Zarządzenie Nr 13/2011

Dyrektora Biblioteki Publicznej Gminy Kozienice
im. ks. Franciszka Siarczyńskiego w Kozienicach
z dnia 27 grudnia 2011 r.

instrukcja w sprawie bezpieczeństwa systemów informatycznych

Działając na podstawie § 10 Statutu Biblioteki Publicznej Gminy Kozienice im. Ks. F. Siarczyńskiego nadanego uchwałą Rady Miejskiej w Kozienicach Nr XXXI/514/2005 w sprawie zmiany nazwy i nadania statutu Bibliotece Publicznej Gminy Kozienice w nawiązaniu do Komunikatu Nr 23 Ministra Finansów z dnia 16 grudnia 2009 r. w sprawie ogłoszenia „Standardów kontroli zarządczej w jednostkach sektora finansów publicznych (Dz. Urz. M.F. Nr 15, poz. 84 z dnia 30.12.2009 r.) zarządzam co następuje:

§ 1.

1. Biblioteka Publiczna Gminy Kozienice, w celu bardziej wydajnego realizowania celów statutowych wykorzystuje sprzęt komputerowy działający w sieci i jako indywidualne stacje robocze oraz użytkowe programy i systemy informatyczne.
2. Za właściwy i optymalny dobór sprzętu komputerowego, jego sprawność oraz instalację odpowiedniego oprogramowania odpowiada Administrator sieci (Administrator systemu informatycznego ASI).
3. Realizując zadanie określone w ust 2, ASI w szczególności:
   - wnioskuje w sprawach zakupu sprzętu komputerowego i oprogramowania podnoszącego jakość pracy w Bibliotece,
   - troszczy się o bezpieczeństwo systemów informatycznych,
   - identyfikuje i analizuje zagrożenia oraz ryzyko, na które może być narażony system informatyczny,
   - zabezpiecza i kontroluje prawidłowość przebiegu czynności serwisowych sprzętu komputerowego oraz systemów informatycznych,
   - instaluje zabezpieczenia w systemach informatycznych,
   - przydziela uprawnienia do poszczególnych systemów,
   - wykonuje kopie zapasowe danych z serwerów, dba o właściwe przechowywanie nośników, sprawdza poprawność zapisu oraz ich likwidowanie,
   - dokonuje wyboru lub migracji do technologii minimalizującej zagrożenia uzyskania dostępu do sieci osobom nieupoważnionym,
   - nadaje hasła dostępu użytkownikom oraz określa uprawnienia w podległych im systemach,
   - wnioskuje w sprawie likwidacji sprzętu przestarzałego i programów, które przestały spełniać oczekiwania, albo zastąpiono je innymi
   - prowadzi ewidencje:
     a) programów i systemów informatycznych wykorzystywanych w Bibliotece,
     b) użytkowników wraz z przydzielonymi im uprawnieniami do poszczególnych funkcji systemu,
     c) sprzętu komputerowego wykorzystywanego w systemie informatycznym w Bibliotece
     d) czynności serwisowych wykonywanych w podległych systemach informatycznych.

§ 2.

1. Za właściwe wykorzystanie sprzętu komputerowego i zainstalowanych programów odpowiadają pracownicy Biblioteki, którzy są użytkownikami systemu informatycznego
2. Dla każdego użytkownika systemu informatycznego, w którym przetwarzane są dane osobowe przydziela się odrębny identyfikator i hasło oraz uprawnienia w systemie zgodnie z zakresem obowiązków.
3. ASI (ASIK) wyrejestrowuje z systemu identyfikator i hasło pracownika, który utracił uprawnienia dostępu do danych.
4. Identyfikatory pracowników oraz hasła dostępu do systemu informatycznego stanowią tajemnicę służbową.
5. Użytkownik po otrzymaniu indywidualnego identyfikatora powinien go zapamiętać, a otrzymane hasło zmienić na znane tylko sobie.
6. Identyfikatorów i haseł nie należy ujawniać, ani zapisywać w miejscach, które umożliwiłyby osobom niepowołanym zapoznanie się nimi.

§ 3.

1. Przed rozpoczęciem pracy użytkownik powinien sprawdzić, czy stan sprzętu komputerowego nie wskazuje na próbę używania tegoż sprzętu przez osobę niepowołaną.
2. Użytkownicy uzyskują bezpośredni dostęp do danych w aplikacji po podaniu identyfikatora i właściwego hasła.
3. Kończąc pracę użytkownik powinien:
   a) wykonać kopię zapasową, jeśli jest do tego zobowiązany,
   b) sprawdzić czy w napędach komputera nie pozostały nośniki zawierające dokumenty lub informacje zawierające dane osobowe, niejawne lub inne do których wgląd powinny mieć jedynie osoby upoważnione,
   c) zamknąć program oraz wylogować się z systemu i wyłączyć komputer oraz inne wykorzystywane urządzenia komputerowe np. drukarka, skaner, itp.,
   d) wyłączyć listwę zasilającą z dopływu prądu,
   e) sprawdzić, czy pozostawione stanowisko pracy nie stwarza jakichkolwiek zagrożeń.
4. Wszystkie zauważone usterki i mankamenty na stanowisku użytkownik powinien natychmiast zgłosić bezpośredniemu przełożonemu oraz ASI.

§ 4.

1. W przypadku stwierdzenia przez użytkownika naruszenia zabezpieczeń systemu informatycznego, na które mogą wskazywać:
   a) stan stacji roboczej (problemy z uruchomieniem, rozkręcona obudowa),
   b) różnice w funkcjonowaniu systemu
   c) różnica w zawartości zbioru danych (np. brak lub nadmiar danych),

   jest on zobowiązany niezwłocznie powiadomić o tym bezpośredniego przełożonego oraz ASI.

§5.

1. Dane zgromadzone w pamięciach komputerów powinny być zabezpieczone przed ich utratą przez tworzenie ich kopii zapasowych w trybie codziennym lub miesięcznym.
2. Za archiwizację danych przechowywanych w pamięci komputerów lokalnych odpowiedzialni są użytkownicy. Archiwizacji należy dokonywać w każdym dniu, w którym dokonywane były jakiekolwiek zmiany. Dane powinny być kopiowane na wyznaczony dysk sieciowy, pamięć USB, dyski przenośne lub płyty CD-R, a następnie przechowywane w bezpiecznym miejscu.
3. ASI może zautomatyzować (jeżeli jest taka możliwość) proces wykonywania kopii bezpieczeństwa na wniosek użytkownika.
4. Za archiwizację danych przechowywanych w pamięci serwerów sieciowych odpowiedzialny jest ASI.
5. W cyklu codziennym należy archiwizować bazy systemu bibliotecznego, a w cyklu miesięcznym bazy pozostałych systemów.
6. Kopie zapasowe danych z serwera archiwizowane w cyklu miesięcznym należy przechowywać w odpowiednio zabezpieczonym miejscu, poza pomieszczeniem w którym znajduje się serwer.
7. Bazy danych przetwarzanych przez system Aleph archiwizowane są przez informatyków Biblioteki Wojewódzkiej w Warszawie i gromadzone na serwerze w Bibliotece - Warszawa, ul. Koszykowa 28.
8. Bazy danych przetwarzanych przez system KOHA archiwizowane są przez informatyka zarządzającego systemem i gromadzone na serwerze w Bibliotece Głównej, ul. J. Kochanowskiego 22.
9. Kopie zapasowe, o których mowa w ust. 2, 5, 6 powinny być przechowywane co najmniej do czasu sporządzenia kolejnej kopii.
10. Nośniki z kopiami zapasowymi powinny być odpowiednio chronione i zabezpieczone przed utratą.

§6.

W celu zwiększenia bezpieczeństwa sieci zabrania się:

1. Udostępniania stanowisk roboczych oraz istniejących na nich danych (w postaci elektronicznej jak i wydruków) osobom nieupoważnionym,
2. Wykorzystywania sieci komputerowej w celach innych niż służbowe,
3. Samowolnego instalowania i używania programów komputerowych (posiadających lub nie posiadających licencji),
4. Trwałego lub czasowego kopiowania programów komputerowych w całości lub w części jakimikolwiek środkami i w jakiejkolwiek formie,

5. Przenoszenia programów komputerowych z własnego stanowiska roboczego na inne stanowisko,
6. Wykorzystywania oprogramowania lub materiałów ściąganych z Internetu do masowego rozpowszechniania bez upoważnienia ASI,
7. Pobierania lub uruchamiania programów otrzymanych pocztą elektroniczną oraz otwierania listów lub załączników w nich zawartych wątpliwego pochodzenia,
8. Kopiowania całości lub części baz danych zawierających dane osobowe na jakichkolwiek nośnikach bez zgody ASI.
9. Pozostawiania bez nadzoru uruchomionych stanowisk roboczych zawierających dane osobowe lub poufne.

§7.

1. W celu zapewnienia bezpieczeństwa systemu informatycznego w Bibliotece zobowiązuję ASI do:
   a) Sporządzenia specyfikacji systemów informatycznych i programów użytkowanych w Bibliotece, w podziale na placówki - w terminie do 15 stycznia oraz weryfikacji zestawienia po każdej zmianie.
   b) Sporządzenia listy użytkowników systemów i programów informatycznych wraz z przydzielonymi im uprawnieniami do poszczególnych funkcji systemu, w podziale na placówki - w terminie do 15 stycznia.
   c) Sporządzenia specyfikacji sprzętu komputerowego wykorzystywanego w Bibliotece, w podziale na placówki - w terminie do 15 stycznia.
   d) Systematycznej adnotacji czynności serwisowych wykonywanych w podległych systemach informatycznych - sukcesywnie, począwszy od wejścia w życie zarządzenia.

§8.

Zobowiązuję Specjalistę ds. organizacyjno-administracyjnych do zapoznania pracowników Biblioteki z treścią zarządzenia.

§9.

Zarządzenie wchodzi w życie z dniem podpisania.

DYREKTOR

mgr Elżbieta Stąpór