Załącznik nr 6

KOMUNIKAT NA TEMAT PRZETARZANIA ORAZ BEZPIECZEŃSTWA DANYCH OSOBOWYCH ZGROMADZONYCH W PORTALU INTERNETOWYM

Celem niniejszego dokumentu jest informacja na temat zapewnienia bezpieczeństwa systemu informatycznego oraz przetwarzanych danych.

Zapisy niniejszego dokumentu skierowane są do wszystkich pracowników zaangażowanych w prace przy systemie informatycznym, którzy mają lub potencjalnie mogą mieć dostęp do danych osobowych.

Ilekroć w niniejszym dokumencie jest mowa o:

1. uczelni – rozumie się przez to każdą Uczelnię, która wdroży narzędzie informatyczne (portal internetowy) do monitorowania losów zawodowych absolwentów opracowany przez Uniwersytet Przyrodniczy we Wrocławiu;
2. ustawie – rozumie się przez to: ustawę z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tekst jednolity Dz. U. nr 101 z 2002 roku, poz. 926 ze zmianami);
3. rozporządzeniu – rozumie się przez to Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. nr 100, poz. 1024);
4. danych osobowych – rozumie się przez to każdą informację dotyczącą zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;

5. **studencie** – użytkownik portalu internetowego do monitorowania losów zawodowych absolwentów danej Uczelni, który wpisuje swoje dane do portalu;
6. **absolwencie -** użytkownik portalu internetowego do monitorowania losów zawodowych absolwentów danej Uczelni, który wpisuje swoje dane do portalu;
7. **pracodawcy** - użytkownik portalu internetowego do monitorowania losów zawodowych absolwentów zarówno instytucja jak i przedsiębiorca, bez względu na wielkość podmiotów, który wpisuje swoje dane do portalu;
8. **pracowniku Uczelni –** uprawniony użytkownik portalu internetowego do monitorowania losów zawodowych absolwentów np: administrator portalu, Redaktor Główny Uczelni, Redaktorzy Wydziałowi Uczelni;
9. **przetwarzaniu danych** – rozumie się przez to wszelkie operacje wykonywane na danych osobowych, takie jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych**;**
10. **zbiorze danych** – rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;
11. **systemie informatycznym** – rozumie się przez to zespół współpracujących ze sobą urządzeń , programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych – portal internetowy do monitorowania losów zawodowych absolwentów;
12. **zabezpieczeniu danych w systemie informatycznym** – rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i informacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;
13. **usuwaniu danych** – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;
14. **Administratorze Danych Osobowych (ADO)** - w sensie formalno-prawnym jest Uczelnia, natomiast w sensie praktycznym za realizację podstawowych obowiązków ADO odpowiedzialny jest rektor.
15. **Administratorze Bezpieczeństwa Informacji (ABI)** - nadzoruje przestrzeganie zasad zabezpieczania danych osobowych w Uczelni. Do jego głównych zadań należy: nadzór

nad przeciwdziałaniem dostępowi osób nieuprawnionych do zbiorów danych oraz wykrywanie naruszeń w systemie ochrony i prawidłowego wykorzystywania danych osobowych w Uczelni.

16. Administratorze Bezpieczeństwa Informacji MLA (ABI MLA) rozumie się przez to osobę nadzorującą przestrzeganie zasad ochrony danych osobowych w skali portalu internetowego, która jest obowiązana zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną. W szczególności powinna ona zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Do jej obowiązków należy między innymi podejmowanie odpowiednich działań w przypadku stwierdzenia naruszenia ochrony danych osobowych w systemach informatycznych, a także nadzór i kontrola w zakresie określonym przepisami o ochronie danych osobowych oraz regulacjami wewnętrznymi Administratora Danych Osobowych. Rolę ABI MLA może pełnić także ABI.
17. Administratora Portalu – upoważniona osoba do przetwarzania danych osobowych zgromadzonych w portalu.

DANE OSOBOWE PRZETWARZANE W SYSTEMIE INFORMATYCZNYM

W portalu przetwarzane są następujące dane osobowe użytkowników portalu internetowego:

1. studentów,
2. absolwentów,
3. pracodawców,
4. pracowników Uczelni.

Powyższy zbiór danych osobowych podlega rejestracji u Generalnego Inspektora Ochrony Danych Osobowych zgodnie z rozdziałem 6 ustawy.

Zakres danych przetwarzanych w systemie informatycznym to:

1. identyfikator użytkownika: PESEL, numer indeksu (dyplomu), imię ojca, adres e-mail, REGON;
2. dane użytkowników: imię i nazwisko, adres (miejscowość, kod pocztowy, ulica, nr domu), nr telefonu.

Poprzez użytkownika rozumie się tutaj każdego **studenta**, **absolwenta**, **pracodawcę** lub **pracownika Uczelni,** którego dane zostają umieszczone w systemie.

W celu zachowania bezpieczeństwa danych w sieci Internet, system informatyczny wykorzystuje dane osobowe w celu weryfikacji użytkownika, w zależności od jego rodzaju (student, absolwent, pracodawca).

Moduł Ankietowy przetwarza dane użytkownika, a wyniki ankiet wysyła do właściwej sobie jednostki, w postaci danych statystycznych bądź zestawień informacji (odpowiedzi na pytania otwarte) nie powiązanych z żadnym użytkownikiem.

Moduł Raportowy operuje na danych statystycznych uzyskanych z jednostki, do której zostały wysłane ankiety. Dane pogrupowane są pod kątem pewnych właściwości badanej populacji (np. wiek, wykształcenie itp.) i jako dane czysto statystyczne mogą być udostępniane przez Uczelnie. Ze względu na autonomię każdej uczelni, decyzją **Administratora Danych Osobowych** dane zostają udostępnione lub mogą zostać utajnione.

PRZETWARZANIE DANYCH OSOBOWYCH

Osobą uprawnioną do przetwarzania danych osobowych w portalu do monitorowania losów absolwentów jest Administrator Portalu, który otrzymuje od ADO upoważnienie do przetwarzania danych osobowych. Pozostali użytkownicy portalu przetwarzają własne dane osobowe. ADO może wydać upoważnienie do przetwarzania danych osobowych również innym użytkownikom portalu np. Redaktorowi Głównemu Uczelni na pisemny wniosek, w uzasadnionych przypadkach.

Dedykowane funkcjonalności poszczególnym użytkownikom (studenci, absolwenci, pracodawcy, Redaktor Główny Uczelni, Redaktorzy Wydziałowi Uczelni) pozwalają jedynie na dostęp, do niektórych danych osobowych użytkowników:

1. **student** – w ramach dedykowanych funkcjonalności będzie miał dostęp do danych osobowych (**TYLKO imię i nazwisko**) pozostałych użytkowników studentów, absolwentów. Umożliwią to funkcjonalności: forum, skrzynka wiadomości, tablica. Student nie ma możliwości przeglądania profili pozostałych studentów i absolwentów. Ma natomiast możliwość ukrycia dla pracodawcy danych teleadresowych. Podczas rejestracji do portalu każdy użytkownik chcący korzystać z portalu musi zaakceptować regulamin oraz wyrazić zgodę na przetwarzanie danych osobowych.
2. **absolwent -** w ramach dedykowanych funkcjonalności będzie miał dostęp do danych osobowych (**TYLKO imię i nazwisko**) pozostałych użytkowników studentów, absolwentów. Umożliwią to funkcjonalności: forum, skrzynka wiadomości, tablica. Absolwent nie ma możliwości przeglądania profili pozostałych studentów i absolwentów. Ma natomiast możliwość ukrycia dla pracodawcy danych teleadresowych. Podczas rejestracji do portalu każdy użytkownik chcący korzystać z portalu musi zaakceptować regulamin oraz wyrazić zgodę na przetwarzanie danych osobowych.
3. **pracodawca** – użytkownik, który po rejestracji i zalogowaniu, w ramach dedykowanych funkcjonalności (wyszukiwanie pracowników/przeglądanie ich profili) będzie miał dostęp do danych osobowych **(imię i nazwisko, dane teleadresowe w przypadku udostępnienia ich przez studenta lub absolwenta)** pozostałych użytkowników studentów, absolwentów jedynie do celów rekrutacji w ramach prowadzonego procesu rekrutacji i wyłącznie po uprzednio uzyskanej zgodzie od studenta, absolwenta. Ponadto, podczas rejestracji do portalu każdy użytkownik chcący korzystać z portalu musi zaakceptować regulamin oraz wyrazić zgodę na przetwarzanie danych osobowych.
4. **pracownik Uczelni –** Redaktor Główny Uczelni i Redaktorzy Wydziałowi Uczelni, będą mieli dostęp do danych osobowych (**TYLKO imię i nazwisko**) pozostałych użytkowników studentów, absolwentów. Umożliwią to funkcjonalności: skrzynka wiadomości. Pracownik Uczelni nie ma możliwości przeglądania profili pozostałych studentów i absolwentów, pracodawców. Podczas rejestracji do portalu każdy użytkownik chcący korzystać z portalu musi zaakceptować regulamin oraz wyrazić zgodę na przetwarzanie danych osobowych.

Podczas prowadzenia badania ankietowego pracownicy nie będą mieli dostępu do danych osobowych studentów/absolwentów, a jedynie np. do wydziału, kierunku, danego roku.

BEZPIECZEŃSTWO DANYCH OSOBOWYCH

I. Środki organizacyjne i techniczne zapewniające ochronę systemu informatycznego oraz danych osobowych.

Do podstawowych zabezpieczeń przed naruszeniem ochrony danych należą:

1. ochrona obiektu przez wszystkie dni w roku,
2. wydzielanie pomieszczeń ,
3. wyposażenie pomieszczeń w specjalne szafy,
4. zabezpieczenie wejść do pomieszczeń odpowiednimi zamkami,
5. odpowiednia obsługa i użytkowanie sprzętu komputerowego przez upoważnione osoby.

Środki organizacyjne i techniczne:

1. Dostęp do danych osobowych mogą mieć tylko i wyłącznie pracownicy posiadający pisemne, imienne upoważnienia podpisane przez ADO;
2. Każdy z pracowników powinien zachować szczególną ostrożność przy przetwarzaniu, przenoszeniu wszelkich danych osobowych;
3. Należy chronić dane przed wszelkim dostępem do nich osób nieupoważnionych.
4. Pomieszczenia, w których są przetwarzane dane osobowe, muszą być zamykane na klucz.
5. Dostęp do kluczy powinni posiadać tylko upoważnieni pracownicy.
6. Dostęp do pomieszczeń możliwy jest tylko i wyłącznie w godzinach pracy uczelni. W wypadku, gdy jest wymagany poza godzinami pracy - możliwy jest tylko na podstawie pisemnego zezwolenia ABI MLA lub ADO;
7. Dostęp do pomieszczeń, w których są przetwarzane dane osobowe mogą mieć tylko upoważnieni pracownicy.

8. W przypadku pomieszczeń do których dostęp mają również osoby nieupoważnione, mogą przebywać w tych pomieszczeniach TYLKO w obecności osób upoważnionych, i tylko w czasie wymaganym na wykonanie niezbędnych czynności.
9. Szafy w których przechowywane są dane osobowe muszą być zamykane na klucz.
10. Klucze do tych szaf powinni posiadać tylko upoważnieni pracownicy.
11. Szafy z danymi powinny być otwarte tylko na czas potrzebny na dostęp do danych, a następnie powinny być zamykane.
12. Dane osobowe w formie papierowej mogą znajdować się na biurkach tylko na czas niezbędny na dokonanie czynności służbowych a następnie muszą być chowane do szaf.
13. Dostęp do komputerów na których są przetwarzane dane osobowe mogą mieć tylko upoważnieni pracownicy.
14. Stacje komputerowe na których przetwarzane są dane osobowe powinny mieć tak ustawione monitory, aby nie miały wglądu w dane osoby nieupoważnione.
15. Każdy plik w którym są zawarte dane osobowe powinien być zabezpieczony hasłem jeśli nie jest to przetwarzanie danych w systemie informatycznym.
16. W przypadku przetwarzania danych osobowych na komputerach przenośnych należy zachować szczególną ostrożność przy ich przewożeniu.
17. W przypadku potrzeby przeniesienia danych osobowych pomiędzy komputerami należy dokonać tego z zachowaniem szczególnej ostrożności i za zgodą ABI MLA.
18. Nośniki użyte do tego należy wyczyścić (skasować nieodwracalnie/zniszczyć), aby nie zostały na nich dane osobowe.
19. W wypadku niemożliwości skasowania danych z nośnika (płyta CD/DVD) należy taką płytę zniszczyć fizycznie (np. za pomocą odpowiedniej niszczarki).
20. W przypadku wykorzystania do przenoszenia dysków, dane należy kasować z tych dysków.
21. Niezabezpieczonych danych osobowych nie należy przesyłać drogą elektroniczną.
22. Sieć komputerowa powinna być zabezpieczona przed nieautoryzowanym dostępem z zewnątrz.
23. Do zabezpieczenia sieci należy stosować:

    a) firewall,

    b) systemy wykrywania włamań IDS,

c) logowanie wszelkich zdarzeń w dziennikach systemowych na serwerach i stacjach roboczych,

d) systemy antywirusowe i antyszpiegowskie,

e) zabezpieczenia skrzynek poczty elektronicznej hasłami "trudnymi" (min. 8 znaków w tym litery, cyfry, znaki specjalne);

f) ustawienie odpowiednich poziomów dostępu dla odpowiednich użytkowników w systemie informatycznym, zmiany mogą zostać przeprowadzone tylko i wyłącznie przez ABI MLA lub ADO.

24. Zabezpieczenia przed utratą danych osobowych w wyniku awarii:

a) odrębne zasilanie sprzętu komputerowego,

b) ochrona serwerów przed zanikiem zasilania poprzez stosowanie zasilaczy zapasowych UPS. Minimalny czas podtrzymania napięcia wynosi 5 min,

c) ochrona przed utratą zgromadzonych danych poprzez cykliczne wykonywanie kopii zapasowych, z których w przypadku awarii odtwarzane są dane i system operacyjny,

d) ochrona przed awarią podsystemu dyskowego poprzez używanie macierzy dyskowych,

e) zapewnienie właściwej temperatury i wilgotności powietrza dla pracy sprzętu komputerowego, poprzez zastosowanie redundantnych klimatyzatorów,

f) zastosowanie ochrony przeciwpożarowej poprzez umieszczenie w serwerowni gaśnic, okresowo kontrolowanych przez specjalistę,

g) zwiększenie niezawodności serwerów i urządzeń sieciowych poprzez logiczne rozmieszczenie ich w szafach serwerowych.

II. Zabezpieczenie danych w systemie informatycznym

Uwzględniając kategorie przetwarzanych danych osobowych oraz zagrożenia, portal internetowy do monitorowania losów zawodowych absolwentów został objęty wysokim poziomem bezpieczeństwa tzn., że zastosowano następujące środki bezpieczeństwa:

1. Wdrożenie fizycznych zabezpieczeń chroniących przed nieuprawnionym dostępem.

Poniżej wskazano najczęściej występujące ataki oraz metody obrony:

a) **ataki semantyczne na adres URL** – wszelkie operacje synchroniczne związane z nawigacją po stronie WWW odbywają się po ściśle typowanych akcjach kontrolerów

(np. ***SaveNote(SaveNoteModel model)***). Podejście to zapewnia, że akcje kontrolerów serwisu WWW nie będą przyjmowały więcej parametrów poza modelem. Dodatkowo z systemu zostały usunięte wszelkiego rodzaju parametry, które przekazywane byłby za pośrednictwem URL – cała komunikacja synchroniczna odbywa sią za pośrednictwem metod POST. Operacje wywołane asynchronicznie, wykorzystujące metodę GET kontrolowane są przez mechanizm ASP.NET co do zgodności z wymaganiami bezpieczeństwa tej platformy;

b) **ataki związane z ładowaniem plików**: aplikacja nie umożliwia wgrywania plików z rozszerzeniami .exe, .cpp, .js oraz .zip. Dla pozostałych formatów plików przeprowadzone zostały testy bezpieczeństwa polegające na próbie osadzenia kodu;
c) JavaScript we wgrywanym na serwer pliku. Testy te wykazały, że system jest odporny na tego typu ataki;
d) **ataki typu cross-site scripting** – nad bezpieczeństwem tego typu ataków czuwa serwer IIS jak również mechanizm sesji użytkownika. W momencie w którym serwer IIS nie jest wykryje próbę wstrzyknięcia kodu JavaScript lub wykonania kodu spoza zaufanej domeny aplikacji zostanie zgłoszony wyjątek: **A potentially dangerous Request.Form value was detected from the client;**
e) **ataki typu CSRF/ XSRF** - w systemie w znacznej większości wykorzystywane jest metoda POST jak również wykorzystano wbudowane w platformę ASP.NET sesje użytkownika.
f) Wykorzystane metody GET nie referują do danych newralgicznych a jedynie do funkcji odczytu danych;
g) **podrabianie zarządzania formularza** – bezpieczeństwo komunikacji klient serwer zapewnia platforma .NET. W momencie rozpoczęcia pracy z aplikacją generowany jest lokalny UID sesji, który jest przechowywany w postaci pliku cookie w przeglądarce klienta i dołączany jest każdorazowo do żądania. Po stronie serwera istnieje bezpośrednie powiązanie ID sesji z adresem klienta. Dodatkowym zabezpieczeniem jest SSL;
h) **ujawnienie uwierzytelnień dostępu** – wszelkie dane dostępowe (loginy oraz hasła) zapisane są w systemie w plikach konfiguracyjnych (web.config dla aplikacji WWW i webserwisów oraz app.config dla grubego klienta). W plikach tych sekcje zawierające

i) newralgiczne dane zostały zakodowane w oparciu o wbudowany w platformę .NET mechanizm szyfrowania (narzędzie aspnet_regiis.exe);

j) **wstrzykiwanie kodu SQL** – ochrona przed tego typu atakami odbywa się na trzech poziomach systemu. Po pierwsze od strony aplikacji WWW nad bezpieczeństwem przesyłanych do serwera danych czuwa technologia ASP.NET. Następnie w celu komunikacji z bazą danych, zostało wykorzystane narzędzie klasy ORM - Entity Framework w wersji 4.1. (Code-First). Narzędzie to, prócz ścisłej kontroli typów oraz wbudowanemu mechanizmowi generowania zapytań, do wykonywania zapytań do bazy danych wykorzystuje procedurę SQL Server sp_ExecuteSql. Specyfika działania tej procedury zapewnia najwyższy z możliwych do osiągnięcia poziomów zabezpieczeń przeciwko wstrzykiwaniu kodu SQL. Zapytania, które są wykonywane poza wyżej wymienionym narzędziem ORM zostały w pełni sparametryzowane;

k) **wstrzykiwanie kodu wykonywalnego innych języków programowania** – serwery IIS systemu skonfigurowano tak aby nie obsługiwały innych niż C# języków programowania (np. CGI czy Python);

l) **kradzież cookies, przechwytywanie sesji, wstrzykiwanie sesji** – bezpieczeństwo sesji zapewnia platforma .NET. W pliku cookie o nazwie ASP.NET_SessionId w momencie pierwszego wyświetlenia strony, zostaje zapisana wartość nowo utworzonej sesji. Id sesji, po stronie serwera, jest jednoznacznie przypisane do adresu hosta. Sesja po stronie serwera jest natychmiastowo niszczona przez platformę .NET w momencie w którym adres hosta dla danej sesji uległ zmianie – powoduje to przejście do panelu logowania;

m) **trawersowanie katalogów** – system został w pełni zabezpieczony przed tego typu atakami poprzez minimalizację wykorzystania funkcji GET na rzecz funkcji POST. W systemie wykorzystano również mechanizm ścisłej kontroli typów co przekłada się bezpośrednio na statyczną strukturę przesyłanych stron. Dodatkowo, dołożono wszelkich starań aby wszelkie przesyłane do klienta ścieżki (do grafik, plików itp.) były ścieżkami względnymi np. /images/logo.png. ;

n) **wstrzykiwanie poleceń systemowych** – system jest zabezpieczony przez wstrzyknięciem poleceń systemowych w dwóch warstwach. Pierwszym poziom bezpieczeństwa stanowi IIS, który posiada zaimplementowaną funkcjonalność wykrywania potencjalnie

niebezpiecznych żądań. Drugi mechanizm wbudowany jest bezpośrednio w system Windows, który sprawdza czy aplikacja chcąca wykonać polecenia systemowe działa w kontekście użytkownika któremu nadano wystarczająco wysokie prawa dostępu;

o) **ujawnienie kodu źródłowego** – kod źródłowy JavaScript został poddany procesowi 'kompilacji', zmniejszającemu znacznie jego czytelność i możliwość wykorzystania. Pozostałe źródła systemy znajdują się w skompilowanych plikach DLL;

p) **przepełnienie bufora lub stosu** – za bezpieczeństwo działania stosu odpowiada platforma .NET. Wbudowany w nią mechanizm zapewnia wyrzucenie silnie typowanego wyjątku w momencie przepełnienia stosu/buforu aplikacji, który z kolei został obsłużony w systemie dzięki wykorzystaniu mechanizmu dziedziczenia.

2. Zastosowano kryptograficzne środki ochrony wobec danych wykorzystywanych do uwierzytelniania, które są przesyłane w sieci publicznej:

a) Zakodowanie hasła dostępu - zakodowane jest jednostronną funkcją skrótu (minimum SHA-1) oraz do hasła dołączany jest losowy ciąg znaków tzw. „sól". Sól generowana jest jednorazowo dla każdego użytkownika indywidualnie, oraz przechowywana w bazie danych.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

I. Procedura nadawania i odbierania uprawnień do przetwarzania danych osobowych:

1) konto **Administratora Portalu (AP)** na serwerze zakłada **ABI MLA**, na podstawie upoważnienia do przetwarzania danych osobowych, nadając **AP** unikalną nazwę, identyfikator i hasło,
2) przydzielone hasło przekazywane jest w formie ustnej,
3) System Informatyczny wymusza zmianę hasła **AP** przy pierwszym zalogowaniu się do systemu,
4) ustanie stosunku pracy lub przejście **AP** do innej jednostki organizacyjnej skutkuje usunięciem jego konta a nazwa użytkownika oraz identyfikator nie mogą być przydzielona innej osobie,

5) AP jest **użytkownikiem uprzywilejowanym**, posiadającym najwyższe uprawnienia w Systemie Informatycznym.

II. Metody i środki uwierzytelniania:

1) uwierzytelnienie AP w Systemie Informatycznym następuje po podaniu nazwy użytkownika i hasła,
2) hasła AP serwera są szyfrowane,
3) AP pod żadnym pozorem nie może udostępniać swojej nazwy użytkownika i hasła innej osobie,
4) nazwa użytkownika składa się z 3 do 8 znaków (liter łacińskich lub/i cyfr),
5) hasło składa się z minimum 8 dowolnych znaków (w tym minimum jedna litera duża litera, jedna mała litera i dwie cyfry),
6) hasło nie może być takie samo jak nazwa użytkownika,
7) hasło nie może być zapisane w miejscu dostępnym dla osób nieuprawnionych,
8) zabrania się zapamiętywania danych dostępowych w przeglądarkach internetowych, menedżerach haseł itp.,
9) system informatyczny wymusza na AP zmianę hasła nie rzadziej niż co 30 dni,
10) w przypadku gdy AP nie zaloguje się w momencie kiedy upłynie termin opisany w p.9 konto zostaje automatycznie zablokowane, do momentu ustanowienia przez AP nowego hasła,
11) aby ustanowić nowe hasło AP musi podać obecnie obowiązujące hasło,
12) w sytuacji kiedy AP nie może zalogować się do systemu wprowadzając (w jego mniemaniu prawidłowe dane do logowania) powinien bezzwłocznie zgłosić ten fakt do ABI MLA,
13) W przypadku zaistnienia sytuacji z ust. 11. ABI ponownie rozpoczyna procedurę opisaną w p. II, ust 2.

III. Procedury rozpoczęcia, zawieszenia i zakończenia pracy:

1) rozpoczęcie pracy:
    a) włączenie monitora i komputera,
    b) uruchomienie portalu,

c) zalogowanie się na koncie użytkownika z ograniczonymi prawami poprzez podanie nazwy użytkownika i hasła.

2) zawieszenie pracy w przypadku czasowego opuszczenia stanowiska pracy lub całkowite zakończenie pracy:
   a) zamknięcie sesji poprzez wylogowanie się z systemu,
   b) ponowne zalogowanie się na koncie użytkownika z ograniczonymi prawami poprzez podanie nazwy użytkownika i hasła,
   c) W przypadku bezczynności trwającej dłużej niż 5 min system wylogowuje AP automatycznie.

IV. Procedura tworzenia kopii zapasowych:

1) archiwizacja przeprowadzana jest automatycznie w późnych godzinach nocnych, przy pomocy wbudowanych w system funkcji,
2) przed uruchomieniem archiwizacji wszystkie procesy (zadania) niewylogowanego użytkownika są usuwane z systemu, a administrator serwera otrzymuje informację o tym zdarzeniu,
3) harmonogram wykonywanych archiwacji:
   a) kopie aktualnych baz danych oraz istotnych elementów systemu operacyjnego serwera są wykonywane codziennie, kopie baz archiwalnych są wykonywane raz w tygodniu,
   b) na serwerze bazodanowym przechowywane są archiwizacje w formie nieskompresowanej – przez 1 dzień i skompresowanej – przez 2 tygodnie,
   c) dane w formie skompresowanej automatycznie są wysyłane codziennie na serwer archiwizacji i przechowywane przez minimum 2 tygodnie,
4) ABI MLA okresowo sprawdza możliwość odtworzenia danych z kopii zapasowych,
5) nośniki danych przeznaczone do likwidacji, są niszczone w sposób uniemożliwiający odczyt danych.

V. Sposób zabezpieczenia systemu informatycznego przed działalnością wirusów komputerowych oraz wszelkiego rodzaju złośliwego oprogramowania:

1) Każdy pracownik korzystający z systemu jest zobligowany do posiadania programu antywirusowego zainstalowanego na stacji roboczej, z której korzysta.
2) W trakcie pracy w systemie pracownik może mieć otwarta jedną zakładkę w przeglądarce – z obecnie używaną częścią systemu.
3) Pracownik powinien mieć świadomość, że korzystanie z programu antywirusowego jest obligatoryjne a jego brak poważnie narusza zasady bezpieczeństwa systemu.
4) Pracownik dba o aktualizację systemu operacyjnego, programu antywirusowego i sygnatur wirusów.

VI. Konserwacja Systemu Informatycznego:

1) **ABI MLA** codziennie sprawdza logi systemowe i programowe serwera,
2) **ABI MLA** okresowo sprawdza spójność danych oraz stan nośników (dysków twardych, taśm magnetycznych),
3) **ABI MLA** dba o aktualność oprogramowania na serwerach.