pochodzą ze sprawdzonego i wiarygodnego źródła,
4) pracownik nieuprawniony nie może samodzielnie zainstalować ani uruchamiać oprogramowania, które nie jest dopuszczone do użytkowania w Starostwie.

§ 37

Oprogramowanie instalowane tymczasowo

1. Dopuszcza się stosowanie oprogramowania, które w założeniu ma funkcjonować tylko w trakcie prowadzonych szkoleń, prezentacji lub konferencji. W takim przypadku pracownik odpowiedzialny za organizowane wydarzenie, wnioskuje do ASI o zainstalowanie oprogramowania. Wniosek powinien zawierać co najmniej: cel instalacji, rodzaj i nazwę programu, okres na jaki ma być zainstalowane, zasady licencjonowania, wymagania systemowe i sprzętowe.
2. Na podstawie wniosku ASI decyduje o zainstalowaniu oprogramowania oraz instaluje i administruje oprogramowaniem. Po zakończeniu użytkowania dokonuje odinstalowania. Data odinstalowania nie może przekroczyć daty końcowej wpisanej we wniosku. W przypadku, gdy wnioskodawca chce użytkować program przez czas dłuższy niż wskazany we wniosku, zobowiązany jest to zgłosić ASI.
3. Wnioskodawca ze swojej strony zapewnia, że oprogramowanie jest legalne i pochodzi z legalnego oraz wiarygodnego źródła. Za ewentualne nieprawidłowości i konsekwencje prawne z tym związane odpowiada wnioskodawca.
4. Niedopuszczalne jest samowolne instalowanie przez organizatorów szkoleń i prezentacji oprogramowania bez dopełnienia wyżej wymienionych warunków.

5. Z obowiązku ubiegania się o zgodę zwolnione jest oprogramowanie instalowane do celów testowych bezpośrednio przez ASI lub osoby przez nich wyznaczone.

IX. Ochrona przed szkodliwym oprogramowaniem

§ 38

Opis postępowania

1. Ochrona przed szkodliwym oprogramowaniem jest kluczowa dla utrzymania systemu bezpieczeństwa informacji. Starostwo stosuje wszelkie rozwiązania, które zapobiegają niepożądanym efektom wywoływanym przez szkodliwe oprogramowanie.
2. Za ochronę przed szkodliwym oprogramowaniem odpowiada ASI.
3. Systemy informatyczne razem z przechowywanymi w nich informacjami są narażone na szkody wyrządzane przez działanie niepożądanego/szkodliwego oprogramowania. Z tego względu wszyscy użytkownicy powinni być świadomi zagrożeń związanych z działaniem niepożądanego oprogramowania.
4. W celu wykrycia oraz zapobieżenia pojawianiu się niepożądanego oprogramowania wdrożone są odpowiednie mechanizmy kontrolne. W szczególności uwaga zwrócona jest na ochronę komputerów użytkowników przed pojawianiem się wirusów komputerowych.
5. Zabezpieczenia przed niepożądanym oprogramowaniem opierają się na świadomości użytkowników, stosowaniu odpowiednich aplikacji zapobiegawczych oraz na prawidłowej kontroli dostępu do systemu.
6. Pracownicy są szkoleni i uświadamiani odnośnie korzystania z zabezpieczeń oraz w zakresie korzyści wynikających z działań zapobiegawczych.
7. Środkami, które zabezpieczają przed szkodliwym oprogramowaniem, są m.in.:
   1) przestrzeganie przez użytkowników zasad bezpieczeństwa,
   2) stosowanie programów zabezpieczających,
   3) stosowanie aktualizacji oprogramowania poprawiających bezpieczeństwo aplikacji oraz systemów,
   4) inne działania ASI i IOD np. szkolenia, spotkania
8. Wdrożone i monitorowane są wszystkie możliwe działania w celu zabezpieczenia komputerów stacjonarnych i przenośnych oraz serwerów.
9. Nośniki zewnętrzne należy sprawdzić oprogramowaniem antywirusowym zainstalowanym na stacji roboczej lub przekazać ASI.
10. W przypadku wykrycia wirusa należy go usunąć i niezwłocznie poinformować ASI. Do czasu usunięcia wirusa lub otrzymania innych poleceń od ASI, pracę na komputerze należy wstrzymać.

11. Przy korzystaniu z poczty elektronicznej należy zwrócić szczególną uwagę na otrzymywane załączniki dołączane do treści wiadomości. Zabrania się otwierania załączników i wiadomości poczty elektronicznej od „niezaufanych" nadawców.
12. Zabrania się użytkownikom komputerów, wyłączania, blokowania, odinstalowywania programów zabezpieczających komputer np. skaner antywirusowy, firewall przed oprogramowaniem złośliwym oraz nieautoryzowanym dostępem.
13. Zabronione jest celowe opracowywanie, generowanie, kompilowanie, kopiowanie, rozpowszechnianie, uruchamianie lub próby wprowadzania kodów komputerowych, które:
    1) mają zdolność samopowielania, uszkadzania lub innego utrudniania działalności pamięci komputerowej, plików systemowych lub oprogramowania,
    2) służą do omijania lub przełamywania zabezpieczeń i praw dostępu,
    3) wymagałyby wykorzystania znacznie większej ilości zasobów informatycznych niż jest to niezbędne do zapewnienia prawidłowego działania systemów informatycznych Starostwa,
    4) powodowałyby zakłócenia w działaniu sieci informatycznej Starostwa.
14. Wymienne nośniki danych przeznaczone wyłącznie do odczytu powinny być, o ile to możliwe, zabezpieczone przed możliwością zapisania na nich informacji, zanim zostaną wprowadzone do odpowiedniego napędu.
15. W czasie uruchamiania systemu operacyjnego komputera nie wolno zostawiać wymiennych nośników danych w napędach.
16. Każdy użytkownik zobowiązany jest do korzystania na swoim komputerze z aktualnego oprogramowania antywirusowego dopuszczonego do użytkowania w Starostwie. Powyższe oprogramowanie musi być aktywne przez cały czas działania komputera.
17. Wszystkie media z danymi dostarczone z zewnątrz Starostwa nie mogą być użyte bez wcześniejszego sprawdzenia programem antywirusowym.
18. Wszystkie pliki przed wysłaniem (np. poprzez pocztę elektroniczną) lub przekazaniem na zewnętrznych nośnikach danych, są testowane oprogramowaniem antywirusowym.

§ 39

Szczególne obowiązki użytkowników

Wszyscy użytkownicy komputerów , w szczególności komputerów przenośnych lub innych urządzeń, które są narażone na działanie szkodliwego oprogramowania, zobowiązani są do:

1) uważnego korzystania z zasobów sieciowych (Internet, sieć lokalna) oraz nośników zewnętrznych kierując się przy tym ograniczonym zaufaniem,

2) sprawdzenia programem antywirusowym wszystkich mediów z danymi dostarczonych z zewnątrz Starostwa przed ich użyciem,
3) nie podawania w portalach internetowych (niezwiązanych z wykonywanymi obowiązkami) adresów służbowych skrzynek pocztowych,
4) niezwłocznego powiadomienia przełożonego lub ASI w przypadku stwierdzenia nieprawidłowego działania komputera lub innego urządzenia czy nośnika, które może być spowodowane przez złośliwe oprogramowanie,
5) tworzenia kopii zapasowych informacji, które stanowią wartość dla Starostwa np. na sieciowych dyskach.

X. Internet

§ 40

1. Wszystkie działania użytkowników w zakresie korzystania z Internetu mogą być monitorowane, rejestrowane oraz okresowo oceniane w celu zapewnienia prawidłowego działania i zapobiegania nieautoryzowanemu wykorzystaniu Internetu.
2. Starostwo zastrzega sobie możliwość dostępu do zasobów danych istniejących w systemie informatycznym Starostwa. Zebrane informacje Starostwo ma prawo udostępnić uprawnionym instytucjom państwowym w uzasadnionych przypadkach.
3. Starostwo ma prawo blokować strony internetowe zawierające obraźliwą zawartość oraz inne treści.
4. Dostęp do Internetu z sieci Starostwa powinien odbywać się wyłącznie za pośrednictwem środków i rozwiązań dostarczonych przez Starostwo. Zabronione jest zestawianie z sieci Starostwa indywidualnych połączeń z Internetem przez poszczególnych pracowników przy wykorzystaniu modemów lub innych urządzeń dostępowych.
5. Jakiekolwiek wykorzystanie systemów informatycznych do działań niezgodnych z prawem lub takich, które mogą zostać uznane za obraźliwe lub łamiące inne zasady obowiązujące w Starostwie, może stanowić podstawę do podjęcia działań dyscyplinarnych.
6. Odblokowanie pracownikowi (z uwagi na wykonywanie określonych obowiązków służbowych) dostępu do zablokowanych stron internetowych lub innych zasobów Internetu wymaga przesłania wniosku do ASI zaakceptowanego przez Starostę z podaniem powodów odblokowania oraz czasu na jaki dostęp powinien być ustalony.

XI. Poczta elektroniczna

§ 41

1. Poczta elektroniczna Starostwa (konta e-mail na serwerze poczty) jest udostępniana Pracownikom do wypełniania obowiązków służbowych.
2. Pracownikom nie wolno używać do wypełniania obowiązków służbowych poczty elektronicznej innej niż wskazana przez ASI.
3. Korespondencja e-mail o charakterze prywatnym powinna być jednoznacznie oznaczona w temacie e-maila w celu ochrony prywatności Pracownika.
4. Pracownicy powinni odbierać i sprawdzać pocztę elektroniczną co najmniej 2 dwa razy dziennie np. na rozpoczęcie oraz zakończenie dnia pracy.
5. Wysyłanie pocztą elektroniczną wiadomości zawierających pornografię, treści dyskryminujące przedstawicieli określonej rasy, płci i religii lub dyskryminujące pod innym względem jest zakazane i może stanowić podstawę do podjęcia działań dyscyplinarnych.
6. Zabrania się rozsyłania za pomocą poczty elektronicznej Starostwa wiadomości mających charakter niechcianych lub reklamowych (tzw. Spam).

§ 42

1. Wiadomości przychodzące do Starostwa są skanowane pod kątem obecności Spamu.
2. Maksymalny rozmiar przesyłek pocztowych może zostać ograniczony przez ASI.
3. Pracownicy powinni być świadomi, że poczta elektroniczna nie gwarantuje dostatecznej ochrony przesyłanych informacji. Z tego względu jeśli przesłaniu mają podlegać dane osobowe, należy przed wysłaniem przesyłki zaszyfrować ją przy użyciu mechanizmów rekomendowanych przez ASI.
4. Starostwo zastrzega sobie prawo do odfiltrowywania lub blokowania wybranych przez ASI rodzajów załączników potencjalnie niebezpiecznych dla systemów komputerowych lub nie związanych z działalnością operacyjną Starostwa np. plików wykonywalnych, tzw. linków i zawartości multimedialnej.
5. Pracownicy zespołów technicznych obsługujący systemy poczty elektronicznej nie mogą przeglądać treści przesyłanych wiadomości bez zgody użytkownika lub jego przełożonego.

§ 43

1. Należy ograniczyć przekazywania poprzez służbową pocztę e-mail wiadomości reklamowych oraz innych informacji o charakterze komercyjnym i handlowym.
2. Zabronione jest rozpowszechnianie przez użytkowników materiałów zawierających logo Starostwa lub innych materiałów reklamowych razem z wiadomościami, w których zawarta jest prywatna opinia użytkownika.
3. Dostęp dla celów służbowych do płatnych usług internetowych np. subskrypcje czasopism w formie elektronicznej, wyniki badań marketingowych itp. nie może odbywać się przy użyciu prywatnych kont pracowników za pośrednictwem systemu informatycznego Starostwa.
4. Kopia poczty e-mail użytkownika powinna być przechowywana na serwerze poczty przez min. 21 dni. Dokładny czas przechowywania jest ustalany z Administratorem poczty e-mail i uzależniony od dostępnej przestrzeni oraz decyzji użytkownika lub przełożonego.
5. Imienne konto pocztowe pracownika, z którym Starostwo rozwiązało stosunek pracy blokowane jest z dniem rozwiązania stosunku pracy, a na koncie pocztowym jednostki obsługiwanym przez pracownika, dokonuje się zmiany hasła.

§ 44

Zabrania się wykorzystywania następujących usług internetowych w sieci Starostwa:

1) prowadzenie rozmów przez Internet (tzw. chat, komunikatory osobiste) z wyłączeniem usług zatwierdzonych przez Starostwo i wskazanych w Rejestrze Oprogramowania,
2) korzystania z portali społecznościowych w celach prywatnych,
3) korzystanie z portali o charakterze seksualnym,
4) prowadzenia gier sieciowych,
5) korzystania z poczty poprzez protokoły POP3, SMTP i IMAP do obsługi kont e-mail innych niż zaakceptowane przez ASI,
6) uprawiania hazardu i udziału w grach losowych.

XII. Postępowanie z nośnikami i ich bezpieczeństwo

§ 45

Dane na stacjach roboczych

1. Dokumenty na stacjach roboczych należy przechowywać w folderze „Moje dokumenty". Zalecane jest umieszczenie folderu na dodatkowej partycji tj. np. dysk „D:\", a nie na tzw. „systemowej" (jest to najczęściej dysk „C:").
2. W szczególności nie należy przechowywać dokumentów na Pulpicie oraz w katalogu głównym dysku.

§ 46

Zarządzanie nośnikami informacji

1. Nośniki informacji zawierające dane osobowe, w tym wydruki, nośniki oprogramowania wraz z kodami aktywacyjnymi produktów przechowuje się w miejscach uniemożliwiających dostęp do nich osób nieuprawnionych.
2. Ogranicza się do niezbędnego minimum ilość wytwarzanych kopii wydruków. Zaleca się zastępować wydruki kopiami na innych nośnikach (np. płyty CD/DVD) jeżeli jest to uzasadnione ekonomicznie.

§ 47

Wycofywanie sprzętu i niszczenie nośników informacji

1. W przypadku tymczasowego (np. w celach serwisowych) lub trwałego (np. sprzedaż, darowizna) przekazywania osobom trzecim sprzętu komputerowego:
   1) wszelkie wymienne nośniki danych muszą być usunięte;
   2) zaleca się także, aby trwałe nośniki danych były usunięte. Jeśli nie jest to możliwe, powinny być usunięte dane zawarte na trwałych nośnikach. Do ich usunięcia zaleca się użyć narzędzi zapewniających trwały i bezpieczny charakter tej operacji np. poprzez wielokrotne zapisanie całego obszaru nośnika losowymi danymi.
2. Za usunięcie wszelkich danych przed przekazaniem sprzętu komputerowego osobom trzecim odpowiada ASI.
3. Dyski twarde, płyty CD/DVD oraz inne komputerowe nośniki danych, zawierające dane osobowe, należy komisyjnie niszczyć w sposób uniemożliwiający odczytanie zapisanych na nich informacji np. poprzez zgniatanie, łamanie, działanie impulsu elektromagnetycznego, całkowite rozpuszczenie. W skład komisji wchodzą ASI, a w uzasadnionych przypadkach także przedstawiciele dostawcy sprzętu. ASI jest zobowiązany do sporządzenia protokołu zniszczenia sprzętu, a następnie do przekazania go IOD.

4. Przenośne nośniki informacji, typu płyta CD/DVD (oprócz dysków twardych i pamięci przenośnych), które nie zawierają danych osobowych, podlegają niszczeniu przez użytkowników po ustaniu ich przydatności.
5. Jeżeli zaistnieje potrzeba zniszczenia nośników zawierających informacje chronione, takich jak zbędne kopie dokumentów papierowych, bądź przechowywanych na płytach CD/DVD itd., każdy pracownik ma obowiązek zniszczyć je w niszczarce, a w przypadku dokumentów papierowych należy uczynić to w poprzek wierszy tekstu lub tabel.
6. Zbędne wydruki, notatki, kopie dokumentów itp. muszą być bezwzględnie niszczone w sposób uniemożliwiający odtworzenie ich treści.
7. Sposób postępowania z dokumentacją określa rozporządzenie Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych oraz inne przepisy w tym zakresie.
8. Niszczenie zbędnych kopii dokumentów, bądź dokumentacji niearchiwalnej, dla której właściwe archiwum państwowe wyraziło zgodę na jej brakowanie, można powierzyć podmiotowi zewnętrznemu przy zachowaniu wymaganych – także w niniejszej polityce - warunków bezpieczeństwa.

XIII. Zapasowe kopie informacji

§ 48

1. Dla Starostwa niezwykle ważne jest, aby wszystkie istotne dane miały kopie zapasowe dzięki czemu w przypadku uszkodzenia systemów komputerowych możliwe będzie odtworzenie danych i kontynuowanie działalności. Kopie zapasowe mają również stanowić gwarancję, że okresowe problemy związane z systemem informatycznym nie będą miały wpływu na działalność operacyjną Starostwa i jego partnerów.
2. Użytkownicy są odpowiedzialni za wykonywanie kopii zapasowych danych przechowywanych na swoich komputerach lokalnych.
3. Kopie ważnych plików z komputerów lokalnych ASI przegrywa na płytę CD/DVD, pamięć zewnętrzną typu USB lub serwer kopii.
4. Nośniki zawierające kopie zapasowe powinny być przechowywane co najmniej do czasu utworzenia piątej kopii, tzn. zawsze powinny być dostępne co najmniej cztery ostatnie kopie.
5. Nośniki zawierające kopie zapasowe są wyposażone w etykiety, na których znajdują się informacje o numerze ewidencyjnym nośnika, zawartości kopii zapasowej, czasie jej wykonania oraz osobie wykonującej kopie.
6. Kopie zapasowe przechowywane są poza pomieszczeniami, w których zostały utworzone, w pomieszczeniach na tyle oddalonych, aby lokalny pożar czy zalanie wodą nie zniszczył jednocześnie nośników w obu pomieszczeniach. Pomieszczenia te powinny zabezpieczać przed zniszczeniem w skutek pożaru, zalania bądź oddziaływaniem silnego pola elektromagnetycznego, jak również przed kradzieżą i nieuprawnionym dostępem.

XIV. Urządzenia mobilne

§ 49

Pracownicy posiadający służbowe urządzenia mobilne tj. telefony komórkowe, smartfony, tablety oraz komputery przenośne są odpowiedzialne za używanie ich w sposób adekwatny do poziomu poufności informacji gromadzonych i przekazywanych przy ich użyciu.

§ 50

1. Obowiązek ochrony urządzenia mobilnego spoczywa na jego użytkowniku.
2. Komputery przenośne podlegają szczególnej ochronie. Ich używanie poza siedzibą Starostwa musi mieć uzasadnienie w realizowanych przez ich użytkownika zadaniach.
3. Dyski w komputerach przenośnych, na których są przetwarzane dane osobowe i są wynoszone poza obszar przetwarzania, należy zabezpieczyć poprzez ich zaszyfrowanie. Kopię klucza szyfrującego przechowuje ASI.
4. Osoby podróżujące z komputerami przenośnymi muszą stosować odpowiednie zasady bezpieczeństwa:
   1) komputery przenośne powinny być zawsze transportowane jako bagaż podręczny,
   2) nie należy ich zostawiać bez dozoru w miejscach takich jak przechowalnie bagażu, wnętrze samochodu, przedziały kolejowe lub innych miejscach zwiększających ryzyko utraty sprzętu gdzie użytkownik nie ma możliwości sprawowania nad nim skutecznego nadzoru.
5. Jeżeli komputer przenośny nie jest użytkowany przez dłuższy okres, musi zostać umieszczony w sejfie lub w szafie zamykanej na zamek.
6. Podczas pracy w miejscach publicznych należy zwracać szczególną uwagę, czy osoby trzecie nie widzą informacji wyświetlanych na ekranie.
7. W przypadku utraty komputera przenośnego Użytkownik natychmiast powiadamia o tym fakcie swojego bezpośredniego przełożonego, IOD i ASI, a w przypadku kradzieży dokonuje również niezwłocznego zgłoszenia popełnienia przestępstwa na policję. W zawiadomieniu do bezpośredniego przełożonego użytkownik, poza danymi przekazanymi do ASI, podaje okoliczności utraty komputera, opis charakteru utraconych danych wraz z podaniem ich znaczenia dla Starostwa. W zawiadomieniu należy określić w szczególności, czy utracono dane osobowe. W tym przypadku, przełożony natychmiast przekazuje notatkę do IOD.

§ 51

Smartfony, tablety

1. Urządzenia mobilne typu smartfony i tablety stanowią szczególną grupę urządzeń i ich ochrona oraz zawartych w nich danych jest ważnym aspektem zapewnienia bezpieczeństwa dostępu do informacji w Starostwie.
2. Użytkownik może aktualizować zainstalowane oprogramowanie tylko w oparciu o legalne, sprawdzone źródła aktualizacji np. „sklep" producenta urządzenia lub systemu operacyjnego.

XV. Ochrona własności intelektualnej

§ 52

Zabronione jest pobieranie z Internetu wszelkich utworów i danych będących przedmiotem ochrony praw autorskich takich jak: programy komputerowe, utwory muzyczne, filmy, gry komputerowe itp. o ile stanowi to naruszenie praw autorskich lub zarządzeń obowiązujących w Starostwie.

§ 53

Aby chronić wszelkie materiały, które mogą być uznane za własność intelektualną, należy:

1) pozyskiwać oprogramowanie tylko z legalnych źródeł, aby zapewnić, że prawa autorskie nie są naruszane,
2) podnosić świadomość pracowników w zakresie ochrony własności intelektualnej,
3) przechowywać dowody własności licencji, oryginalnych dysków, podręczników, instrukcji itp.,
4) stosować zabezpieczenia zapewniające, że nie jest przekraczana maksymalna dozwolona liczba użytkowników,
5) przeprowadzać kontrole sprawdzające, czy zainstalowano tylko autoryzowane oprogramowanie i licencjonowane produkty,
6) opracować i stosować procedury niszczenia lub przekazywania oprogramowania,
7) używać odpowiednie narzędzia audytu oprogramowania,
8) przestrzegać zasad, warunków dotyczących oprogramowania i informacji udostępnianych w sieciach publicznych,
9) sprawdzać zgodność z prawem autorskim w zakresie powielania, przekształcania do innego formatu lub wyodrębniania zarówno baz danych jak i nagrań komercyjnych (filmów, nagrań dźwiękowych),
10) sprawdzać zgodność z prawem autorskim w zakresie kopiowania całości lub części książek, artykułów, raportów lub innych dokumentów (dotyczy również dokumentów w postaci elektronicznej).

XVI. Zarządzanie oprogramowaniem

§ 54

Ewidencja oprogramowania

Oprogramowanie działające w Starostwie jest ewidencjonowane przez ASI w ramach Rejestru Oprogramowania (RO).

Ewidencja powinna zawierać:

1) nazwę programu,
2) dysponenta,
3) ilość licencji,
4) rodzaj oprogramowania,
5) osoby wyznaczone do administracji,
6) datę, od której oprogramowanie zaczęło działać w Starostwie,
7) datę wycofania z użytkowania,
8) potwierdzenie legalności oprogramowania,
9) uwagi.

§ 55

Opis standardowego oprogramowania

1. ASI określa i przechowuje opis standardowego oprogramowania, które powinno być zainstalowane na każdym stanowisku pracy.
2. Do oprogramowania standardowego zalicza się pakiety biurowe, przeglądarki internetowe, programy obsługi poczty elektronicznej lub inne programy narzędziowe dopuszczone do użytkowania w Starostwie.

§ 56

Nowe oprogramowanie

1. Starostwo może wejść w posiadanie nowego oprogramowania:
   1) w drodze zakupu lub nabycia praw do użytkowania,
   2) tworzenia oprogramowania we własnym zakresie,
   3) przekazania w użytkowanie zgodnie z podpisanymi umowami.
2. Działania mające na celu wejście w posiadanie przez Starostwo praw do użytkowania oprogramowania, muszą zostać poprzedzone wydaniem pozytywnej opinii ASI. Wyjątek stanowi testowanie wstępne nowego oprogramowania. W takim przypadku można zainstalować oprogramowanie do przeprowadzenia testów za zgodą ASI.

3. Po nabyciu praw do użytkowania, oprogramowanie jest przekazywane do ASI w celu zainstalowania aplikacji jeśli nie zostało to wykonane przez np. Wykonawcę umowy w ramach jej zakresu. ASI uzupełnia niezwłocznie Rejestr Oprogramowania.
4. Wszystkie licencje, jeśli zawarte umowy nie stanowią inaczej, z uwagi na wartość materialną oraz znaczenie prawne, stanowią aktywa, a ich dysponentem jest ASI, który przechowuje je w miejscu zapewniającym bezpieczeństwo.

§ 57

Aktualizacje oprogramowania

1. Aktualizacje oprogramowania podzielone są na:
   1) poprawki i tzw. „łaty" poprawiające bezpieczeństwo,
   2) poprawki błędów polepszające funkcjonowanie oprogramowania,
   3) nowe wersje oprogramowania zagwarantowane w umowie licencyjnej i nie zmieniające w znaczący sposób funkcjonalności i walorów użytkowych oprogramowania,
   4) nowe wersje oprogramowania, które wymagają nabycia nowej licencji lub zmieniają w znaczący sposób funkcjonalność i walory użytkowe oprogramowania.
2. Przed dokonaniem aktualizacji wrażliwego oprogramowania aplikacyjnego, wskazanego w Rejestrze Oprogramowania, należy wykonywać kopie bezpieczeństwa tego oprogramowania oraz danych przetwarzanych w tym oprogramowaniu.
3. Po aktualizacji serwerowego systemu operacyjnego ASI sprawdza poprawność działania programu. W przypadku błędnego funkcjonowania podejmuje odpowiednie działania.

§ 58

Administracja oprogramowaniem antywirusowym

1. Oprogramowanie antywirusowe powinno być zarządzane centralnie przez ASI w zakresie instalacji oprogramowania na stanowiskach użytkowników, aktualizacji oprogramowania i baz sygnatur, monitoringu stanu aktualizacji na stacjach roboczych, instalacji kluczy licencyjnych oraz śledzenia stanu kluczy, zarządzanie kwarantanną, uruchamianie zadań np. skanowania na odległość.
2. Stacje robocze użytkowników są skonfigurowane tak, aby uruchomienie systemu operacyjnego następowało tylko z dysku twardego, z wyłączeniem wymiennych nośników danych.
3. Program antywirusowy należy skonfigurować w sposób umożliwiający jego automatyczną aktualizację bez interwencji użytkownika.
4. Wszystkie komputery po ich każdorazowym uruchomieniu są poddane podstawowym testom przez program antywirusowy.

5. W przypadku wystąpienia infekcji i braku możliwości automatycznego usunięcia wirusów przez system antywirusowy, ASI podejmuje działania zmierzające do usunięcia zagrożenia.
6. Oprogramowanie antywirusowe jest instalowane w miarę możliwości na wszystkich serwerach sieciowych i konfigurowane w taki sposób, aby działało przez cały czas jako oddzielny proces. Szczególną uwagę należy zwrócić na serwery obsługujące znaczną ilość użytkowników, np. serwery pocztowe lub aplikacji.
7. Sposób zabezpieczenia systemu informatycznego przed działalnością szkodliwego oprogramowania:
   1) ruch w sieci komputerowej Starostwa jest zabezpieczony za pomocą zapór sieciowych;
   2) ruch jest monitorowany przez ASI w celu kontroli przepływu danych między siecią publiczną, a siecią Starostwa oraz kontroli działań w sieciach;
   3) aktualizacje baz danych oprogramowania zabezpieczającego pobierane są automatycznie z serwerów producenta oprogramowania.
8. Programy zabezpieczające należą do aktywów chronionych. Powinny być one zainstalowane na serwerach, każdej stacji roboczej oraz na komputerach przenośnych.
9. Wdrożone oprogramowanie zabezpieczające musi spełniać podstawowe zadania takie jak:
   1) ochronę przed wirusami komputerowymi,
   2) ochronę przed innym szkodliwym i złośliwym oprogramowaniem,
   3) monitorowanie transmisji poprzez interfejsy sieciowe,
   4) monitorowanie zewnętrznych nośników danych (płyty CD/DVD, pamięci flash i inne),
   5) monitorowanie poczty elektronicznej na serwerze poczty oraz stacjach roboczych.
10. Administrator zobowiązany jest do:
    1) aktualizacji programów zabezpieczających,
    2) systematycznego przeglądania logów oraz komunikatów tworzonych przez oprogramowanie zabezpieczające,
    3) natychmiastowej reakcji w przypadku zdarzeń lub incydentów, które zostały wykryte przez oprogramowanie zabezpieczające, mającej na celu zminimalizowanie zagrożenia, naprawę powstałych luk w bezpieczeństwie oraz zabezpieczenie informacji, które mogą okazać się istotne w ustaleniu przyczyn incydentu lub zdarzenia.

XVII. Zarządzanie kopiami nośników i danych

§ 59

1. Zabezpieczenia w postaci kopii zapasowych wymagają wszystkie zbiory przetwarzane w systemach informatycznych, a także inne składniki niezbędne w procesie odtworzenia aplikacji.
2. Procedury odzyskiwania danych z kopii zawarte są w instrukcjach aplikacji wykonujących kopie bezpieczeństwa.
3. ASI wykonuje regularnie kopie zapasowe baz danych przetwarzanych w systemach i systemów przetwarzania tych danych, w przypadku systemów zarządzanych przez Starostwo.
4. Kopie zbiorów przetwarzanych w systemach informatycznych, inne składniki niezbędne do odtworzenia aplikacji oraz pliki przechowywane na dyskach sieciowych są przechowywane co najmniej do czasu utworzenia piątej kopii, tzn. zawsze powinny być dostępne co najmniej cztery ostatnie kopie.
5. Kopie zapisywane są na nośnikach zewnętrznych.
6. Harmonogram wykonywania kopii zapasowych stanowi załącznik nr 14.

XVIII. Zarządzanie systemami

§ 60

Procedury eksploatacyjne oraz zakresy odpowiedzialności

1. W celu zapewnienia prawidłowej i bezpiecznej eksploatacji wszystkich systemów użytkowych wprowadza się, realizuje i dokumentuje procedury związane z cyklem życia tychże systemów. W przypadku nowych systemów procedury obejmują prace projektowe, testowanie, obsługę i ich rozwój.
2. Za bezpieczeństwo i dostęp do komputera oraz za jego prawidłową eksploatację odpowiedzialny jest użytkownik danego komputera.
3. W przypadku korzystania z komputera przez kilku użytkowników, kierownik komórki wyznacza osobę odpowiedzialną za sprzęt. Określa on uprawnienia i obowiązki wszystkich współużytkowników tego sprzętu.
4. Przy realizacji szczególnie odpowiedzialnych zadań wymagany jest podział uprawnień, tak aby wykonanie zadania wymagało ścisłej współpracy co najmniej dwóch osób (autoryzacja co najmniej dwóch osób).
5. Pracownicy mogą zgłaszać wnioski dotyczące:
   1) funkcjonowania systemu teleinformatycznego – do ASI,
   2) bezpieczeństwa systemu teleinformatycznego – do IOD i ASI.
6. Rejestr Systemów Teleinformatycznych (RST) powinien zawierać:
   1) nazwę systemu,
   2) imię i nazwisko pracownika,
   3) identyfikator pracownika,
   4) datę oraz podstawę nadania Pracownikowi uprawnień do systemu,
   5) datę oraz podstawę odebrania uprawnień Pracownikowi.

§ 61

Dostęp do systemów informatycznych

1. W celu realizacji wymogu kontroli dostępu do systemów teleinformatycznych wykorzystuje się wchodzące w skład tych systemów mechanizmy uwierzytelniania użytkowników.
2. Do systemów informatycznych Starostwa mogą uzyskać dostęp wyłącznie uprawnieni użytkownicy.
3. Dostęp musi być indywidualnie zdefiniowany dla każdego użytkownika lub grupy użytkowników.
4. Użytkownik może mieć dostęp jedynie do zasobów, które są mu niezbędne do wykonywania obowiązków służbowych.

5. Tożsamość każdego użytkownika systemów informatycznych Starostwa musi być jednoznacznie określona (identyfikacja) i musi być sprawdzona przed rozpoczęciem pracy w systemie (uwierzytelnienie). W przypadku połączeń dokonywanych z sieci wewnętrznej Starostwa uwierzytelnienie użytkownika polega na sprawdzeniu identyfikatora i hasła przypisanych do profilu użytkownika.
6. Wszystkie systemy informatyczne Starostwa powinny posiadać uaktywnioną opcję wygaszacza ekranu i blokowania dostępu do systemu w przypadku braku aktywności użytkownika. Czas, po którym następuje uaktywnienie wygaszacza ekranu i zablokowanie systemu nie może być dłuższy niż 5 minut. Odblokowanie systemu ekranu wymaga podania hasła.
7. Wszystkie sesje dostępu do zasobów informatycznych (a w szczególności do komend systemu operacyjnego) są zawieszane (lub zrywane) po 10 minutach bezczynności. System umożliwia zablokowanie systemu i/lub uaktywnienie wygaszacza ekranu na żądanie użytkownika.
8. W systemach informatycznych Starostwa nie mogą być aktywne ogólnodostępne profile domyślne typu „gość".

§ 62

Nadanie i zmiana uprawnień dostępu do systemów

1. Kierownik wydziału Starostwa Powiatowego w Ząbkowicach Śląskich jest odpowiedzialny za przygotowanie oraz złożenie wniosku o nadanie/ odebranie uprawnień i upoważnień, który zawiera załącznik nr 11.
2. Wniosek wskazany w pkt. 1 powinien zostać złożony w formie papierowej do ADO.
3. Wniosek składany jest przez Kierownika wydziału w momencie zatrudnienia pracownika oraz zwolnienia.
4. W przypadku braku uzyskania informacji przez IOD o złożeniu wniosku, IOD samodzielnie wygeneruje wniosek w ciągu 7 dni od uzyskania informacji o zatrudnieniu lub zwolnieniu pracownika i prześle Kierownikowi wydziału do edycji, a następnie złożenia do ADO, do czego Kierownik wydziału jest zobligowany.
5. Kierownik wydziału po akceptacji wniosku przez ADO przekazuje opatrzony podpisem wniosek w obszarze nadania lub odebrania uprawnień i upoważnień do ASI.
6. ASI na podstawie otrzymanego wniosku dokonuje nadania lub odebrania uprawnień.
7. Po nadaniu lub odebraniu uprawnień ASI dokonuje aktualizacji w RST i przekazuje informacje o wniosku w formie mailowej do IOD.
8. IOD po uzyskaniu informacji od ASI dokonuje przeszkolenia pracownika za pomocą platformy szkoleniowej, w ramach której pracownik zobowiązany jest do niezwłocznego odbycia szkolenia, a

następnie wytwarza dokumenty wymagane na podstawie Polityki Bezpieczeństwa Informacji, które przekazuje pracownikowi do podpisu.

9. Wniosek wskazany w pkt. 1 jest przechowywany przez ASI. IOD przekazuje wytworzone dokumenty: Oświadczenie o zapoznaniu się z Polityką Bezpieczeństwa Informacji, Upoważnienie do przetwarzania danych osobowych oraz Deklarację o zachowaniu poufności, które stanowią załączniki numer 1, 13 i 15 i po podpisaniu przez pracowników przekazywane są do Wydziału Organizacyjnego i Spraw Obywatelskich.
10. Dokumenty wskazane w pkt. 9 wraz z dokumentacją Polityki Bezpieczeństwa Informacji przechowywane są przez pracownika odpowiedzialnego za sprawy kadrowe.
11. Przyjmuje się, iż potrzeba nadania lub odebrania prawa do korzystania z oprogramowania pracownikowi jest tożsama z koniecznością instalacji/odinstalowania oprogramowania lub ustalenia/zablokowania właściwych praw dostępu.
12. ASI w oparciu o wniosek, o którym mowa w ust. 1 wprowadza uprawnienia do systemu i informuje użytkownika o nadanych uprawnieniach, loginie oraz haśle początkowym. Nazwa profilu użytkownika musi być unikatowa i nie powinna zmieniać się przez cały okres jego pracy w Starostwie, nie licząc przypadków wyjątkowych takich jak np. zmiana nazwiska.
13. Liczba użytkowników mających uprawnienia specjalne do korzystania z zasobów danego systemu informatycznego Starostwa powinna być ograniczona do niezbędnego minimum, jednak nie mogą to być mniej niż 2 osoby.
14. Uprawnienia niezbędne do przeprowadzenia testów poziomu bezpieczeństwa systemów informatycznych Starostwa mogą być wydane na ściśle określony czas, niezbędny do przeprowadzenia testów i wymagają zgody IOD.
15. Konto Użytkownika musi być zablokowane po 45 dniach nieaktywności.
16. Komórka merytoryczny właściwa do spraw pracowniczych („Kadry") zobowiązana jest informować niezwłocznie ASI oraz IOD o planowanych nieobecnościach pracowników dłuższych niż 30 dni.
17. Jeżeli dany podsystem kontroli dostępu do systemów informatycznych Starostwa nie funkcjonuje prawidłowo, uprawnienia użytkowników powinny być zablokowane. W przypadku nieprawidłowego funkcjonowania podsystemów kontroli dostępu, decyzje o dalszych działaniach podejmuje Właściciel zasobu.
18. Uprawnienia posiadane przez użytkownika nie mogą być rozszerzane, o ile nie istnieje umotywowana potrzeba związana ze zmianą zakresu obowiązków użytkownika.
19. Systemy informatyczne Starostwa przetwarzające dane osobowe:
    a) muszą być skonfigurowane w taki sposób, aby uniemożliwić użytkownikom dostęp do zasobów systemów, do których nie mają prawa dostępu.

b) powinny być wyposażone w narzędzia pozwalające na monitorowanie i rejestrowanie działań użytkowników.

20. Osoby trzecie mogą uzyskać profil użytkownika lub uprawnienia w zakresie korzystania z systemów informatycznych Starostwa na podstawie wniosku, którego wzór stanowi załącznik nr 11.
21. Uprawnienia użytkowników dla osób trzecich mogą być przyznane jedynie na czas określony w umowie lub zaakceptowanym wniosku.
22. Osoby trzecie mające dostęp do systemów informatycznych Starostwa muszą podpisać zobowiązanie, że będą przestrzegać zasad dotyczących bezpieczeństwa systemów informatycznych Starostwa.
23. Warunki korzystania z połączenia wewnętrznej sieci Starostwa z systemami zewnętrznymi regulują podpisane umowy, szczegółowo precyzujące warunki techniczne i funkcjonalne połączenia. Umowy muszą być regularnie odnawiane. Umowa musi zawierać klauzulę dotyczącą przestrzegania zasad PBI.
24. Pracownicy odpowiedzialni za współpracę z dostawcami zewnętrznymi są zobowiązani do informowania o zmianach statusu pracowników dostawcy zewnętrznego posiadających dostęp do systemów Starostwa.

§ 63

Ograniczanie przez Starostwo dostępu do zasobów systemów informatycznych przebiega w następujący sposób:

1) fizyczny dostęp do sieci mogą mieć tylko takie urządzenia sieciowe, które uzyskały akceptację ASI,
2) mechanizmy kontroli powinny umożliwiać wykrycie obecności nieautoryzowanych urządzeń sieciowych.

§ 64

Dostęp do aplikacji

Aplikacje użytkowe, eksploatowane w systemie Starostwa, posiadają:

1) mechanizmy autoryzacji i sprawdzania wprowadzanych danych pod względem ich kompletności (dane są oceniane w trakcie procesu ich wprowadzania),
2) procedury postępowania umożliwiające terminową i sumienną korektę danych,
3) mechanizmy kontroli przetwarzanych danych, zapobiegające nieautoryzowanemu usunięciu lub modyfikacji danych.

§ 65

Dostęp do systemów operacyjnych

1. Identyfikacja użytkownika odbywa się na podstawie identyfikatora skojarzonego z hasłem. Z identyfikatorem związane są również prawa dostępu określające uprawnienia użytkownika.
2. Stosowane są konta indywidualne, zapewniające możliwość jednoznacznego wskazania osób wykonujących operacje na systemach lub danych.
3. Użytkownik sam ustala hasło (jest twórcą hasła), którym się posługuje (nie dotyczy pierwszego rejestrowania się w systemie, gdy hasło nadaje ASI).
4. Blokowany jest dostęp do systemu dla użytkownika, który trzykrotnie pod rząd podał błędne hasło, jeżeli taki mechanizm został udostępniony przez system. Odblokowania systemu dokonuje ASI, który nie może w tym celu tworzyć automatów (skryptów) programowych odblokowujących dostęp np. po określonym czasie.
5. Zbędne oprogramowanie narzędziowe i systemowe usuwane jest z systemu przez ASI.

§ 66

Test odbioru i montaż sprzętu

1. Komórka właściwa ds. zamówień publicznych w porozumieniu z ASI powinna w miarę możliwości zapewnić, aby wszystkie zakupione elementy systemów informatycznych były kompatybilne z istniejącym sprzętem komputerowym, aplikacjami i systemami komputerowymi.
2. Wszystkie zainteresowane strony powinny być poinformowane o planowanej instalacji nowego sprzętu komputerowego.
3. Sprzęt komputerowy musi być odpowiednio przetestowany przez ASI przed rozpoczęciem pracy przez Użytkownika.

XIX. Zarządzanie sieciami

§ 67

1. Konfiguracja i administracja urządzeń sieciowych wchodzących w skład sieci LAN jest wykonywana bezpośrednio przez ASI.
2. W przypadku sieci WAN konfiguracja urządzeń sieciowych i administracja tymi urządzeniami może być sprawowana przez usługodawców zewnętrznych, o ile Starostwo ma zapewnioną możliwość kontroli konfiguracji urządzeń sieciowych i zasad ich administracji.
3. Komunikacja w sieci WAN oraz LAN powinna być szyfrowana, przy czym Starostwo musi mieć zapewnioną możliwość kontrolowania konfiguracji urządzeń szyfrujących. Wszelkie zmiany w konfiguracji urządzeń szyfrujących mogą być wykonywane tylko za zgodą i pod kontrolą Starostwa.
4. Zasoby podlegające szczególnej ochronie, m. in. serwery baz danych, aplikacyjne, zlokalizowane są w sekcjach chronionych (wyodrębnionej części sieci podlegającej szczególnej ochronie).

§ 68

1. Sieć komputerowa Starostwa nie może być wykorzystywana do przesyłania informacji niejawnych, o ile informacje te nie są dodatkowo zabezpieczone rozwiązaniami zaakceptowanymi przez Agencję Bezpieczeństwa Wewnętrznego.
2. Dopuszczalne jest tworzenie dedykowanych lokalnych sieci komputerowych przeznaczonych do przetwarzania informacji niejawnych, o ile są one oddzielone od sieci ogólnego przeznaczenia i dostęp do tych sieci jest chroniony rozwiązaniami zaakceptowanymi przez Agencję Bezpieczeństwa Wewnętrznego.
3. Połączenie wewnętrznej sieci Starostwa z Internetem jest realizowane za pośrednictwem dedykowanych urządzeń znajdujących się w gestii ASI zapewniających ochronę zasobów komputerowych znajdujących się w sieci Starostwa.

§ 69

1. ASI odpowiedzialny jest za określenie:
   1) zakresu dopuszczalnych usług sieciowych,
   2) procesu autoryzacji dostępu do zasobów sieciowych,
   3) procedur nadzoru nad urządzeniami sieciowymi,
   4) mechanizmów kontrolnych chroniących sieć Starostwa.

2. Urządzenia sieciowe są skonfigurowane tak, aby spełnione były następujące warunki:
   1) aktywność urządzenia oraz działania użytkowników są rejestrowane w dziennikach zdarzeń ze szczególnym uwzględnieniem sytuacji wyjątkowych,
   2) wbudowane funkcje alarmowe automatycznie powiadamiające ASI w przypadkach wystąpienia sytuacji wyjątkowych są aktywne.
3. Udostępnienie każdej usługi sieciowej wymaga wcześniejszej zgody ASI. Udostępniane są wyłącznie usługi niezbędne do prawidłowego funkcjonowania systemów i całej sieci, których ryzyko udostępnienia zostało określone i zaakceptowane.
4. Kopie konfiguracji urządzeń sieciowych przechowywane są na specjalnie do tego celu przeznaczonych serwerach i trwałych nośnikach danych.
5. Wszystkie poprawki przed wprowadzeniem do systemu są oceniane przez ASI również pod kątem ich wpływu na bieżące bezpieczeństwo infrastruktury informatycznej Starostwa.
6. Pracownicy Starostwa nie powinni się łączyć poprzez sieci bezprzewodowe z innymi sieciami niż udostępnione przez Starostwo bez zgody ASI.

§ 70

Dostęp do urządzeń sieciowych

7. ASI używa unikatowych profili chronionych hasłami do przeprowadzania czynności administracyjnych zgodnie z zasadami kontroli dostępu i wykorzystania haseł.
8. ASI ma obowiązek zmienić hasła dostarczone wraz z pierwszą konfiguracją urządzenia.
9. W sytuacjach wyjątkowych dopuszcza się zdalny dostęp do sieci komputerowej Starostwa dla ASI w celu usunięcia usterek. W takich wypadkach należy zaimplementować mechanizmy „silnego" uwierzytelniania użytkowników.

§ 71

Monitorowanie urządzeń sieciowych

1. Sesje terminalowe do urządzeń sieciowych są automatycznie przerywane po 10 minutach nieaktywności.
2. Należy przeszkolić wszystkich użytkowników w zakresie zgłaszania ASI wszelkich zauważonych anomalii w funkcjonowaniu sieci komputerowej. Użytkownicy mają obowiązek zgłaszania zauważonych anomalii.
3. Wszystkie elementy sieci posiadające funkcje zapisywania dzienników systemowych przesyłają wykonane zapisy do dedykowanych zasobów w sieci Starostwa.

4. ASI regularnie przegląda dzienniki systemowe w poszukiwaniu niestandardowych zapisów świadczących o próbach nieautoryzowanych działań w sieci komputerowej Starostwa. Wszystkie powyższe przypadki niezwłocznie zgłaszane są do IOD.
5. ASI jest okresowo szkolony, aby jego stan wiedzy odpowiadał aktualnym rozwiązaniom i pojawiającym się zagrożeniom w zakresie bezpieczeństwa sieciowego i oprogramowania.

§ 72

Szyfrowanie połączeń

1. Wszystkie punkty zdalnego dostępu do sieci Starostwa muszą zostać zweryfikowane przez ASI.
2. Wszystkie połączenia między siecią Starostwa a sieciami publicznymi muszą odbywać się przy użyciu Zapór Sieciowych.
3. Standardowo tylko połączenia inicjowane przez systemy komputerowe Starostwa są akceptowane przez firewall. Konfiguracja dostępu inicjowanego z sieci publicznej musi być zweryfikowana i zaakceptowana przez ASI.

§ 73

Dostęp do zasobów Starostwa z sieci innych instytucji

1. W celu uzyskania możliwości podłączenia do sieci Starostwa każda instytucja musi wystąpić z odpowiednim wnioskiem do ADO lub osoby przez niego upoważnionej.
2. Wniosek o podłączenie do sieci Starostwa powinien zawierać informacje o celu podłączenia, przewidywanej liczbie podłączonych stanowisk i użytkowników oraz czasie trwania podłączenia.
3. Przed wydaniem decyzji o zgodzie na podłączenie do sieci Starostwa, ADO lub osoba upoważniona zasięga opinii IOD.
4. IOD przed wydaniem opinii na temat podłączenia do sieci Starostwa zasięga opinii merytorycznej ASI w zakresie proponowanych rozwiązań technicznych.
5. W przypadku podłączenia innej instytucji do sieci Starostwa, połączenie powinno być szyfrowane kluczem kryptograficznym (rozwiązania softwarowe lub sprzętowe).
6. Połączenie powinno być zestawiane jedynie między ściśle określonymi adresami IP podłączanej sieci, ściśle określonymi adresami IP sieci wewnętrznej Starostwa oraz dla ściśle określonych portów protokołu TCP/IP.
7. Każdorazowe zestawienie połączenia między siecią innej instytucji a siecią Starostwa powinno być autoryzowane hasłem lub certyfikatem.

8. Użytkownicy z innych instytucji mogą uzyskać ograniczone wsparcie ze strony pracowników Starostwa w zakresie obsługi aplikacji. Zasady i formę tego wsparcia określa Starostwo. W szczególności zdalna zmiana hasła zewnętrznego użytkownika wymaga dodatkowej autoryzacji.

§ 74

Urządzenia innych instytucji w sieci Starostwa

1. Urządzenia innych instytucji np. komputery, switche, routery zainstalowane w budynkach Starostwa i użytkowanych przez Starostwo muszą pracować w wydzielonej fizycznie sieci bez wpływu na działanie infrastruktury teleinformatycznej Starostwa.
2. Zgodę na instalację urządzeń wskazanych w ust. 1 wydaje ADO lub osoba przez niego upoważniona na wniosek instytucji, która jest właścicielem urządzeń.

XX. Zabezpieczenia kryptograficzne

§ 75

Szyfrowanie informacji w Starostwie

Przedmiotem niniejszego rozdziału jest przedstawienie zaleceń dotyczących zasad szyfrowania informacji w Starostwie. Zasady stosowania kryptografii oraz zarządzania kluczami będą dotyczyły wszystkich systemów przetwarzania, transmitowania i przechowywania danych należących do Starostwa lub przez niego zarządzanych, w przypadku podjęcia decyzji o ich wdrożeniu.

§ 76

Zasady stosowania kryptografii

1. Zaleca się, aby Starostwo w zakresie realizacji i udoskonalania PBI wprowadziło zabezpieczenia kryptograficzne.
2. Starostwo wykorzystując infrastrukturę klucza publicznego, opracuje odpowiednie procedury i instrukcje związane z polityką ich używania, a także zasady bezpieczeństwa związane z zabezpieczeniami kryptograficznymi.
3. Klucze stosowane do szyfrowania danych Starostwa klasyfikowane są zawsze jako zasoby kategorii I. Dostęp do kluczy kodowych ogranicza się wyłącznie do osób, którym są one niezbędne do wykonywania obowiązków służbowych.
4. Nie wolno ujawniać kluczy kodowych: konsultantom, podwykonawcom, nieuprawnionym pracownikom, pracownikom tymczasowym ani osobom trzecim.
5. W przypadku zastosowania szyfrowania wszelkie urządzenia i materiały stosowane do generowania kluczy szyfrujących oraz ich kopie zapasowe muszą być zabezpieczone przed dostępem osób niepowołanych. W przypadku szyfrowania opartego na technologii pary kluczy kryptograficznych prywatnego i publicznego ochronie podlega jedynie klucz prywatny.
6. W przypadku, gdy stosowane jest szyfrowanie oraz podpis elektroniczny należy dla każdego z tych elementów stosować odrębny klucz.
7. Klucze używane w urządzeniach komputerowych muszą być przechowywane przy zachowaniu takich środków ostrożności, jak w przypadku haseł do profili uprzywilejowanych. Klucze indywidualne muszą być przechowywane przy zachowaniu takich środków ostrożności, jak w przypadku haseł dostępu.

§ 77

Zarządzanie kluczami

1. W celu zapewnienia właściwej ochrony zaszyfrowanych informacji zawartych w systemach informatycznych Starostwa zaleca się stosowanie automatycznych systemów zarządzania kluczami szyfrowymi.
2. W przypadku stosowania szyfrowania danych ASI odpowiada za administrowanie kluczami szyfrowymi. Kopię kluczy szyfrowych przechowuje ASI w przeznaczonym do tego miejscu.
3. Tam, gdzie jest to potrzebne, system szyfrowania powinien uwzględniać wymóg, aby jedna osoba nie znała w pełni żadnego klucza szyfrowego. Musi być to osiągnięte w drodze podziału obowiązków służbowych i spełniać zasadę podwójnej kontroli. Podział obowiązków dotyczy zaangażowania więcej niż jednej osoby do wykonywania ważnej czynności, natomiast podwójna kontrola oznacza, że do wykonania ważnej czynności konieczna jest jednoczesna obecność dwóch osób.
4. Wszystkie klucze szyfrowe muszą mieć zdefiniowany okres ich ważności. Zmiana klucza musi nastąpić nie później niż w terminie upływu jego ważności. Nowy klucz kodowy musi zostać wygenerowany ze stosownym wyprzedzeniem.
5. Przez cały okres ważności informacji zaszyfrowanej z użyciem klucza szyfrującego, klucz ten musi być przechowywany i zabezpieczony przed dostępem osób niepowołanych.
6. Klucze szyfrowe chroni się przed ujawnieniem osobom nieupoważnionym środkami technicznymi takimi jak szyfrowanie z zastosowaniem odrębnego klucza lub przy zastosowaniu sprzętu odpornego na manipulacje przez osoby niepowołane.
7. Klucze szyfrowe przed przesłaniem ich siecią telekomunikacyjną muszą zostać zaszyfrowane. Szyfrowanie kluczy odbywa się z zastosowaniem silniejszego algorytmu niż używany do szyfrowania innych danych.
8. W przypadku przechowywania zaszyfrowanych informacji na nośniku komputerowym, zabrania się przechowywania na tym samym nośniku kluczy szyfrowych i związanych z nimi materiałów w postaci niezaszyfrowanej.

XXI. Sprzęt komputerowy

§ 78

Zabezpieczenie sprzętu

1. Komputery przenośne oraz stacjonarne powinny być zabezpieczone przed niepowołanym uruchomieniem poprzez zastosowanie hasła logowania do systemu operacyjnego.
2. Dyski komputerów przenośnych oraz stacjonarnych, na których przetwarzane są dane osobowe, powinny być szyfrowane.
3. Informacje przetwarzane w komputerach przenośnych lub stacjonarnych powinny być w odpowiedni sposób zabezpieczone przed nieautoryzowanym dostępem.
4. Serwery, urządzenia sieci teleinformatycznej, centrale telefoniczne, urządzenia zapewniające zasilanie bezprzerwowe oraz rozdzielnie energetyczne zasilające wymieniony sprzęt, magazyny kopii zapasowych i archiwa są umieszczone w wydzielonych pomieszczeniach.
5. Urządzenia infrastruktury zapewniające warunki środowiska, w którym przetwarzane są informacje, są przeglądane i konserwowane zgodnie z instrukcjami i wymaganiami ich producentów.

§ 79

Konserwacja i naprawy sprzętu

1. Sprzęt, stanowiący zasób teleinformatyczny podlega konserwacji według ustalonego planu, wynikającego z zaleceń jego producenta.
2. Konserwacja i naprawy mogą być prowadzone jedynie przez uprawniony personel Starostwa lub podmiot zewnętrzny świadczący tego rodzaju usługi na podstawie umowy lub w ramach gwarancji.
3. W przypadku, gdy na nośnikach danych, stanowiących integralną część sprzętu przekazywanego do naprawy, znajdują się dane chronione, sprzęt taki naprawiany jest pod nadzorem uprawnionego pracownika Starostwa. Jeżeli zaś taki nadzór nie jest możliwy, dane chronione są skutecznie usuwane. O ile zachodzi taka możliwość, usuwane dane są uprzednio zarchiwizowane.
4. Jeżeli gwarant, w ramach naprawy gwarancyjnej, żąda zwrotu urządzenia służącego do przechowywania danych (np. dyski twarde), dane znajdujące się w takim urządzeniu zostają z niego trwale usunięte.
5. W przypadku zbywania sprzętu należy skutecznie usunąć z niego wszystkie dane lub zbyć sprzęt bez nośników danych.

XXII. Monitorowanie naruszenia zasad PBI

§ 80

Monitorowanie i analiza

1. Każdy system informatyczny Starostwa jest wyposażony w mechanizmy umożliwiające Administratorowi weryfikację stanu zabezpieczeń systemu. Mechanizmy te umożliwiają co najmniej rejestrację prób uzyskania dostępu do systemu.
2. Systemy informatyczne Starostwa posiadają mechanizmy uniemożliwiające automatyczną instalację nieautoryzowanego oprogramowania.
3. Systemy informatyczne Starostwa zawierają dzienniki rejestrujące istotne zdarzenia dotyczące działań użytkowników i funkcjonowania urządzeń.
4. Jeżeli nie regulują tego inaczej przepisy szczegółowe, dzienniki zawierające informacje na temat zdarzeń dotyczących zabezpieczeń systemów informatycznych powinny być przechowywane przez co najmniej 12 miesięcy. W tym okresie dzienniki powinny być zabezpieczone tak, aby uniemożliwić ich modyfikację, a dostęp do nich mają wyłącznie osoby upoważnione.
5. Wszystkie rejestry zdarzeń są regularnie przeglądane przez ASI.
6. W celu ograniczenia nadużyć, zwiększenia odpowiedzialności użytkowników i umożliwienia zarządzania systemami należy zapewnić możliwość rekonstrukcji kluczowych działań użytkowników na podstawie dzienników i innych zarejestrowanych materiałów.
7. Zegary komputerów systemów informatycznych Starostwa są zsynchronizowane, aby ułatwić analizę zdarzeń zachodzących symultanicznie w kilku systemach.
8. ASI regularnie przegląda logi systemowe w poszukiwaniu zdarzeń mogących wskazywać na próby niewłaściwego wykorzystania systemu lub jego wadliwego działania.
9. Dostęp do informacji zawartych w dziennikach mogą mieć tylko upoważnione osoby będące pracownikami komórek kontroli wewnętrznej, audytora wewnętrznego, pracownicy odpowiedzialni za bezpieczeństwo systemów, pracownicy zarządzający systemami oraz IOD. Informacje te mogą być udostępniane audytorom zewnętrznym w związku z realizowaną przez nich kontrolą.

§ 81

Naruszenie zasad PBI może być skutkiem różnych czynników, w szczególności:

1) szkodliwego wpływu środowiska na system przetwarzania informacji, zewnętrznych zdarzeń losowych dotyczących systemu przetwarzania informacji,

2) zamierzonych lub niezamierzonych czynności użytkowników upoważnionych do przetwarzania informacji,
3) nieuprawnionych działań osób nieupoważnionych do przetwarzania informacji.

§ 82

Za naruszenie zasad PBI uważa się, w szczególności:

1) ujawnienie indywidualnych haseł dostępu użytkowników do systemu przetwarzającego informacje,
2) wykonanie nieuprawnionych kopii informacji – wydruki, kopie na nośnikach zewnętrznych np. pamięci USB itp.,
3) niewykonywanie kopii bezpieczeństwa,
4) niewłaściwe parametry środowiska, takie jak temperatura czy wilgotność w pomieszczeniach, w których znajdują się systemy przetwarzające informacje,
5) naruszenie lub próby naruszenia integralności systemu przeznaczonego do przetwarzania informacji,
6) naruszenie lub próby naruszenia integralności informacji w systemie przetwarzania – wszelkie modyfikacje (dodanie, zmiana, usunięcie), zniszczenie lub próby ich dokonania przez osoby nieupoważnione lub upoważnione działające w złej wierze lub jako błąd osoby uprawnionej (np. zmiana zawartości danych, utrata całości lub części danych),
7) naruszenie poufności poprzez celowe lub nieświadome przekazanie informacji osobie nieuprawnionej do ich otrzymania,
8) naruszenie ochrony informacji w systemie np. nieautoryzowane logowanie do systemu lub inny objaw wskazujący na próbę lub działanie związane z nielegalnym dostępem do systemu z zewnątrz,
9) nieuprawniony dostęp lub próba dostępu do systemu przetwarzania informacji np. nieuprawniona praca na koncie użytkownika czy istnienie nieautoryzowanych kont dostępu do informacji, pojawienie się nowych lub nie zablokowanie czy usunięcie starych kont dostępu,
10) umożliwienie dostępu do informacji osobie nieuprawnionej np.: pozostawienie kopii danych (w drukarce/skanerze, ksero, na stole), nie zablokowanie dostępu do systemu (podczas nieobecności osoby uprawnionej), brak nadzoru nad serwisantami i innymi osobami nieuprawnionymi przebywającymi w pomieszczeniach, gdzie przetwarza się informacje,
11) nieuprawniony dostęp lub próba dostępu do pomieszczeń, gdzie przetwarza się informacje,
12) zmiana lub usunięcie informacji zapisanych na kopiach bezpieczeństwa lub kopiach archiwalnych,
13) brak nośnika zawierającego informacje – kradzież lub zaginięcie wydruku, kopii bezpieczeństwa, CD/DVD czy dysku,

14) niewłaściwe niszczenie nośników informacji pozwalające na ich odczyt – wyrzucanie na śmietnik niezniszczonych nośników np.: wydruk, CD/DVD, pamięć USB,
15) błędne nadanie uprawnień do przetwarzania informacji lub nadanie uprawnień osobie nie spełniającej wymagań.

§ 83

Reagowanie na naruszenia zasad PBI i niewłaściwe funkcjonowanie systemu

1. Każdy pracownik, który stwierdził naruszenie bezpieczeństwa informacji ma obowiązek zgłosić ten fakt ASI i/lub IOD.
2. Każdy pracownik, który stwierdził niewłaściwe funkcjonowanie systemu teleinformatycznego ma obowiązek zgłosić ten fakt do przełożonego lub ASI. Jeśli nieprawidłowe funkcjonowanie systemu ma związek z naruszeniem PBI, ASI natychmiast informuje o tym IOD.
3. W celu zapewnienia dowodów dla celów wyjaśniającego, postępowania sądowego i procedury dyscyplinarnej, w przypadku podejrzenia przestępstwa lub nadużycia komputerowego, należy zgromadzić odpowiednie informacje o incydencie. Powinny być one bezpiecznie przechowywane poza systemami komputerowymi do czasu, aż Starostwo podejmie decyzję o podjęciu działań prawnych lub innym ich wykorzystaniu.
4. Informacje, które należy zgromadzić natychmiast po wystąpieniu incydentu obejmują dzienniki systemowe, zapisy przebiegu przetwarzania, inne wskaźniki aktualnego stanu systemu, jak również kopie zbiorów będących przedmiotem potencjalnego przestępstwa. W przypadku poważnych naruszeń bezpieczeństwa należy zachować pełne kopie systemów.
5. IOD wspólnie z ASI podejmuje postępowanie wyjaśniające, mające na celu ustalenie przyczyn i osób odpowiedzialnych za naruszenie bezpieczeństwa informacji. IOD sporządza szczegółowy raport z przeprowadzonego postępowania i przedstawia go ADO.
6. Przygotowany raport jest podstawą zgłoszenia przez ADO organowi nadzorczemu, nie później niż w ciągu 72 godzin, faktu stwierdzenia naruszenia bezpieczeństwa informacji, chyba że jest mało prawdopodobne, by naruszenie skutkowało naruszeniem praw lub wolności osób fizycznych.
7. Wobec Pracowników winnych naruszenia bezpieczeństwa informacji na skutek nie przestrzegania obowiązujących zasad może zostać wszczęte postępowanie dyscyplinarne.

XXIII. Załączniki do PBI

§ 84

Załączniki:

1) Oświadczenie o zapoznaniu się z Polityką Bezpieczeństwa Informacji.
2) Wniosek o wpis do rejestru czynności przetwarzania
3) Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe
4) Wzór rejestru czynności przetwarzania
5) Wykaz udostępnień D.O. osobom których dotyczą
6) Wykaz udostępnień D.O. innym podmiotom
7) Wykaz podmiotów, którym powierzono przetwarzania D.O.
8) Lista przykładowych incydentów
9) Protokół obsługi incydentu
10) Rejestr incydentów
11) Wniosek o nadanie / odebranie uprawnień i upoważnień
12) Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych
13) Upoważnienie do przetwarzania danych osobowych
14) Harmonogram tworzenia kopii zapasowych
15) Deklaracja o zachowaniu poufności
16) Procedura retencji danych w Biuletynie Informacji Publicznej

STAROSTA ZĄBKOWICKI
Roman Fester

WNIOSEK O NADANIE/ODEBRANIE UPRAWNIEŃ I UPOWAŻNIEŃ

RODZAJ WNIOSKU *zaznaczyć odpowiednią kratkę*	Nadanie uprawnień	☐	*oznaczyć właściwe*	Odebranie uprawnień	☐
DATA OBOWIĄZYWANIA **) wpisać w przypadku upoważnienia okresowego*	od ...../...../..... RR MM DD		do*) ...../...../..... RR MM DD		
DANE IDENTYFIKACYJNE PRACOWNIKA	Imię i nazwisko ..... Stanowisko				
DOSTĘP DO POMIESZCZEŃ					
Pobieranie klucza do pomieszczenia	TAK ☐		NIE ☐		
Numer pokoju/ów:					

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

(wnioskodawca zaznacza znakiem „x" właściwe zbiory danych osobowych)

	DZIENNIKI BUDOWY		KARY ZA NIEZAREJESTROWANIE POJAZDU
	AKTA OSOBOWE DYREKTORÓW SZKÓŁ I PLACÓWEK		KIEROWCY
	ARCHIWUM ZAKŁADOWE		KONKURSY OFERT NA REALIZACJĘ ZADAŃ PUBLICZNYCH
	ARKUSZE ORGANIZACYJNE SZKÓŁ I PLACÓWEK		KORESPONDENCJA PRZYCHODZĄCA I WYCHODZĄCA
	AWANS ZAWODOWY NAUCZYCIELI		LICENJCE, ZEZWOLENIA I ZAŚWIADCZENIA NA PRZEWÓZ OSÓB I RZECZY
	CZYNNOŚCI DOTYCZĄCE UŻYTKOWANIA WIECZYSTEGO		NALICZANIE WYNAGRODZEŃ PRACOWNIKÓW
	CZŁONKOWIE RADY POWIATU		NIELETNI SKIEROWANI DO MŁODZIEŻOWYCH OŚRODKÓW WYCHOWAWCZYCH I MŁODZIEŻOWYCH OŚRODKÓW SOCJOTERAPII
	DANE OSOBOWE STUDENTÓW / PRAKTYKANTÓW / STAŻYSTÓW		OŚWIADCZENIA MAJĄTKOWE
	DOKUMENTACJA PRACOWNICZA		POSTĘPOWANIE W ZAKRESIE PRAW KONSUMENCKICH
	DOKUMENTACJA UBEZPIECZENIOWA PRACOWNIKÓW		REJESTR DECYZJI ADMINISTRACYJNYCH
	DZIECI I MŁODZIEŻ SKIEROWANA DO SZKÓŁ SPECJALNYCH		REJESTR POSTANOWIEŃ WYDZIAŁU BUDOWNICTWA
	EWIDENCJA DIAGNOSTÓW ORAZ STACJI DIAGNOSTYCZNYCH		REJESTR SKARG, WNIOSKÓW I PETYCJI
	EWIDENCJA GRUNTÓW I BUDYNKÓW		REJESTR SPRZĘTU SŁUŻĄCEGO DO POŁOWU RYB
	EWIDENCJA KIEROWCÓW		REJESTR ZGŁOSZEŃ PRAC GEODEZYJNYCH I KARTOGRAFICZNYCH
	EWIDENCJA MATERIAŁÓW ZASOBÓW		ŚWIADCZENIA Z ZFŚS
	EWIDENCJA POJAZDÓW		UDOSTĘPNIENIA INFORMACJI PUBLICZNEJ
	EWIDENCJA RZECZY ZNALEZIONYCH		UMOWY CYWILNOPRAWNE
	EWIDENCJA WYDANYCH LEGITYMACJI INSTRUKTOROM NAUKI JAZDY		UPOWAŻNIENIA I PEŁNOMOCNICTWA
	FAKTURY / DOWODY KSIĘGOWE		WNIOSKI
	GATUNKI ZWIERZĄT NIEBIEZPIECZNYCH		WYKŁADOWCY

	INSTRUKTORYZ NAUKI JAZDY		ZAMÓWIENIA PUBLICZNE
	KANDYDACI NA INSTRUKTORÓW NAUKI JAZDY		ZAŚWIADCZENIA O ODRĘBNOŚCI LOKALU
	KANDYDACI NA KIEROWCÓW		ZGŁOSZENIA BUDOWY
	KANDYDACI NA WYKŁADOWCÓW		Baza danych związanych z realizowaniem zadań Instytucji Zarządzającej przez Zarząd Województwa Dolnośląskiego w ramach RPO WD na lata 2014-2020
	KARTY WĘDKARSKIE		Centralny system teleinformatyczny wspierający realizację programów operacyjnych
INNY ZBIÓR		.....	
Zakres upoważnienia		Zgodnie z zakresem obowiązków	

DOSTĘP DO SYSTEMU INFORMATYCZNEGO (wypełnia wnioskodawca)

Nazwa aplikacji/systemu	Rodzaj/ zakres/ poziom uprawnień *(*jeżeli wymaga ograniczeń)*	Identyfikator *(Przyznaje ASI)*
1. EWID 2007		
2. E-PUAP		
3. QNT F-K		
4. QNT Faktury		
5. QNT Kadry		
6. QNT Płace		
7. QNT Środki trwałe		
8. QNT AZF		
9. QNT ASA		
10. QNT QDeklaracje		
11. QNT PPK		
12. Płatnik		

WNIOSKODAWCA	
DATA WYPEŁNIENIA WNIOSKU	**IMIĘ i NAZWISKO/STANOWISKO/PODPIS I PIECZĄTKA**

AKCEPTACJA WNIOSKU	
DATA AKCEPTACJI WNIOSKU	**PODPIS I PIECZĄTKA ADO**

NADANIE UPRAWNIEŃ

POTWIERDZENIE NADANIA UPRAWNIEŃ	
DATA NADANIA UPRAWNIEŃ	**PODPIS I PIECZĄTKA ASI**

ODEBRANIE UPRAWNIEŃ

POTWIERDZENIE ODEBRANIA UPRAWNIEŃ	
DATA ODEBRANIA UPRAWNIEŃ	**PODPIS I PIECZĄTKA ASI**

STAROSTA ZĄBKOWICKI
Roman Fester