PISMO OKÓLNE

Nr 8/2013

Rektora
Uniwersytetu Marii Curie-Skłodowskiej
w Lublinie

z dnia 30 sierpnia 2013 r.

w sprawie procedur związanych z systemami informatycznymi Uniwersytetu przetwarzającymi dane osobowe

Na podstawie art. 66 ust. 2 ustawy z dnia 27 lipca 2005 r. - Prawo o szkolnictwie wyższym (tj. Dz. U. z 2012 r., poz. 572 z późn. zm.)

określam, co następuje:

§ 1
Procedury wykonywania kopii zapasowych w systemach informatycznych UMCS przetwarzających dane osobowe

1. Celem procedury jest określenie zasad tworzenia kopii zapasowych umożliwiających pełne odtworzenie funkcjonalności systemu informatycznego.
2. W celu zapewnienia bezpieczeństwa pracy systemu i możliwości odtworzenia danych po wystąpieniu awarii zaleca się następujące harmonogramy wykonywania poszczególnych kopii zabezpieczających:
    1) codzienne wykonywanie kopii przyrostowych, do tego kopiowania użyć tego samego nośnika danych (taśma magnetyczna, dysk CD-R, CD-RW, zrzut plików na dysk HDD do odpowiednio oznaczonego katalogu lub inny nośnik umożliwiający zapis), nośnik przechowywać (katalog na dysku HDD) przez min. 4 tygodnie. UWAGA: Dopuszcza się wykonywanie kopii na dysku HDD pod warunkiem, że jest to jedyny dostępny nośnik do wykonania kopii bezpieczeństwa przeznaczony tylko i wyłącznie na archiwizowanie danych;
    2) co tydzień wykonywać – pełną kopię, nośnik z danymi (taśma magnetyczna, dysk CD-R, CD-RW, zrzut plików na dysk HDD do odpowiednio oznaczonego katalogu lub inny nośnik umożliwiający zapis) przechowywać (katalog na dysku HDD) przez min. 4 tygodnie. UWAGA: Dopuszcza się wykonywanie kopii na dysku HDD pod warunkiem, że jest to jedyny dostępny nośnik do wykonania kopii bezpieczeństwa przeznaczony tylko i wyłącznie na archiwizowanie danych;
    3) co miesiąc, jeśli wymaga tego system, wykonać export bazy danych w dwóch kopiach, a nośniki przechowywać co najmniej 3 miesiące;

4) raz w miesiącu jeśli wymaga tego system wykonać kodowane kopiowanie plików aplikacji i bazy danych, nośnik przekazać upoważnionemu przedstawicielowi UMCS;
5) wykonywanie kopii systemu operacyjnego i oprogramowania (jeśli tego wymaga system) powinno być wykonane zawsze po zainstalowaniu nowych składników systemu lub zmianie konfiguracji. Zaleca się wykonanie nośników ratunkowych nie rzadziej niż co miesiąc. Powinny istnieć przynajmniej dwa zestawy takiej kopii zapisywane naprzemiennie.

3. Kopia pełna wraz z następującymi po niej kopiami przyrostowymi stanowią zestaw pozwalający na odtworzenie danych do chwili wykonania ostatniej kopii przyrostowej. Powinno istnieć przynajmniej 5 zestawów zapisanych jeden po drugim, jednak zestaw może zostać użyty po okresie nie krótszym niż 4 tygodnie.
4. Kopie danych powinny być okresowo sprawdzane pod kątem ich przydatności, prawidłowości wykonania oraz możliwości odtworzenia.
5. Każda kopia powinna zostać opisana w taki sposób, by zawierała następujące informacje:
   1) etykieta nośnika;
   2) data wykonania;
   3) numer kolejny nośnika;
   4) typ kopii;
   5) nazwa jednostki organizacyjnej;
   6) nazwa systemu informatycznego/zbioru danych;
   7) identyfikator osoby wykonującej kopię.
6. Narzędzia programowe i urządzenia do tworzenia kopii zależą od platformy sprzętowo-programowej, w przypadku ich braku to administrator systemu informatycznego określa sposób tworzenia kopii zabezpieczających.
7. Fakt wykonania kopii bezpieczeństwa administrator systemu odnotowuje w rejestrze – dzienniku tworzenia kopii bezpieczeństwa, który stanowi ***załącznik*** do niniejszego pisma okólnego. Dopuszczalne jest prowadzenie dziennika w formie elektronicznej.
8. Nośniki danych wykorzystywane do sporządzenia kopii nie mogą być stosowane do więcej niż:
   1) taśmy magnetyczne - 50 cykli kopiowania;
   2) dyski CD-RW - 1000 cykli kopiowania;
   3) pozostałe nośniki patrz zalecenia producenta.
9. Kopie zabezpieczające powinny być przechowywane w bezpiecznym miejscu, poza serwerownią.

§ 2
Procedury przekazywania do likwidacji lub naprawy sprzętu zawierającego nośniki z danymi osobowymi

1. Procedurę stosuje się do sprzętu, który uległ awarii, jest wycofywany z użycia lub podlega przeglądowi gwarancyjnemu i były lub są na nim przetwarzane dane osobowe bądź służy do wykonywania wydruków (w szczególności komputery, serwery, drukarki igłowe). Naprawa sprzętu powinna się odbyć w obecności upoważnionego do tego pracownika jeśli odbywa się na miejscu lub za pokwitowaniem podpisanym przez upoważnione osoby(ę) w przypadku przekazania sprzętu do jednostki naprawczej oraz firmie zajmującej się niszczeniem i/lub utylizacją.
2. Bezwzględnie należy przestrzegać zasady, że sprzęt na którym są przetwarzane dane osobowe nie może być przekazany do jednostki naprawczej/serwisowej lub jest naprawiany/serwisowany

w obecności upoważnionego pracownika UMCS. UWAGA: wszystkie umowy na dostawę dla UMCS sprzętu przeznaczonego do przetwarzania danych osobowych powinny zawierać stosowne zapisy w tym zakresie.
3. Ze sprzętu uszkodzonego przeznaczonego do naprawy poza jednostką lub zniszczenia muszą zostać usunięte nośniki informacji, tj. dyski, pamięci, tasiemki.
4. Fakt wymontowania nośnika musi zostać potwierdzony na piśmie (protokolarnie). Notatka (protokół) musi zawierać informacje kto i kiedy wymontował nośnik oraz czy został on zamontowany do innego sprzętu lub czy został zdeponowany w sejfie służącym przechowywania kopii bezpieczeństwa.
5. Notatki (protokoły) dołącza się do zgłoszenia awarii.
6. Nośniki informacji są niszczone mechanicznie, na wniosek kierownika jednostki organizacyjnej odpowiedzialnej za system informatyczny przetwarzający dane osobowe. Obsługę formalną procesu zapewnia specjalnie do tego celu powołana przez Rektora UMCS Komisja Likwidacyjna. Obsługę techniczną procesu zapewnia upoważniony pracownik LubMAN UMCS, przy czym sam proces fizycznego niszczenia nośników odbywa się nie częściej niż raz w miesiącu.

§ 3
Zasady ochrony systemów informatycznych UMCS przed zagrożeniami z sieci publicznej

1. Sieć komputerowa UMCS, w zakresie systemów informatycznych przetwarzających dane osobowe, jest odseparowana od sieci publicznej sprzętowymi firewallami.
2. Sieć komputerowa UMCS, w zakresie systemów informatycznych przetwarzających dane osobowe, zapewnia, poprzez stosowanie zapasowych łączy telekomunikacyjnych, niezawodność transmisji w celu uzyskania maksymalnego poziomu integralności i dostępności danych osobowych przekazywanych w systemach i sieciach teleinformatycznych.
3. Technologie oparte na falach radiowych nie mogą być wykorzystywane do przekazu danych osobowych, o ile połączenie nie jest szyfrowane. Takie połączenia mogą być używane jedynie dla wymiany poczty elektronicznej o ile wiadomo, że nie zawiera ona danych osobowych.
4. Wszystkie połączenia zewnętrzne do systemu informatycznego powinny być monitorowane, a logi połączeń archiwizowane w trybie ciągłym i bezterminowym.
5. System informatyczny służący do przetwarzania danych osobowych, administratorzy systemu powinni chronić przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem.
6. Zabezpieczenia logiczne, o których mowa w ust. 4 powyżej, obejmują:
    1) kontrolę przepływu informacji pomiędzy systemem informatycznym a siecią publiczną;
    2) kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego.
7. Kontrola powinna być nadzorowana przez administratorów systemu, a jej wynik powinien być dokumentowany w dziennikach pracy administratorów systemu.
8. Systemy informatyczne przetwarzające dane osobowe, które umożliwiają dostęp do swoich zasobów z sieci publicznej, za pomocą przeglądarek internetowych, muszą zapewniać w tym zakresie szyfrowanie transmisji za pomocą protokołu HTTPS.

§ 4
Zasady ochrony kryptograficznej transmisji

1. Przesyłanie danych osobowych drogą teletransmisji powinno odbywać się wyłącznie przy wykorzystaniu wymaganych zabezpieczeń logicznych chroniących przed nieuprawnionym dostępem, w szczególności takich jak ochrona kryptograficzna.
2. Administratorzy systemów Informatycznych przetwarzających dane osobowe są zobowiązani do zdalnego administrowania systemami przy użyciu narzędzi zapewniających ochronę kryptograficzną, np. protokół SSH.
3. Połączenia sieciowe realizowane z sieci publicznej do sieci chronionej w celu przetwarzania danych osobowych w systemach informatycznych muszą być realizowane za pomocą narzędzi zapewniających ochronę kryptograficzną, np. szyfrowane połączenie VPN.

§ 5

Pismo okólne wchodzi w życie z dniem podpisania.

R E K T O R

dr hab. Stanisław Michałowski, prof. nadzw.

Załącznik
do Pisma okólnego Nr 8/2013
Rektora UMCS

Dziennik tworzenia kopii systemu informatycznego

Lp.	Oznaczenie nośnika	Data wykonania	Typ kopii	Oznaczenie systemu/zbioru danych	Uwagi