PRZEDSZKOLE SAMORZĄDOWE NR 26
INTEGRACYJNE
IM. JOANNY STRZAŁKOWSKIEJ-KUCZYŃSKIEJ
w BIAŁYMSTOKU
15-472 Białystok, ul. Ciepła 19
tel./fax 85 6754255, e-mail: ps26@um.bialystok.pl
NIP 5423189823, REGON 200406865

(oznaczenie dyrektora przedszkola)

Zarządzenie Nr 5/2024

Dyrektora Przedszkola Samorządowego nr 26 Integracyjnego

im. Joanny Strzałkowskiej – Kuczyńskiej w Białymstoku

z dnia 07.02.2024

w sprawie określenia Zasad administrowania systemem informatycznym w Przedszkolu Samorządowym Nr 26 Integracyjnym im. Joanny Strzałkowskiej-Kuczyńskiej w Białymstoku.

Na podstawie art. 68 ust. 1 pkt. 12 ustawy z 14.12.2016 r. - Prawo oświatowe (Dz. U. z 2021 r., poz. 1082) w związku z art. 24 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L119 s.1 z 2016 r., sprost. Dz. Urz. UE L127 s.2 z 2018 r., sprost. Dz. Urz. UE L74 s.35 z 2021 r.),

zarządzam, co następuje:

§ 1

1. Ustala się Zasady administrowania systemem informatycznym w **Przedszkolu Samorządowym Nr 26 Integracyjnym im. Joanny Strzałkowskiej-Kuczyńskiej w Białymstoku** w treści stanowiącej załącznik do zarządzenia.

2. Ustanowienie Zasad administrowania systemem informatycznym ma na celu podniesienie poziomu bezpieczeństwa informacji w związku z zarządzaniem systemem informatycznym w **Przedszkolu Samorządowym Nr 26 Integracyjnym im. Joanny Strzałkowskiej-Kuczyńskiej w Białymstoku** poprzez określenie zasad przetwarzania informacji, wprowadzenie procesów ułatwiających zarządzanie i monitorowanie bezpieczeństwa oraz przypisanie odpowiedzialności w sposób zapewniający odpowiedni poziom bezpieczeństwa informacji i oraz zgodnie z obowiązującymi przepisami prawa.

§ 2

Zobowiązuje się wszystkie osoby administrujące systemem informatycznym **Przedszkola Samorządowego Nr 26 Integracyjnego im. Joanny Strzałkowskiej-Kuczyńskiej w Białymstoku** do przestrzegania **Zasad administrowania systemem informatycznym w Przedszkolu Samorządowym Nr 26 Integracyjnym im. Joanny Strzałkowskiej-Kuczyńskiej w Białymstoku**.

§ 3

Niniejsze zarządzenie wchodzi w życie z dniem podpisania.

DYREKTOR PRZEDSZKOLA
mgr Beata Józkowicz
.....
(podpis dyrektora)

PRZEDSZKOLE SAMORZĄDOWE NR 26
INTEGRACYJNE
IM. JOANNY STRZAŁKOWSKIEJ-KUCZYŃSKIEJ
w BIAŁYMSTOKU
15-472 Białystok, ul. Ciepła 19
tel./fax 85 6754255, e-mail: ps26@um.bialystok.pl
NIP 5423189823, REGON 200406865

Załącznik nr 1
do Zarządzenia nr 5/2024
dyrektora Przedszkola Samorządowego nr 26 Integracyjnego

im. Joanny Strzałkowskiej – Kuczyńskiej w Białymstoku

z dnia 07.02.2024

Zasady administrowania systemem informatycznym

Spis treści:

Rozdział 1

Zasady ogólne

§ 1

1. Zasady administrowania systemem informatycznym obowiązują wszystkich informatyków administrujących systemem informatycznym, zwanych dalej ASI.
2. Podstawowym obowiązkiem ASI jest zapewnienie bezpieczeństwa systemu informatycznego, rozumianego jako zapewnienie poufności, integralności, rozliczalności, autentyczności, dostępności i odporności.
3. Za dobór środków ochrony systemu informatycznego odpowiada ASI. Dobór środków ochrony powinien być odpowiedzią na zagrożenia bezpieczeństwa, wynikać z wiedzy fachowej ASI, zapewniać zgodność z niniejszymi Zasadami administrowania systemem informatycznym oraz oczekiwaniami Dyrektora placówki.

Rozdział 2

Zarządzanie aktywami sprzętowymi oraz informacyjnymi

§ 2

Bezpieczeństwo aktywów

1. ASI prowadzi ewidencję sprzętu komputerowego zawierającą m. in. numer inwentarzowy, producenta, nazwę modelu urządzenia oraz lokalizację urządzenia.
2. Sprzęt komputerowy podlega inwentaryzacji prowadzonej zgodnie z zasadami określonymi dla środków trwałych.
3. Niezgodności w inwentaryzacji oraz nieautoryzowane zmiany konfiguracji należy zgłaszać jako incydent.

§ 3

Nośniki informacji

1. Nośniki informacji należy chronić przed nieautoryzowanym dostępem lub zniszczeniem.
2. ASI odpowiada za trwałe usuwanie danych z elektronicznych nośników danych, w tym przekazywanych przez użytkowników. W przypadku braku możliwości trwałego usunięcia danych z elektronicznych nośników danych należy rozważyć ich wycofanie z użytku i bezpiecznego zniszczenia.
3. Wycofane nośniki należy zniszczyć w bezpieczny sposób lub przechowywać w miejscu chronionym przed nieuprawnionym dostępem. Z przeprowadzonej operacji należy zapewnić stosowny protokół potwierdzający skuteczne dokonanie zniszczenia.
4. Po zakończeniu pracy lub używania nośnika informacji, należy go przechowywać w wyznaczonym do tego celu miejscu na terenie obszaru kontrolowanego dostępu i stosownie do wymogów wobec zawartej na nośniku informacji.

5. Trwałe usuwanie danych z elektronicznych nośników danych należy wykonywać poprzez wielokrotny zapis na nośniku (co najmniej 4-krotny).
6. Dane w postaci elektronicznej należy usunąć z nośnika informacji w sposób uniemożliwiający ich ponowne odtworzenie, zgodny z typem nośnika, nie później niż po upływie 3 dni po zakończeniu ich wykorzystywania chyba, że z odrębnych przepisów wynika obowiązek ich przechowywania.

§ 4

Zasady bezpieczeństwa fizycznego i środowiskowego

1. ASI odpowiada za weryfikację wymogów fizycznych i środowiskowych dotyczących pomieszczeń zawierających wartościowy sprzęt komputerowy oraz telekomunikacyjny jak również dane podlegające ochronie.
2. ASI jest zobowiązany poinformować Dyrektora o niezgodnościach związanych z wymogami fizycznymi i środowiskowymi.
3. Fakt przeprowadzenia napraw i konserwacji należy dokumentować.
4. Jeśli producent nie przewidział dla danego urządzenia lub oprogramowania potrzeby dokonywania konserwacji lub też nie określił ich częstotliwości, to o ich przeprowadzeniu oraz sposobie jego przeprowadzenia decyduje ASI.

Rozdział 3

Bezpieczna konfiguracja

§ 5

Zarządzanie uprawnieniami

1. ASI odpowiada za nadawanie, zmianę i odbieranie uprawnień.
2. ASI nadaje dostęp do systemu informatycznego na podstawie stosownego wniosku lub upoważnienia wydanego przez dyrektora lub osobę przez niego wskazaną.
3. Przy nadawaniu uprawnień, obowiązuje zasada wiedzy koniecznej tj. ograniczania nadawania uprawnień w systemie informatycznym do niezbędnego minimum wynikającego z upoważnienia lub określonego w upoważnieniu.
4. W systemie informatycznym stosuje się uwierzytelnianie dwustopniowe, na poziomie:
   1) dostępu do systemu operacyjnego;
   2) dostępu do aplikacji.
5. Do uwierzytelnienia użytkownika w systemie na obu poziomach uwierzytelniania używa się unikalnych identyfikatorów użytkowników oraz haseł, tak aby wszelkie działania można było przypisać w sposób jednoznaczny konkretnemu użytkownikowi.
6. Przekazywanie haseł musi odbywać się w sposób bezpieczny, w zamkniętej kopercie, bezpośrednio pomiędzy osobami zainteresowanymi.

7. Zaleca się aby system informatyczny automatycznie wymuszał na użytkowniku zmianę nadanego hasła przy pierwszym logowaniu.
8. Należy stosować następujące polityki haseł:
   1) z wymuszaniem zmiany hasła:
      a) system wymusza zmianę hasła co 30 dni lub co miesiąc,
      b) hasło musi mieć co najmniej 8 znaków,
      c) hasło musi zawierać dużą literę, cyfrę oraz znak specjalny;
   2) bez wymuszania zmiany hasła:
      a) brak wymuszonej okresowej zmiany hasła,
      b) blokada tworzenia hasła znajdującego się na liście słabych i często używanych haseł,
      c) blokada hasła zawierającego przewidywalne człony,
      d) hasło musi mieć co najmniej 12 znaków,
      e) system musi umożliwiać utworzenie hasła nie krótszego niż 64 znaki,
      f) brak dodatkowych kryteriów złożoności np. znaków specjalnych, cyfr, czy dużych liczb;
   3) uwierzytelnienie dwuskładnikowe:
      a) do uwierzytelnienia wymagane jest użycie dwóch składników tj. hasła oraz tokenu sprzętowego, kodu otrzymanego na SMS, karty procesorowej,
      b) system nie wymaga zmiany hasła,
      c) hasło musi mieć co najmniej 8 znaków.
9. Przy wprowadzaniu nowych rozwiązań informatycznych należy wykorzystywać politykę haseł bez wymuszania zmiany hasła lub uwierzytelnienie dwuskładnikowe. Polityka haseł z wymuszanie zmiany hasła jest wycofywana i zabrania się jej wprowadzania do użytku w nowych rozwiązaniach.

§ 6

Wykorzystywanie kont awaryjnych z uprawnieniami administratora

1. Informacje niezbędne do zalogowania się na awaryjne konta z uprawnieniami administracyjnymi podlegają szczególnej ochronie poprzez składowanie tych informacji u Dyrektora lub upoważnionego przez niego pracownika, innego niż ASI.
2. W wypadku, gdy systemem informatycznym administruje Centrum Usług Informatycznych w Białymstoku, Dyrektor Centrum Usług Informatycznych w Białymstoku zapewnia przechowywanie informacji niezbędnych do zalogowania się na awaryjne konta z uprawnieniami administracyjnymi.
3. ASI jest odpowiedzialny za przekazanie informacji o awaryjnych kontach administracyjnych do upoważnionej osoby w zapieczętowanej kopercie, w sposób umożliwiający zalogowanie się do obszaru którego dotyczą.

4. Jeżeli dane do logowania w jakimkolwiek zakresie się zmienią, ASI pod rygorem konsekwencji dyscyplinarnych, zobowiązany jest dokonać ponownego przekazania, o którym mowa w ust. 1 i 2.
5. Przekazywanie haseł do awaryjnych kont administracyjnych musi odbywać się w sposób bezpieczny, w zamkniętej kopercie, bezpośrednio pomiędzy osobami zainteresowanymi.
6. Jeżeli dany system informatyczny lub urządzenie nie przewiduje możliwości założenia dodatkowego konta administracyjnego, to czynności opisane w niniejszym paragrafie są przeprowadzane na koncie administracyjnym przypisanym ASI.

§ 7

Zabezpieczanie systemów operacyjnych

1. Zgodnie z zasadą minimalnych uprawnień, należy zapewnić by każdy pracownik posiadał dostęp wyłącznie do tych zasobów, które są mu niezbędne do wykonania powierzonych obowiązków służbowych.
2. Stacje robocze należy skonfigurować w taki sposób by użytkownicy nie posiadali uprawnień administracyjnych, jak również dostępu do zasobów zbędnych do wykonywanych zadań, w szczególności do Internetu, oprogramowania, systemów i narzędzi. Zakres uprawnień należy zapewnić zgodnie z zasadą wiedzy koniecznej.
3. Na komputerach użytkowników powinno być instalowane jedynie legalne oprogramowanie.
4. Serwery plików, serwery poczty elektronicznej, stacje robocze oraz urządzenia mobilne należy zabezpieczać aktualnym oprogramowaniem antywirusowym.
5. Konfiguracja oprogramowania antywirusowego powinna uniemożliwiać wyłączenie go przez użytkownika.

§ 8

Zabezpieczanie sieci i zasobów

1. Należy zarządzać i nadzorować sieci w celu ochrony informacji w systemach i aplikacjach, w szczególności:
   1) należy stosować ochronę sieci przed nieuprawnionym dostępem z zewnętrznych sieci poprzez wykorzystanie zapór sieciowych, urządzeń wykrywających i przeciwdziałających nieautoryzowanemu dostępowi;
   2) należy wydzielać strefy DMZ dla usług dostępnych z zewnętrznych sieci w tym Internet;
   3) należy monitorować ruch przychodzący i wychodzący w sieci i zapewniać mechanizmy tworzenia dzienników zdarzeń oraz rozliczalność pracowników, jak również zewnętrznych dostawców;
   4) należy stosować tam gdzie to możliwe izolację i segmentację sieci zgodnie z zakresem wykorzystywanych usług i zasobów, w szczególności izolowanie obszarów podwyższonego ryzyka, w tym:

a) środowisk produkcyjnych i testowych,
b) serwerów,
c) stacji roboczych,
d) urządzeń peryferyjnych,
e) systemów bez wsparcia producenta, a w wyniku czego pozbawionych aktualizacji bezpieczeństwa,
f) infrastruktury zewnętrznych dostawców,
g) pracowni komputerowych;

5) należy zapewnić filtrowanie poczty oraz połączeń realizowanych za pomocą przeglądarki www pod względem szkodliwych treści;
6) należy stosować zabezpieczenia przed nieuprawnionym dostępem do zasobów sieci z wewnątrz sieci lokalnej;
7) należy stosować mechanizmy ochrony danych jak np. szyfrowanie, podczas przesyłania poufnych lub krytycznych informacji przez sieci (np. dane uwierzytelniające, poufne informacje);
8) w przypadku dostępu do sieci placówki przez dostawców zewnętrznych lub pracowników, dokonywanego z sieci zewnętrznej należy ograniczać ten dostęp do dedykowanego urządzenia. Dostęp do zasobów należy zapewnić na zasadach wiedzy koniecznej.

2. Administrator danego urządzenia sieciowego ma obowiązek zmienić dostarczone wraz z pierwszą konfiguracją urządzenia hasła.
3. Zarządzanie siecią odbywa się wyłącznie z wydzielonych, wcześniej zdefiniowanych stacji roboczych lub tam, gdzie jest to technicznie możliwe i wykonalne poprzez konsole bezpośrednio podłączone do urządzeń sieciowych.

§ 9

Kryptografia

1. Szyfrowanie obejmuje obowiązkowo:
   1) dyski twarde komputerów przenośnych;
   2) elektroniczne nośniki danych zawierające dane osobowe, które są wynoszone poza teren placówki;
   3) załączniki wiadomości poczty elektronicznej zawierające dane osobowe;
   4) kanały komunikacyjne do sieci informatycznej oraz do serwera placówki z Internetu.
2. ASI odpowiada za wdrożenie do użytku narzędzi do szyfrowania, w tym do udostępnienia ich użytkownikom.
3. Minimalne wymagania szyfrowania powinny uwzględniać szyfrowanie zbiorów algorytmem powszechnie uważanym za bezpieczny i z użyciem odpowiednio długiego i skomplikowanego hasła.

Rozdział 4

Zasady wprowadzania zmian w środowisku informatycznym, w tym bezpieczne pozyskiwanie urządzeń oraz systemów

§ 10

1. Pozyskiwanie nowych urządzeń, oprogramowania oraz systemów informatycznych stanowi zmianę w środowisku informatycznym i wymaga podjęcia działań zapewniających bezpieczeństwo informacji do których należą:
   1) zaplanowanie procesu zmian w środowisku informatycznym, uwzględniając zidentyfikowanie ryzyka jakie wprowadza zmiana, wykonanie kopii zapasowych danych i oprogramowania, niezbędne do przeprowadzenia testy poprawności, przygotowanie procedury wycofania się ze zmiany, w przypadku problemów, których nie można usunąć;
   2) przedstawienie planu procesu zmian w środowisku informatycznym Dyrektorowi i uzyskanie jego zgody na wykonanie tych zmian;
   3) przeprowadzanie testów poprawności po wykonaniu zmiany;
   4) zapewnienie kontroli wersji oprogramowania oraz bezpiecznych repozytoriów dla kodu i oprogramowania.
2. Za wykonanie zadań, o których mowa w ust. 1 odpowiada ASI.
3. ASI jest zobowiązany informować Dyrektora o ryzykach związanych z wdrożeniem i utrzymaniem urządzeń oraz systemów informatycznych oraz proponować rozwiązania zmniejszające te ryzyka.

Rozdział 5

Zasady bezpiecznej eksploatacji

§ 11

Zarządzanie pojemnością

ASI planuje, monitoruje i dostosowuje wykorzystanie zasobów oraz przewiduje wymaganą ich pojemność. Ponadto, identyfikuje i eliminuje wąskie gardła, jak również miejsca pojedynczej awarii (dotyczy to również uzależnienia od kluczowego personelu i dostawców).

§ 12

Kopie bezpieczeństwa

1. ASI odpowiada za wykonywanie kopii bezpieczeństwa danych i oprogramowania zgromadzonych na serwerze.
2. ASI zapewnia dokładny i kompletny spis kopii zapasowych oraz procedur ich odtwarzania.
3. ASI regularnie weryfikuje poprawność zapisywania kopii zapasowych i możliwość odtworzenia z nich informacji w przypadku awarii.

4. W przypadku gromadzenia danych w bazie danych zainstalowanej na komputerze użytkownika:
   1) za przygotowanie i przekazanie do użytku procedury wykonywania kopii bezpieczeństwa oprogramowania i danych zgromadzonych w bazie danych na komputerze użytkownika odpowiada ASI;
   2) za wykonywanie kopii zgodnie z przekazaną mu procedurą odpowiada użytkownik komputera;
   3) za okresowe wykonywania testów przydatności kopii zapasowych odpowiada ASI.
5. Kopie zapasowe należy zabezpieczać przed nieautoryzowanym dostępem.
6. Kopie bezpieczeństwa powinny być planowane w sposób umożliwiający odtworzenie danych po utracie lub uszkodzeniu wraz ze środowiskiem programowym, w którym były przetwarzane.
7. Kopie bezpieczeństwa wykonywane są:
   1) cyklicznie, zgodnie z ustalonym harmonogramem wykonywania kopii;
   2) w związku z zakończeniem funkcjonowania systemu, zwane dalej kopiami końcowymi systemu.
8. Do wykonywania kopii cyklicznych należy wykorzystywać co najmniej 2 komplety nośników danych, każdy komplet wykorzystywany w kolejnym cyklu wykonywania kopii danych.
9. Kopie końcowe systemu przechowywane są przez okres co najmniej 15 lat. Raz na 5 lat następuje przegląd kopii końcowych, podczas którego ustalana jest ich przydatność. W wypadku, gdy systemem informatycznym administruje Centrum Usług Informatycznych w Białymstoku, podejmowana jest tam decyzja o ewentualnym wycofaniu kopii z użytku. Dla pozostawionych kopii bezpieczeństwa ustalany jest dalszy okres przechowywania.
10. Kopie końcowe systemu muszą zawierać:
    1) dane przetwarzane w systemie informatycznym;
    2) oprogramowanie systemu;
    3) informacje o sposobie odtworzenia, instalacji i uruchomienia systemu informatycznego;
    4) hasła administracyjne w zapieczętowanej kopercie.
11. Nie stosuje się ochrony kryptograficznej kopii końcowych systemu.
12. Kopie cykliczne oraz kopie końcowe systemu wykonuje się na zewnętrznych, odłączanych od infrastruktury nośnikach: taśmach magnetycznych, płytach CD/DVD, magnetycznych dyskach twardych.
13. Niedopuszczalne jest wykonywanie kopii końcowych systemu na trwałych pamięciach elektronicznych typu flash.
14. Niezależnie od wymienionych w ust. 2 kopii bezpieczeństwa, ASI może wykonywać kopie tymczasowe, których potrzeba wynika z prac administracyjnych. Kopie tymczasowe nie mogą być przechowywane dłużej, niż przez okres 3 miesięcy.
15. Oznaczenie nośników kopii końcowych systemu zawiera co najmniej:
    1) oznaczenie roku, miesiąca i dnia, w którym kopia została wykonana;

2) słowne oznaczenie obszaru funkcjonalnego, z którego pochodzi np. poprzez podanie: nazwy serwera, blade, nazwy storage, nazwy systemu.

16. Kopie końcowe systemu są ewidencjonowane w „Rejestrze nośników kopii zapasowych" prowadzonym w formie papierowej, zawierającym co najmniej informacje:
    1) oznaczenie nośników kopii danych;
    2) wykaz zawartości nośnika kopii danych;
    3) informację o narzędziach programowych i sprzętowych wykorzystanych do wykonania kopii danych (producent, nazwa, wersja, system operacyjny);
    4) czy kopia na nośniku została wykonana poprawnie wraz z datą i podpisem ASI potwierdzającym wykonanie weryfikacji kopii danych - w razie potrzeby należy dodać uwagi do wykonania kopii np. jakie elementy zostały wyłączone z kopii;
    5) czy nośnik został przekazany do archiwum kopii danych wraz z datą i podpisem ASI potwierdzającym ten fakt;
    6) czy nośnik został wycofany z użytku wraz z datą i podpisem ASI potwierdzającym fakt wycofania z użytku.

§ 13

Logowanie i monitorowanie zdarzeń

1. Należy zapewnić monitorowanie podstawowych parametrów środowiskowych w serwerowniach, w szczególności temperatury i wilgotności otoczenia.
2. Należy zapewnić logowanie i monitorowanie przyłączonych do środowiska teleinformatycznego urządzeń pod względem:
    1) obecności w środowisku teleinformatycznym;
    2) poprawnej konfiguracji;
    3) prawidłowego działania.
3. Należy tworzyć, przechowywać i regularnie przeglądać dzienniki zdarzeń w systemach w szczególności rejestrujące:
    1) dostęp do systemu z uprawnieniami administracyjnymi;
    2) dostęp do konfiguracji systemu w tym konfiguracji zabezpieczeń;
    3) działania użytkowników;
    4) błędy i wyjątki;
    5) zdarzenia związane z bezpieczeństwem informacji;
    6) funkcjonowanie i aktualności baz wirusów oprogramowania antywirusowego;
    7) przeprowadzanie aktualizacji oprogramowania stacji roboczych w zakresie systemów operacyjnych, przeglądarek internetowych, pakietów oprogramowania biurowego;
    8) wykonywanie kopii bezpieczeństwa danych.
4. Należy chronić dzienniki zdarzeń przed nieautoryzowanym dostępem.

5. Należy logować i monitorować aktywność urządzeń sieciowych, wykorzystanie łącza i usług sieciowych, w szczególności:
   1) ruchu wchodzącego do Sieci Lokalnej z Sieci Rozległej oraz ruchu wychodzącego z Sieci Lokalnej do Sieci Rozległej w zakresie informacji umożliwiających ustalenie urządzenia i osoby, które były związane z tym ruchem;
   2) prób autoryzacji i udanych autoryzacji do systemów operacyjnych serwerów, stacji roboczych, baz danych, programów, urządzeń sieciowych oraz innych urządzeń biorących udział przy przetwarzaniu danych takich jak: NAS, SAN, biblioteki taśmowe;
   3) stanu funkcjonowania serwerów oraz urządzeń do składowania danych w zakresie ostrzeżeń i alarmów zgłaszanych przez systemy operacyjne zainstalowane na tych urządzeniach;
   4) zmian konfiguracji urządzeń sieciowych;
   5) przydziału adresów IP z usług DHCP;
   6) podłączania urządzeń do Sieci Lokalnej.
6. Monitorowanie systemu informatycznego musi umożliwiać identyfikację użytkowników systemu oraz urządzeń i zakresu ich działań. Dopuszcza się identyfikację pośrednią na podstawie kilku obszarów monitorowania.
7. Oprogramowanie niespełniające wymogów monitoringu należy dostosować do potrzeb monitoringu na etapie eksploatacji w trakcie pierwszej istotnej modyfikacji tego oprogramowania.
8. Informacje dzienników systemów należy przechowywać nie krócej, niż przez 12 miesięcy od dnia zapisu.
9. Należy zapewnić bezpieczny dostęp do logów, umożliwiający niepodważalne i jednoznaczne identyfikowanie zdarzeń i osób je wykonujących.
10. Za poprawne zapisywanie logów z systemów odpowiada ASI
11. Należy zapewnić każdemu z systemów infrastruktury jednakowe źródło informacji o czasie.

§ 14

Monitorowanie pracy użytkowników

1. Przez monitorowanie pracy użytkownika rozumie się zespół działań ukierunkowanych na śledzenie aktywności użytkownika systemu.
2. Monitorowanie pracy użytkownika dopuszczalne jest w szczególnych i uzasadnionych przypadkach, w celu:
   a) realizacji obsługi informatycznej w zakresie analizy i rozwiązywania problemów związanych z funkcjonowaniem systemu informatycznego,
   b) zapewnienia bezpieczeństwa systemu informatycznego,
   c) kontroli jakościowej i ilościowej pracy.

3. Monitorowanie pracy użytkowników wymaga zapewnienia zgodności z przepisami prawa, a w szczególności z Kodeksem Pracy. W tym celu ASI, przed rozpoczęciem monitorowania musi uzgodnić jego zakres z Dyrektorem.
4. Przed każdym podłączeniem się pod zdalny pulpit na komputerze wykorzystywanym przez użytkownika należy poinformować użytkownika o tym fakcie.
5. Niedopuszczalne jest dokonywanie kontroli ilościowej i jakościowej pracy pracownika przy komputerze bez jego wiedzy.
6. Wszelkie wykorzystywane techniki monitoringu muszą ograniczać możliwość poznania haseł użytkownika. W przypadku nieumyślnego poznania hasła użytkownika należy go, o tym fakcie poinformować.

§ 15

Podatności techniczne

1. Należy identyfikować i eliminować podatności bezpieczeństwa, w szczególności poszukiwać informacji o powszechnie znanych błędach oprogramowania np. na specjalistycznych stronach internetowych, forach dyskusyjnych, mediach społecznościowych lub listach mailingowych.
2. Należy zapewnić ciągłą aktualizację wszystkich systemów operacyjnych środowiska teleinformatycznego, ze szczególnym uwzględnieniem aktualizacji krytycznych.
3. W przypadku braku możliwości aktualizacji systemu, należy rozważyć jego izolację.
4. Należy zapewnić konfigurację elementów środowiska teleinformatycznego zgodnie z najlepszymi praktykami:
   1) należy zapewnić działanie infrastruktury w minimalnej potrzebnej konfiguracji;
   2) należy odinstalować bądź dezaktywować zbędne oprogramowanie;
   3) należy dezaktywować zbędne usługi i procesy;
   4) należy przeglądać konfigurację.

§ 16

Przeglądy i konserwacja infrastruktury technicznej

1. Przeglądy infrastruktury teleinformatycznej powinny odbywać się regularnie w zaplanowanym czasie i zakresie oraz minimalnym wpływie na środowisko produkcyjne i powinny obejmować:
   1) przegląd logów i konfiguracji infrastruktury placówki;
   2) skanowanie podatności infrastruktury teleinformatycznej;
   3) przegląd zestawień inwentaryzacyjnych sprzętu;
   4) weryfikację stanu przeglądów i konserwacji urządzeń;
   5) weryfikację poprawności realizacji umów przez strony trzecie;
   6) weryfikację legalności oprogramowania i stanu licencji.

2. Urządzenia i oprogramowanie wymaga dokonywania konserwacji i przeglądów zgodnie z terminami określonymi przez producenta. Jeżeli producent nie określił ich częstotliwości, to o ich przeprowadzeniu oraz sposobie jego przeprowadzenia decyduje ASI.
3. Wyniki przeglądów powinny być chronione i udostępniane na zasadach wiedzy koniecznej.

Rozdział 6

Dokumentacja systemu informatycznego

§ 17

1. Na dokumentację systemu informatycznego składa się co najmniej:
   1) dokumentacja licencyjna oprogramowania tj. wszystkie atrybuty legalności oprogramowania, które towarzyszyły przy wejściu w jego posiadanie np. poprzez zakup;
   2) instrukcja użytkownika oprogramowania, zawierająca opis funkcjonalności użytkowych oprogramowania i sposobów ich wykorzystania;
   3) instrukcja administratora oprogramowania, zawierająca opis funkcjonalności administracyjnych oprogramowania i sposobów ich wykorzystania;
   4) opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposób przepływu danych pomiędzy poszczególnymi zbiorami danych, zwany dalej opisem struktur danych;
   5) dokumentacja konfiguracji systemu;
   6) procedura wykonywania kopii zapasowych danych oraz procedura odtwarzania danych z kopii zapasowych oraz rejestr wykonanych kopii zapasowych;
   7) schemat połączeń bloków funkcjonalnych systemu wraz z ich miejscem instalacji;
   8) wykaz podsieci zawierający, co najmniej opis funkcjonalny i adresację IP;
   9) wykaz dopuszczalnych połączeń z podsieciami spoza systemu informatycznego w kierunkach „z" i „do" danej podsieci, ze szczególnym uwzględnieniem połączeń dopuszczonych „z" i „do" sieci Internet;
   10) wykaz istotnych adresów IP z punktu widzenia działania systemu informatycznego np. bramy podsieci, serwery;
   11) ewidencja reguł urządzenia punktu styku z Internetem (np. firewall) wpuszczających ruch do sieci Urzędu.
2. Kompletność dokumentacji w zakresie elementów środowiska teleinformatycznego, w tym systemów informatycznych, infrastruktury teleinformatycznej, urządzeń komputerowych i zabezpieczeń zapewnia ASI, w szczególności dokumentacji wskazanej w ust. 1.
3. W sytuacjach wyjątkowych dopuszcza się powierzenie dokumentacji licencyjnej, wskazanej w ust. 1 pkt 1, wyznaczonym przez Dyrektora pracownikom, na zasadach odpowiedzialności materialnej.
4. Instrukcja użytkownika oprogramowania, wskazana w ust. 1 pkt 2, jest udostępniana wszystkim zainteresowanym użytkownikom.

5. Dokumentacja wskazana w ust. 1 pkt 3-11 może zawierać treści obniżające bezpieczeństwo systemu informatycznego i dostęp do niej powinien być ograniczony na zasadzie wiedzy koniecznej.

Rozdział 7

Zasady bezpiecznej współpracy ze stronami trzecimi

§ 18

1. ASI lub wyznaczony przez Dyrektora pracownik ma obowiązek sprawować nadzór nad realizacją zadań przez wykonawcę lub dostawcę.
2. Współpraca z podmiotami zewnętrznymi powinna być oparta na stosownej umowie zawierającej zapisy o poufności i jeśli to potrzebne, umowę powierzenia przetwarzania danych osobowych.
3. Przekazywanie informacji chronionych podmiotom zewnętrznym odbywa się zawsze za zgodą Dyrektora oraz tylko i wyłącznie mogą być przekazywane wyznaczonym do ich odbioru przedstawicielom dostawcy.
4. Przekazanie danych lub informacji musi mieć postać udokumentowaną.
5. Przekazanie danych lub informacji musi odbywać się kanałami powszechnie uznawanymi za bezpieczne, a zabezpieczenia muszą być adekwatne do kategorii przekazywanych danych lub informacji.

Rozdział 8

Zasady zarządzania incydentami bezpieczeństwa informacji

§ 19

O incydentach bezpieczeństwa ASI informuje IOD, który dokonuje ich rejestracji.

Rozdział 9

Zasady zapewnienia ciągłości działania

§ 20

1. Należy zapewnić gotowość techniczną i organizacyjną we wsparciu i realizacji kluczowych zadań, a w tym:
   1) stosować nadmiarowość w kluczowych miejscach infrastruktury technicznej i organizacji w celu wyeliminowania miejsc pojedynczych awarii, mogących skutkować zatrzymaniem kluczowego procesu;
   2) przygotowywać, uaktualniać i testować instrukcje awaryjne poszczególnych systemów teleinformatycznych;
   3) należy zapewnić możliwość uruchomienia i obsługi kluczowej infrastruktury na poziomie pozwalającym na realizację kluczowych zadań.

2. ASI jest zobowiązany poinformować Dyrektora o zagrożeniach mogących prowadzić do braku ciągłości działania.
3. ASI analizuje zagrożenia i zapewnia instrukcje awaryjne na wypadek potencjalnych incydentów, które w negatywny sposób wpłynie na kluczową infrastrukturę systemów placówki. Instrukcje te przekazuje Dyrektorowi.

DYREKTOR PRZEDSZKOLA
mgr Beata Jóźwowicz