Zarządzenie nr 37/2016/2017
Rektora Uniwersytetu Kazimierza Wielkiego
z dnia 30 marca 2017 r.

w sprawie wprowadzenia Szczegółowej Polityki Bezpieczeństwa Użytkowania Systemu Informatycznego "Uniwersytecki System Obsługi Studiów" w Uniwersytecie Kazimierza Wielkiego

Na podstawie art. 66 ust. 1 i ust. 2 ustawy z dnia 27 lipca 2005 r. prawo o szkolnictwie wyższym (Dz.U. z 2016 r. poz. 1842) w związku z § 1 ust. 6 załącznika nr 1 do Zarządzenia nr 82/2013/2014 Rektora Uniwersytetu Kazimierza Wielkiego z dnia 24 czerwca 2014 r. w sprawie wprowadzenia Polityki Bezpieczeństwa Użytkowania Systemów Informatycznych w Uniwersytecie Kazimierza Wielkiego

zarządzam,

co następuje:

§ 1

1. Wprowadzam Szczegółową Politykę Bezpieczeństwa Użytkowania Systemu Informatycznego "Uniwersytecki System Obsługi Studiów" (USOS) w Uniwersytecie Kazimierza Wielkiego stanowiącą załącznik nr 1 do niniejszego zarządzenia.
2. Szczegółowa Polityka Bezpieczeństwa określa podstawowe zasady nadawania, zmieniania i odbierania uprawnień w systemie informatycznym USOS, zawieszania kont użytkowników, politykę haseł dla systemu oraz zasady zabezpieczenia systemu.

§ 2

Zarządzenie wchodzi w życie z dniem podpisania.

Rektor

prof. dr hab. Jacek Woźny

Załącznik Nr 1
do Zarządzenia Nr 37/2016/2017
Rektora UKW
z dnia 30 marca 2017 r.

SZCZEGÓŁOWA POLITYKA BEZPIECZEŃSTWA UŻYTKOWANIA SYSTEMU INFORMATYCZNEGO "UNIWERSYTECKI SYSTEM OBSŁUGI STUDIÓW" W UNIWERSYTECIE KAZIMIERZA WIELKIEGO W BYDGOSZCZY

§ 1
Postanowienia ogólne

1. Szczegółowa Polityka Bezpieczeństwa Użytkowania Systemu Informatycznego "Uniwersytecki System Obsługi Studiów" (USOS) w Uniwersytecie Kazimierza Wielkiego w Bydgoszczy, zwanego dalej Systemem, jest dokumentem określającym podstawowe zasady dostępu do danych w systemie informatycznym USOS, zasady postępowania, stosowane środki techniczne i organizacyjne mające na celu zapewnienie bezpieczeństwa w systemie informatycznym USOS.
2. Polityka ma zastosowanie we wszystkich komórkach organizacyjnych UKW wykorzystujących system informatyczny USOS.

§ 2
Nadawanie, zawieszanie i odbieranie uprawnień do systemu informatycznego USOS

1. Kierownik komórki odpowiadającej za informatyzację Uniwersytetu wyznacza dla Systemu co najmniej jednego administratora systemu, posiadającego uprawnienia do zarządzania Systemem.
2. Dostęp do Systemu użytkownik uzyskuje na podstawie pisemnego wniosku potwierdzonego przez przełożonego, po pozytywnym rozpatrzeniu wniosku przez kierownika Działu Informatyzacji.
3. Wniosek musi zawierać imię i nazwisko użytkownika, jego stanowisko oraz zakres wnioskowanych uprawnień w Systemie wynikających z zakresu obowiązków służbowych.
4. Wniosek może odwoływać się do zdefiniowanych w systemie ról i powiązanych z nimi uprawnień. Zakres uprawnień dla roli zatwierdza kierownik Działu Informatyzacji.
5. Opis roli musi zawierać jej nazwę, zakres uprawnień przypisanych do roli oraz dla aktualnie obowiązującego opisu datę wprowadzenia, a dla opisów wcześniejszych daty obowiązywania.
6. Aktualne oraz wcześniejsze opisy ról przechowuje administrator Systemu.
7. W przypadku przejścia użytkownika na urlop bezpłatny, macierzyński, wychowawczy lub w przypadku innej nieobecności użytkownika trwającej powyżej 14 dni, bezpośredni przełożony użytkownika zobowiązany jest powiadomić niezwłocznie o tym fakcie administratora Systemu, a administrator zobowiązany jest niezwłocznie zawiesić aktywność konta użytkownika w Systemie.
8. Po powrocie użytkownika z nieobecności wymienionej w ust. 7 bezpośredni przełożony użytkownika powiadamia o tym fakcie administratora Systemu, a ten ponownie aktywuje konto użytkownika w Systemie.
9. W przypadku zakończenia zatrudnienia użytkownika w UKW lub zmiany zakresu obowiązków służbowych użytkownika, która spowoduje brak konieczności posiadania przez użytkownika

dostępu do Systemu, bezpośredni przełożony użytkownika zobowiązani są powiadomić niezwłocznie o tym fakcie administratora Systemu, a administrator zobowiązany jest niezwłocznie wyłączyć aktywność konta użytkownika w Systemie. Konta użytkowników w Systemie przechowywane są bezterminowo.

10. W przypadku zmiany zakresu obowiązków służbowych użytkownika, powodującej konieczność zmiany zakresu uprawnień użytkownika w Systemie, bezpośredni przełożony użytkownika zobowiązany jest złożyć nowy wniosek o dostęp użytkownika do Systemu, zawierający zakres wnioskowanych nowych uprawnień w Systemie. W przypadku pozytywnego rozpatrzenia takiego wniosku przez kierownika Działu Informatyzacji, administrator Systemu modyfikuje odpowiednio uprawnienia użytkownika w Systemie.

§ 3

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

1. Użytkownicy podłączeni do wewnętrznej separowanej sieci łączą się bezpośrednio do Systemu USOS. Użytkownicy spoza wewnętrznej sieci dostęp do serwera, na którym znajduje się System USOS uzyskują poprzez zalogowanie się do usługi VPN (Wirtualnej Sieci Prywatnej) przez podanie loginu i hasła przypisanego do e-Tożsamości UKW użytkownika. Dostęp do tego serwera poprzez usługę VPN mają jedynie uprawnieni użytkownicy Systemu USOS.
2. Użytkownik uzyskuje dostęp do Systemu poprzez podanie własnego identyfikatora i hasła dla Systemu USOS.
3. Identyfikator musi być unikatowy w Systemie i jest w sposób jednoznaczny przypisany do użytkownika i jego konta. Użytkownik jest odpowiedzialny za wszystkie czynności wykonane w Systemie przy użyciu swojego identyfikatora.
4. Hasło składa się z co najmniej ośmiu (8) znaków. Hasło musi zawierać przynajmniej jedną małą i jedną wielką literę oraz jedną cyfrę lub znak specjalny.
5. System automatycznie wymusza zmianę hasła co 30 dni.
6. System przechowuje historię haseł użytkownika z ostatniego roku i nie pozwala użytkownikowi na ponowne wykorzystanie hasła przechowywanego w historii.
7. Pierwsze hasło dla konta użytkownika wprowadza do Systemu administrator. Administrator ustawia odpowiedni parametr opisu konta użytkownika tak, by System wymusił na użytkowniku zmianę hasła podczas pierwszego logowania.

§ 4

Tworzenie kopii zapasowych Systemu

1. System oraz dane w nim przetwarzane podlegają zabezpieczeniu poprzez tworzenie kopii zapasowych.
2. Za wykonywanie kopii zapasowych odpowiada administrator Systemu.
3. Kopie zapasowe bazy danych Systemu muszą być wykonywane przed każdą aktualizacją Systemu (i przechowywane w takim przypadku co najmniej przez czas niezbędny do sprawdzenia poprawności działania Systemu) oraz po każdej aktualizacji.
4. Kopie zapasowe bazy danych Systemu muszą być wykonywane w każdy dzień roboczy, przed rozpoczęciem dnia pracy użytkowników.
5. Kopie zapasowe bazy danych Systemu muszą być przechowywane do czasu ustania ich przydatności.
6. Kopie zapasowe muszą być przechowywane w innej lokalizacji, niż pomieszczenie serwerowni.

§ 5
Zabezpieczenie jednostek końcowych przed działaniem złośliwego kodu

1. Za zabezpieczenie Systemu przed złośliwym kodem (np.: wirusami komputerowymi, końmi trojańskimi, oprogramowaniem szpiegującym, kradnącym dane lub hasła dostępu) na komputerze odpowiada użytkownik Systemu.
2. Środki na zakup odpowiedniego oprogramowania zabezpieczającego zapewnia Prorektor sprawujący nadzór nad informatyzacją Uniwersytetu, Kanclerz lub kierownicy jednostek wykorzystujących System.
3. Niedozwolone jest wyłączanie, blokowanie i odinstalowywanie programów zabezpieczających komputer przed złośliwym kodem oraz nieautoryzowanym dostępem z zewnątrz (np.: skanerów, programów antywirusowych, zapór firewall).