POLITYKA BEZPIECZEŃSTWA INFORMACJI

Rezydencji „KORAB”

1. Wstęp.

Przez pojęcie „Polityka Bezpieczeństwa Informacji” należy rozumieć zestaw praw, reguł i praktycznych doświadczeń regulujących sposób zarządzania, ochrony i dystrybucji informacji wrażliwej wewnątrz organizacji. Kierownictwo każdej jednostki organizacyjnej, zobowiązane jest przepisami prawa do stworzenia optymalnego modelu zabezpieczeń technicznych i elektronicznych przetwarzanych informacji. Klasyfikacja informacji w postaci aktywów relewantnych – istotnych z punktu widzenia organizacji, w płaszczyznach działania JO, stanowi podstawowe zadanie osób zaangażowanych w procesie tworzenia zasad zabezpieczenia zasobów informacyjnych. Istotnym wyzwaniem jest kwalifikowanie kategorii potencjalnych zagrożeń integralności informacji, w coraz większym stopniu instytucje, ich systemy i sieci informatyczne stają w obliczu zagrożeń pochodzących z rozmaitych źródeł, takich jak oszustwa dokonywane za pomocą komputerów, komunikatorów, urządzeń mobilnych oraz sieci. Szpiegostwo, sabotaż, wandalizm, pożar lub powódź to zjawiska aktywnej lub losowej utraty informacji oraz danych istotnych w procesie dostarczania usług. Poufność, dostępność i integralność informacji przy zachowaniu jej autentyczności, rozliczalności oraz niezaprzeczalności ma podstawowe znaczenie dla utrzymania płynności finansowej, zgodności z przepisami prawa oraz wizerunku jednostki.

1. Dokument PBI zwraca uwagę na konsekwencje, jakie mogą ponosić osoby przekraczające określone granice oraz procedury postępowania dla zapobiegania i minimalizowania skutków zagrożeń. Jednocześnie deklaruje zaangażowanie kierownictwa i wyznacza systematyczne procesowe podejście instytucji do zarządzania bezpieczeństwem informacji.
2. Omawiane zasady opierają się na obowiązujących uregulowaniach prawnych, a należą do nich w szczególności:
    a) ochrona danych osobowych i prywatności osób,
    b) ochrona dokumentów finansowych,
    c) dokumenty związane z PBI,
    d) odpowiedzialność związana z bezpieczeństwem informacji,
    e) edukacja użytkowników w dziedzinie bezpieczeństwa informacji,
    f) wsparcie i zaangażowanie kadry kierowniczej,

g) systematyczne i planowane w zakresie potrzeb, upowszechnianie wytycznych dotyczących PBI wśród wszystkich osób zaangażowanych w procesach przetwarzania informacji,

h) zgłaszanie przypadków naruszenia bezpieczeństwa informacji,

i) ocena zjawisk i potencjalnych zagrożeń.

3. Głównym celem niniejszej PBI jest organizacyjne, fizyczne i logiczne zabezpieczenie posiadanych danych (informacji) oraz planowane kształcenie użytkowników systemu ochrony bezpieczeństwa informacji, w zróżnicowanych wariantach prowadzonych zajęć [wewnętrzne instruktaże, analizy przypadków, omówienia zdarzeń].
4. PBI jest jednocześnie materiałem określającym zadania w zakresie właściwej realizacji poufności i integralności informacji przez nadanie uprawnień legalizujących przetwarzanie danych użytkownikom systemu ochrony informacji.
5. Niniejsza PBI została opracowana na podstawie rozporządzenia KRI oraz Polskiej Normy PN-ISO/IEC 27001.

2. Cel oraz zakres Polityki Bezpieczeństwa Informacji - PBI

Nadrzędnym celem PBI jest:

1. Zapewnienie właściwej ochrony zasobów.
2. Właściwy dobór zabezpieczeń (środków bezpieczeństwa) oparty na rezultatach i wnioskach wynikających z procesów szacowania i postępowania z ryzykiem, wymagań prawnych, wymagań nadzoru, zobowiązań kontraktowych oraz pozostałych wymagań dotyczących bezpieczeństwa informacji w Rezydencji „KORAB".

Zakres obowiązywania PBI w Rezydencji „KORAB":

1. Niniejszy dokument dotyczy wszystkich pracowników w rozumieniu ustawy Kodeks Pracy, a także innych osób mających dostęp do informacji chronionych w Rezydencji „KORAB" (np. pracowników firm zewnętrznych realizujących prace na rzecz Rezydecji „KORAB").
2. Dokument ma zastosowanie do wszystkich informacji chronionych niezależnie od formy, w jakiej są przechowywane (papierowej, elektronicznej, video lub innej).
3. Z dokumentem PBI są zobowiązani zapoznać się wszyscy pracownicy mający dostęp do danych osobowych/informacji.

3. Podstawa Prawna

Polityka bezpieczeństwa informacji oraz inne dokumenty szczegółowe związane z bezpieczeństwem informacji opierają się na:

1. Polskiej Normie PN-ISO/IEC 27001:2014, 27005:2014.
2. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, zwane dalej jako UODO;
3. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 zadnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, zwane dalej jako RODO

4. Słownik podstawowych pojęć:

Przez użyte w treści PBI sformułowania należy rozumieć:

a.i.1. ***„KORAB”*** – Rezydencja „KORAB” w Międzyzdrojach, Dąbrówki 3, 72-500 Międzyzdroje, Administrator Danych Osobowych (ADO), reprezentowany przez Dyrektora,

a.i.2. ***PBI*** – Polityka Bezpieczeństwa Informacji obowiązująca w Rezydencji „KORAB”,

a.i.3. ***PBDO*** - Polityka Bezpieczeństwa Danych Osobowych obowiązująca w Rezydencji KORAB”

a.i.4. ***zbiór danych*** - oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;

a.i.5. ***aktywa*** – wszystko co ma wartość dla organizacji (zasoby),

a.i.6. ***dostępność*** – właściwość bycia dostępnym i użytecznym na żądanie upoważnionego podmiotu,

a.i.7. ***poufność*** – właściwość polegająca na tym, że informacja nie jest udostępniana lub wyjawiana nieupoważnionym osobom, podmiotom lub procesom,

a.i.8. ***integralność*** – właściwość polegająca na zapewnieniu dokładności i kompletności aktywów,

a.i.9. ***autentyczność***- właściwość polegająca na tym, że pochodzenie lub zawartość danych opisujących obiekt są takie, jak deklarowane,

a.i.10. ***niezaprzeczalność*** - brak możliwości zanegowania swego uczestnictwa w całości lub w części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie,

a.i.11. ***rozliczalność*** - funkcja umożliwiająca przypisanie w sposób jednoznaczny działania użytkownika lub podmiotu tylko temu użytkownikowi lub podmiotowi,

a.i.12. ***uwierzytelnianie*** - rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości użytkownika,

a.i.13. ***bezpieczeństwo informacji*** – zachowanie poufności, integralności i dostępności informacji; dodatkowo mogą być brane pod uwagę inne własności, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność,

a.i.14. ***zdarzenie związane z bezpieczeństwem informacji*** – jest określonym stanem systemu, usługi lub sieci, który wskazuje na możliwe naruszenie polityki bezpieczeństwa informacji, błąd zabezpieczenia lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem,

a.i.15. ***incydent związany z bezpieczeństwem informacji –*** jest to pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji,

a.i.16. ***postępowanie z ryzykiem*** – proces wyboru i wdrażania środków modyfikujących ryzyko,

a.i.17. ***UODO*** - ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych:

a.i.18. ***RODO*** - Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 zadnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE,

a.i.19. ***Administrator, dalej jako „ADO”*** - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to

również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania;

a.i.20. ***Administrator Systemu Informatycznego, dalej jako „ASI”*** - pracownik wyznaczony przez ADO, odpowiedzialny za bezpieczeństwo i funkcjonowanie systemów informatycznych oraz stosowanie technicznych i organizacyjnych środków ochrony w tym systemie,

a.i.21. ***podmiot przetwarzający*** -oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora

a.i.22. ***Użytkownik*** - osoba upoważniona przez ADO do przetwarzania danych osobowych (pracownik, osoba wykonująca pracę na podstawie umowy cywilno-prawnej, osoba odbywająca staż pracy, praktykant),

a.i.23. ***dane osobowe*** - oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności 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;

a.i.24. ***sieć publiczna*** – publiczna sieć telekomunikacyjna, niebędąca siecią wewnętrzną wykorzystywana głównie do świadczenia publicznie dostępnych usług telekomunikacyjnych,

a.i.25. ***identyfikator użytkownika*** - jest to ciąg znaków literowych (login) jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,

a.i.26. ***sieć telekomunikacyjna*** - urządzenia telekomunikacyjne i linie telekomunikacyjne, zestawione i połączone w sposób umożliwiający przekaz sygnałów pomiędzy określonymi zakończeniami sieci, za pomocą przewodów, fal radiowych bądź optycznych lub innych środków wykorzystujących energię elektromagnetyczną,

a.i.27. ***zabezpieczenie danych w systemie informatycznym*** - wdrożenie i wykorzystywanie stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem,

a.i.28. ***system informatyczny*** - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,

a.i.29. ***usuwanie danych osobowych***- rozumie się przez to zniszczenie zbiorów danych, danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,

a.i.30. ***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,

a.i.31. ***ograniczenie przetwarzania*** - oznacza oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania

a.i.32. ***pseudonimizacja*** - oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;

a.i.33. ***profilowanie*** - oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;

a.i.34. ***PUODO*** – Prezes Urzędu Ochrony Danych Osobowych – organ do spraw ochrony danych osobowych, powoływany i odwoływany przez Sejm za zgodą Senatu.

a.i.35. ***elektroniczne nośniki informacji – „ENI”*** - zewnętrzne nośniki danych, w szczególności płyty CD, DVD, PenDrive, pamięci typu FLASH,

5. Osoby odpowiedzialne za bezpieczeństwo informacji i przetwarzanie danych osobowych

1. **Administrator /ADO/**

1. Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane.

2. Jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki, o których mowa w ust. 1, obejmują wdrożenie przez administratora odpowiednich polityk ochrony danych.

2. **Administrator Systemu Informatycznego /ASI/**

Administrator Systemu Informatycznego realizuje zadania w zakresie zarządzania i bieżącego nadzoru nad systemem informatycznym Administratora Danych, w tym zwłaszcza:

1) zarządza systemem informatycznym przetwarzającym informacje, posługując się hasłem dostępu do wszystkich stacji roboczych z pozycji administratora,
2) przeciwdziała dostępowi osób niepowołanych do systemu informatycznego, w którym przetwarzane są dane,
3) przydziela każdemu użytkownikowi identyfikator oraz hasło do systemu informatycznego oraz dokonuje ewentualnych modyfikacji uprawnień, a także usuwa lub wyłącza konta użytkowników zgodnie z zasadami określonymi w instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych,
4) nadzoruje działanie mechanizmów uwierzytelniania użytkowników oraz kontroli

dostępu do danych,

5) podejmuje działania w zakresie ustalania i kontroli identyfikatorów dostępu do systemu informatycznego,
6) wyrejestrowuje użytkowników,
7) zmienia w poszczególnych stacjach roboczych hasła dostępu, ujawniając je wyłącznie danemu użytkownikowi oraz w razie potrzeby, Administratorowi Bezpieczeństwa Informacji lub Administratorowi Danych,
8) w sytuacji stwierdzenia naruszenia zabezpieczeń systemu informatycznego informuje ADO o naruszeniu i współdziała z nim przy usuwaniu skutków naruszenia,
9) prowadzi szczegółową dokumentację naruszeń bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym,
10) sprawuje nadzór nad wykonywaniem napraw, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe, nad wykonywaniem kopii zabezpieczających, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu informatycznego,
11) prowadzi rejestr wykonywanych kopii zabezpieczających,
12) podejmuje działania służące zapewnieniu niezawodności zasilania komputerów, innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych oraz zapewnieniu bezpiecznej wymiany danych w sieci wewnętrznej i bezpiecznej teletransmisji,
13) prowadzi inwentaryzację sprzętu komputerowego i oprogramowania.

6. Struktura dokumentu Polityki bezpieczeństwa informacji

Na Politykę Bezpieczeństwa informacji składają się następujące załączniki:

Zał. nr 1 Polityka bezpieczeństwa danych osobowych.

7. Monitorowanie uprawnień

Polityka bezpieczeństwa informacji i dokumenty z nią powiązane powinny być poddawane regularnemu przeglądowi, w celu utrzymania zapisów w aktualności względem zmieniającego się stanu faktycznego jednostki oraz wymagań wynikających z obowiązujących przepisów prawa. Administrator Danych Osobowych zobowiązany jest do dokonywania co najmniej raz na kwartał okresowej kontroli przyznanych pracownikom uprawnień, również w systemach informatycznych.

8. Zapewnienie szkolenia osób zaangażowanych w proces przewarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak:

a) zagrożenia bezpieczeństwa informacji,
b) skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna,
c) stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich.

Każdy pracownik zaangażowany w proces przetwarzania informacji zobowiązany jest do stosowania obowiązujących przepisów prawa oraz wewnętrznych procedur jednostki z zakresu bezpieczeństwa informacji .

Proces uświadamiania i kształcenia pracowników obejmuje również regularne przeprowadzanie szkoleń organizowane przez Administratora Danych Osobowych ze szczególnym uwzględnieniem zagadnień wskazanych powyżej.

Informacja o uczestnictwie szkoleniu powinna znaleźć się w aktach osobowych pracowników.

9. Zgłaszanie incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących.

ADO lub upoważniona przez niego osoba dokonuje wstępnej identyfikacji

Analiza incydentu uwzględnia następujące kryteria:

1) charakter incydentu i jego znaczenie związane z naruszeniem bezpieczeństwa fizycznego lub teleinformatycznego,
2) miejsce wystąpienia incydentu
-identyfikacja punktu, w którym nastąpiło zdarzenie (lokalizacja, serwer, stacja robocza itp.),
4) identyfikację zasobów potrzebnych przy dalszych działaniach w ramach postępowania z incydentem związanym z bezpieczeństwem informacji,
5) możliwości rozszerzania się incydentu i sposoby jego ograniczania,
6) szacowany poziom szkód finansowych,
7) rodzaj ujawnionej informacji (jeśli ma zastosowanie –np. dane osobowe),
8)szacunkowy czas, po którym skutki incydentu zostaną zlikwidowane, jeżeli nie ma możliwości natychmiastowego usunięcia stanu naruszenia bezpieczeństwa informacji,
9) skutki organizacyjne i prawne (wstępny szacunek).

Dokumentowanie i wyciąganie wniosków

ADO lub upoważniona przez niego osoba sporządza raport z zaistniałej sytuacji uwzględniające informacje wskazane powyżej oraz identyfikuje dane zdarzenie w rejestrze incydentów.

ADO lub upoważniona przez niego osoba każdorazowo po wpisaniu nowego incydentu do rejestru analizuje poprzednie incydenty celem wykrycia ewentualnych powiązań pomiędzy nimi i podjęcia dodatkowych działań mających na celu minimalizację ryzyka jego ponownego wystąpienia.

Dodatkowo, incydenty mogą być wykorzystywane podczas szkoleń pracowniczych jako przykłady tego co może się wydarzyć, jak unikać ich w przyszłości i jak reagować jak się wydarzą. Podczas wykorzystywania powyższych informacji należy wykazać się daleko idącą ostrożnością w aspekcie zachowania poufności.