Załącznik nr 2 do Zarządzenia Nr 22/2017

z dnia 4 września 2017r.

Instrukcja

zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Państwowej Wyższej Szkole Zawodowej w Elblągu

I. Niniejsza instrukcja określa zasady zarządzania każdym systemem informatycznym służącym do przetwarzania danych osobowych w Państwowej Wyższej Szkole Zawodowej w Elblągu – zgodnie z *Rozporządzeniem MSWiA z dnia 29.04.2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.*

II. Systemy informatyczne w PWSZ w Elblągu, w których przetwarza się dane osobowe:

1. System: Suita
   Program: „Suita Akademicka”

2. System: E-rekrutacja
   Program: „Elektroniczna rekrutacja - PWSZ w Elblągu”

3. System: SOWA
   Program: „Zintegrowany System Obsługi Biblioteki SOWA”

4. System: Symfonia FK
   Program: „Sage Symfonia Finanse i Księgowość”

5. System: Symfonia FP
   Program: „Sage Symfonia Faktura Premium”

6. System: Kadry, płatnik
   Program: „QNT Quorum”, „Prokom Płatnik”

7. System: Płace, płatnik
   Program: „QNT Quorum”, „Prokom Płatnik”

8. System: IBIZNES24
   Program: „BZWBK ”

9. System: BGK24
   Program: „BGK”

10. System: USOS
    Program: „Uczelniany System Obsługi Studentów”

11. System: Administracja systemu
    Program: „MS Windows – domena”, „Squirrelmail – poczta”

III. Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności

1. Do obsługi systemu informatycznego służącego do przetwarzania danych osobowych, może być dopuszczona wyłącznie osoba posiadająca upoważnienie do przetwarzania danych osobowych.
2. Rejestracji użytkownika systemu informatycznego dokonuje się na podstawie upoważnienia, o którym mowa w punkcie 1.
3. Dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora użytkownika i właściwego hasła.
4. Dla każdego użytkownika systemu informatycznego, który przetwarza dane osobowe, Kierownik Działu IT ustala niepowtarzalny identyfikator i hasło początkowe.
5. Identyfikator użytkownika nie powinien być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego, nie powinien być przydzielany innej osobie.
6. Kierownik Działu IT wyznacza dla każdego systemu informatycznego, Administratora Systemu Informatycznego oraz osobę zastępującą w przypadku jego nieobecności. Administratorowi Systemu Informatycznego przydziela się w systemie identyfikator użytkownika uprzywilejowanego.
7. Kierownik jednostki organizacyjnej PWSZ, w ramach której działa podległy mu użytkownik informuje Kierownika Działu IT o fakcie utraty przez daną osobę uprawnień do dostępu do danych osobowych w systemie informatycznym. Identyfikator osoby, która utraciła uprawnienia do dostępu do danych osobowych, należy niezwłocznie wyrejestrować z systemu informatycznego, unieważnić jej hasło, oraz podjąć inne stosowne działania w celu zapobieżenia dalszemu dostępowi tej osoby do danych. Za realizację procedury rejestrowania i wyrejestrowywania użytkowników w systemie informatycznym odpowiedzialny jest Kierownik Działu IT.
8. Kierownik Działu IT lub osoba przez niego upoważniona przekazując użytkownikowi identyfikator i hasło przeprowadza szkolenie z zakresu pracy w systemie informatycznym oraz bezpieczeństwa danych w systemie informatycznym.
9. Ewidencję użytkowników każdego systemu informatycznego przetwarzającego dane osobowe prowadzi Kierownik Działu IT, który odpowiada za jej aktualizację.

IV. Stosowane metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem

1. Dane osobowe przetwarzane są w PWSZ z użyciem dedykowanych serwerów, komputerów stacjonarnych i przenośnych.
2. Kierownik Działu IT nadaje hasło początkowe i wymusza w systemie zmianę haseł użytkowników.
3. Na wydzielonych stanowiskach komputerowych (nie pracujących w ramach sieciowego systemu informatycznego) oraz w systemach, w których automatyczne wymuszenie zmiany hasła nie następuje, hasło powinno być zmieniane nie rzadziej niż raz na 30 dni. Za jego zmianę odpowiedzialny jest użytkownik.
4. Stanowiska komputerowe na których skonfigurowanie identyfikatora i hasła zapewniającego ochronę jest nieskuteczne, zabezpiecza się dodatkowym hasłem (hasło wygaszacza ekranu, hasło BIOSu).
5. Hasło nie może być zapisywane w miejscu dostępnym dla osób nieuprawnionych. Użytkownik nie może udostępnić swojego identyfikatora oraz hasła jak również dostępu do stanowiska roboczego po uwierzytelnieniu w systemie osobom nieuprawnionym ani żadnej osobie postronnej.

6. Raz użyty identyfikator nie może być przydzielony innemu użytkownikowi.
7. Hasła Administratorów Systemu Informatycznego są zdeponowane w Dziale IT.
8. W przypadku, gdy istnieje podejrzenie, że hasło mogła poznać osoba nieuprawniona, użytkownik zobowiązany jest do natychmiastowej zmiany hasła, lub w razie problemów powiadomić o tym fakcie Administratora Systemu Informatycznego.
9. W przypadku przetwarzania danych na komputerach przenośnych, dyski twarde oraz inne wykorzystywane nośniki informacji powinny być zabezpieczone w sposób uniemożliwiający dostęp do tych danych osobom postronnym (np. nieuprawniony dostęp, kradzież komputera, szpiegostwo przemysłowe), poprzez wykorzystanie metod i środków kryptograficznych (szyfrowane partycje dysków twardych, szyfrowanie plików, ochrona fizyczna nośników).

V. Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu

1. Dane osobowe, których administratorem jest PWSZ mogą być przetwarzane z użyciem systemu informatycznego tylko na potrzeby realizowania zadań statutowych i organizacyjnych Uczelni.
2. Rozpoczęcie pracy w aplikacji musi być zgodne z Regulaminem funkcjonowania i korzystania z zasobów teleinformatycznych PWSZ w Elblągu.
3. Zakończenie pracy użytkownika następuje po poprawnym wylogowaniu się z systemu oraz poprzez uruchomienie odpowiedniej dla danego systemu opcji jego zamknięcia zgodnie z instrukcją zawartą w dokumentacji, w przypadku braku takiej w dokumentacji, według zasad opracowanych przez Kierownika Działu IT.
4. Niedopuszczalne jest zakończenie pracy w systemie bez wykonania pełnej i poprawnej operacji wylogowania z aplikacji i poprawnego zamknięcia systemu.
5. Monitory stanowisk komputerowych znajdujące się w pomieszczeniach, gdzie przebywają osoby, które nie posiadają upoważnień do przetwarzania danych osobowych, należy ustawić w taki sposób, aby uniemożliwić osobom postronnym wgląd w dane.
6. Użytkownik ma obowiązek wylogowania się lub zablokowania systemu w przypadku dłuższej, zaplanowanej nieobecności na stanowisku pracy lub w przypadku zakończenia pracy. Stanowisko komputerowe nie może pozostać z uruchomionym i dostępnym systemem bez nadzoru pracującego na nim pracownika.
7. Wydruki zawierające dane osobowe należy przechowywać w miejscu uniemożliwiającym ich odczytanie przez osoby postronne. Wydruki nieprzydatne należy zniszczyć w stopniu uniemożliwiającym ich odczytanie (niszczarka dokumentów).
8. Przebywanie osób nieuprawnionych w pomieszczeniach znajdujących się na obszarze, w którym są przetwarzane dane osobowe jest dopuszczalne tylko w obecności osoby upoważnionej do ich przetwarzania.
9. Pomieszczenia, w których przetwarzane są dane osobowe, należy zamykać, na czas nieobecności osób zatrudnionych, w sposób uniemożliwiający dostęp do nich osobom trzecim.
10. Użytkownik niezwłocznie powiadamia Administratora Systemu Informatycznego w przypadku braku możliwości zalogowania się na swoje konto w przypadku podejrzenia fizycznej ingerencji w przetwarzane dane osobowe lub użytkowane narzędzia programowe lub sprzętowe. Wówczas, użytkownik jest zobowiązany do natychmiastowego wyłączenia sprzętu.

VI. Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania

1. Zbiory danych w systemie informatycznym są zabezpieczane przed utratą lub uszkodzeniem za pomocą:
a. urządzeń zabezpieczających przed awarią zasilania lub zakłóceniami w sieci zasilającej,
b. sporządzania kopii zapasowych zbiorów danych (kopie pełne).
2. Za tworzenie kopii bezpieczeństwa systemu informatycznego odpowiedzialny jest Kierownik Działu IT za pośrednictwem wyznaczonego przez siebie Administratora Systemu.
3. Pełne kopie zapasowe zbiorów danych są tworzone co najmniej raz na tydzień, kopie przyrostowe w wykonywane są codziennie.
4. W szczególnych przypadkach – przed aktualizacją lub zmianą w systemie należy bezwarunkowo wykonać pełną kopię zapasową systemu.
5. Kopie zapasowe zbiorów danych należy okresowo sprawdzać pod kątem ich przydatności do odtworzenia w przypadku awarii systemu. Za przeprowadzanie tej procedury odpowiedzialny jest właściwy Administrator Systemu Informatycznego.
6. Nośniki danych po ustaniu ich użyteczności należy pozbawić danych lub zniszczyć w sposób uniemożliwiający odczyt danych.
7. W przypadku komputerów stacjonarnych i przenośnych nie będących własnością PWSZ, użytkownik systemu ma obowiązek sporządzania kopii zapasowych jak również ochrony nośników informacji. Wymaga się od użytkownika stosowania zasad dotyczących ochrony danych osobowych przed dostępem osób nieuprawnionych.

VII. Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych

1. Okresowe kopie zapasowe wykonywane są na dyskietkach, płytach CD, DVD, streamerach lub innych elektronicznych nośnikach informacji. Kopie powinny być przechowywane w innych pomieszczeniach niż te, w których przechowywane są zbiory danych osobowych wykorzystywane na bieżąco. Kopie zapasowe przechowuje się w sposób uniemożliwiający nieuprawnione przejęcie, modyfikacje, uszkodzenie lub zniszczenie.
2. Dostęp do nośników z kopiami zapasowymi systemu oraz kopiami danych osobowych, ma wyłącznie Rektor, Kierownik Działu IT oraz Administrator danego Systemu Informatycznego, którego kopie zawierają konkretne nośniki.
3. Kopie miesięczne przechowuje się przez okres 3 miesięcy. W przypadku danych finansowo - księgowych okres przechowywania danych wynosi 5 lat. Wykonywane co pół roku pełne kopie systemu kadrowego przechowuje się przez 50 lat. Kopie zapasowe należy bezzwłocznie usuwać po ustaniu ich użyteczności.
4. Usunięcie danych z systemu powinno zostać zrealizowane przy pomocy oprogramowania przeznaczonego do bezpiecznego usuwania danych z nośnika informacji.
5. W przypadku kopii zapasowych sporządzanych indywidualnie przez użytkownika, za ich zniszczenie odpowiada użytkownik.
6. W przypadku nośników informacji, przez ich zniszczenie rozumie się ich trwałe i nieodwracalne zniszczenie fizyczne do stanu nie dającego możliwości ich rekonstrukcji i odzyskania danych.
7. W przypadku braku możliwości zrealizowania procedury zniszczenia nośników informacji, należy fakt ten zgłosić Kierownikowi Działu IT. Po przekazaniu nośników zostaną one zniszczone w ramach środków technicznych Działu IT, bądź poddane procedurze utylizacji nośników informacji realizowanej przez firmę zewnętrzną.

VIII. Sposób zabezpieczenia systemu informatycznego przed działalnością szkodliwego oprogramowania

1. Ruch w sieci komputerowej PWSZ jest zabezpieczony przed dostępem z zewnętrznej publicznej sieci przez zastosowanie rozbudowanej ściany ogniowej (firewall) i serwera *proxy*. Ruch jest monitorowany przez Administratora Systemu i Sieci w celu kontroli przepływu danych między siecią publiczną, a siecią PWSZ oraz kontroli działań w sieciach.
2. Poczta elektroniczna jest zabezpieczona przed przesyłaniem nie zamówionej informacji handlowej (tzw. *SPAM*) oraz oprogramowania złośliwego za pomocą filtrów poczty.
3. Na wszystkich stacjach roboczych oraz serwerach zainstalowane jest oprogramowanie antywirusowe F-SECURE Anti-Virus.
4. Aktualizacje baz danych pobierane są codziennie do lokalnego repozytorium, z którego aktualizacje pobierane są przez pozostałe komputery.
5. Funkcjonowanie oprogramowania antywirusowego nadzorowane jest centralnie przez oprogramowanie konsoli zarządzającej.
6. Użytkownicy zostali przeszkoleni z zasad bezpieczeństwa danych, w ramach wewnętrznych szkoleń adaptacyjnych, w szczególności:

a. z zasad bezpiecznej pracy pozwalających unikać szkodliwego oprogramowania,
b. zasad postępowania w przypadku wykrycia, lub podejrzenia działania złośliwego oprogramowania.

IX. Udostępnianie danych osobowych i sposób odnotowania informacji o udostępnionych danych

1. Udostępnienie danych osobowych instytucjom, osobom spoza Uczelni może odbywać się wyłącznie na pisemny uzasadniony wniosek, za zgodą Rektora.
2. Kierownik Działu IT prowadzi ewidencję udostępniania danych osobowych.

X. Wykonywanie przeglądów i konserwacji systemu oraz nośników informacji służących do przetwarzania danych

1. Przeglądy i konserwacje systemu oraz zbiorów danych wykonuje na bieżąco wyznaczony przez Kierownika Działu IT Administrator Systemu Informatycznego - nie rzadziej niż raz w miesiącu. Sprawdzana jest spójność danych, indeksów oraz stan nośników informacji, np. dysków twardych oraz urządzeń peryferyjnych.
2. Administrator Systemu Informatycznego okresowo sprawdza możliwość odtworzenia danych z kopii zapasowej. Częstotliwość wykonywania procedury odtwarzania danych jest ustalana przez Kierownika Działu IT.
3. Umowy dotyczące instalacji i konserwacji sprzętu należy zawierać z podmiotami, których kompetencje nie budzą wątpliwości, co do wykonania usługi oraz których wiarygodność finansowa została sprawdzona na rynku – z pełnym zastosowaniem procedur określonych w zarządzeniu Rektora dotyczącym zakupu dostaw i usług.
4. Naprawa sprzętu, na którym mogą znajdować się dane osobowe powinna odbywać się pod nadzorem osób użytkujących sprzęt oraz wyznaczonego przez Kierownika Działu IT pracownika, w miejscu jego użytkowania.
5. W przypadku konieczności naprawy poza miejscem użytkowania, sprzęt komputerowy, przed oddaniem do serwisu, powinien być odpowiednio przygotowany. Dane należy zarchiwizować na nośniki informacji, a dyski twarde, bezwzględnie, wymontować na czas naprawy.

6. Zmiana konfiguracji sprzętu komputerowego, na którym znajdują się dane osobowe lub zmiana jego lokalizacji, może być dokonana tylko za wiedzą i zgodą Kierownika Działu IT.
7. W przypadku komputerów stacjonarnych i przenośnych nie będących własnością PWSZ użytkownik systemu jest odpowiedzialny za zabezpieczenie danych osobowych znajdujących się na jego komputerze, przed przekazaniem sprzętu do serwisu. W przypadku problemów z realizacją zabezpieczenia danych osobowych, użytkownik systemu zobowiązany jest zwrócić się o pomoc, w tym zakresie, do pracowników Działu IT.
8. Niesprawne nośniki danych, na których przechowywano dane osobowe powinny być niszczone trwale, aby nie był możliwy odczyt z nich jakichkolwiek danych.
9. Postępowanie z urządzeniami i nośnikami uszkodzonymi, a zawierające dane osobowe, powinno preferować ich trwałe zniszczenie, o ile pozwalają na to względy finansowe i organizacyjne. Jeżeli nie można sobie pozwolić na zakup nowych urządzeń lub nośników i odtworzenie utraconych danych z kopii zapasowych, to należy podjąć ich naprawę na miejscu w obecności upoważnionego pracownika PWSZ w Elblągu.
10. W przypadku zbywania/darowizny komputerów lub nośników wykorzystywanych dotychczas przez PWSZ wszystkie dane osobowe w nich zawarte powinny być wykasowywane nieodwracalnie

XI. Kierownik Działu IT ponosi bezpośrednią odpowiedzialność przed Rektorem za wdrożenie i stosowanie w PWSZ w Elblągu niniejszej Instrukcji.