

Sprawozdanie z zadania audytowego

Temat zadania audytowego	Ocena systemu kontroli zarządczej w zakresie bezpieczeństwa informacji.
Jednostka audytowana imię i nazwisko kierownika jednostki	Urząd Gminy Kozy 43-340 Kozy, ul. Krakowska 4 Krzysztof Fiałkowski – Wójt Gminy Kozy
Nr upoważnienia	OrS.077.31.2013
Cel zadania audytowego	Dostarczenie kierownikowi jednostki niezależnej i obiektywnej oceny dotyczącej bezpieczeństwa informacji poprzez weryfikację zgodności zabezpieczeń systemów informatycznych z wymogami określonymi przez przepisy prawa, mając na uwadze rosnącą wartość informacji oraz niebezpieczeństwo utraty informacji lub nieuprawnionego ujawnienia.
Przedmiotowy zakres zadania	Podstawowe założenia polityki bezpieczeństwa informacji Zarządzanie bezpieczeństwem informacji Klasyfikacja i kontrola aktywów Bezpieczeństwo osobowe Bezpieczeństwo fizyczne i osobowe Zarządzanie systemami informatycznymi Kontrola dostępu do systemu
Założenia organizacyjne	Planowany czas trwania audytu od 3.09.2013 – 1.10.2013 r. Czynności przeprowadzane będą w oparciu o udostępnianą dokumentację oraz realizację technik audytu. W toku prowadzonych badań należy dążyć, aby prowadzone zadanie nie dezorganizowało działalności badanego wydziału. Czynności przeprowadzane będą zgodnie ze standardami audytu, praktyką określoną w procedurach audytu i zakresem przedmiotowym zadania.
Termin przeprowadzenia audytu	3.09.2013 – 1.10.2013
Data sporządzenia sprawozdania	1 października 2013 r.

I. Tło informacyjne

Podstawą do przeprowadzenia audytu bezpieczeństwa informacji jest § 20 ust. 2 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. poz. 526), gdzie w określono zasady zarządzania bezpieczeństwem informacji, które realizowane jest w szczególności przez zapewnienie warunków umożliwiających realizację i egzekwowanie następujących działań:

1. zapewnienia aktualizacji regulacji wewnętrznych,
2. utrzymania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji,
3. przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji,
4. podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji,
5. bezzwłocznej zmiany uprawnień, w przypadku zmiany osób, o których mowa w pkt. 4,
6. zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień jak:
 - zagrożenia bezpieczeństwa informacji,
 - skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna,
 - stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich,
7. zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez:
 - monitorowanie dostępu do informacji,
 - czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji,
 - zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji,
8. ustanowienia podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość,
9. zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikację, usunięcie lub zniszczenie,
10. zawierania w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji,
11. ustalenia zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych,
12. zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na:
 - dbałości o aktualizację oprogramowania,
 - minimalizowaniu ryzyka utraty informacji w wyniku awarii,
 - ochronie przed błędami, utratą, nieuprawnioną modyfikacją,
 - zapewnieniu bezpieczeństwa plików systemowych,
 - redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych,
 - niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa,
 - kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa,
13. bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących,
14. zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.

II. Streszczenie

Celem audytu było dostarczenie kierownikowi jednostki niezależnej i obiektywnej oceny dotyczącej bezpieczeństwa informacji poprzez weryfikację zgodności zabezpieczeń systemów informatycznych z wymogami określonymi przez przepisy prawa, mając na uwadze rosnącą wartość informacji oraz niebezpieczeństwo utraty informacji lub nieuprawnionego ujawnienia.

Bezpieczeństwo informacji w Urzędzie Gminy Kozy jest zadaniem, na które należy zwracać szczególną uwagę. Jest to podyktowane nie tylko wymogiem ochrony informacji, ale także zabezpieczeniem nośników informacji i urządzeń, na których są zapisywane i przetwarzane. Wdrożenie zasad bezpieczeństwa odbywa się przy wykorzystaniu prawidłowo funkcjonującego systemu informatycznego oraz przy odpowiednim poziomie świadomości pracowników.

III. Ustalenie stanu faktycznego

W Urzędzie Gminy Kozy funkcjonuje wprowadzona Zarządzeniem Nr 73/2011 r. Wójta Gminy Kozy z dnia 29 sierpnia 2011 r. Polityka Bezpieczeństwa Informacji i ochrony danych Urzędu Gminy oraz Instrukcja zarządzania systemem informatycznym. Dokumentacja nie jest jednak wystarczająca, gdyż jej niewątpliwym elementem jest jej skuteczne wdrożenie oraz stosowanie. Dzięki przeprowadzonym szkoleniom, prawidłowej komunikacji oraz zarządzaniem incydentami budowana jest świadomość wszystkich pracowników, będąca podstawą skutecznego wdrożenia bezpieczeństwa informacji. Wśród głównych korzyści należy wymienić:

1. zwiększenie poziomu bezpieczeństwa informacji przetwarzanych w Urzędzie, co przekłada się na jakość zarządzania,
2. zapewnienie zgodności z wymaganiami prawnymi w obszarze bezpieczeństwa informacji,
3. zwiększenie świadomości pracowników, a tym samym budowę kultury organizacji i ładu,
4. systemowe podejście do tematu bezpieczeństwa, dzięki monitoringowi, ewaluacji i wdrażaniu zabezpieczeń w obszarze bezpieczeństwa informacji.

W Zarządzeniu nr 31/13 Wójta Gminy Kozy z dnia 27 marca 2013 r. w sprawie wprowadzenia Planu ochrony i zapewnienia ciągłości działania Urzędu Gminy Kozy określono zasady bezpieczeństwa fizycznego, w zakresie dozoru i zabezpieczenia obiektu oraz zarządzania kluczami.

W Urzędzie Gminy Kozy został przeprowadzony audyt weryfikujący stan zgodności z wymaganiami wynikającymi z obowiązujących przepisów z zakresu ochrony danych osobowych oraz bezpieczeństwa informacji.

W ramach zadania dokonano wybiórczego sprawdzenia stanowisk komputerowych. Ocena środowiska informatycznego polegała na zbadaniu stanu podstawowych zabezpieczeń stanowisk komputerowych w zakresie:

1. aktualizacji systemu operacyjnego,
2. stosowania właściwej polityki haseł przy pracy z komputerem,
3. zabezpieczenia antywirusowego,
4. zabezpieczenia komputerów,
5. legalności oprogramowania,
6. ochrony serwerów,
7. urządzeń aktywnych i sieci urzędu,
8. dostępu do sieci zewnętrznej,
9. okablowania strukturalnego.

W zakresie zgodności działania urzędu z przepisami o ochronie danych osobowych dokonano analizy i przeglądu:

1. dokumentowania sposobu zaznajamiania się z przepisami pracowników,
2. zasad postępowania z dokumentami zawierającymi dane osobowe,
3. stosowania procedur ochrony dokumentów.

Sprawdzono stan bezpieczeństwa fizycznego i środowiskowego w zakresie:

1. oceny zabezpieczenia wewnętrznego,
2. zasad dostępu pracowników do urzędu,

3. system identyfikowania urzędników,
4. system procedur ochrony przeciwwłamaniowej,
5. procedur działania na wypadek zagrożeń,
6. zabezpieczeń zewnętrznych budynku.

Wdrożona w Urzędzie Gminy Kozy Polityka Bezpieczeństwa Informacji odnosi się do zabezpieczenia danych osobowych zarówno do przetwarzanych tradycyjnie jak i danych przetwarzanych w systemach informatycznych. Wskazuje ona na działania jakie należy wykonać oraz ustanawia zbiór zasad i reguł postępowania, które należy stosować w Urzędzie Gminy Kozy. Określa ponadto praktyczne zasady zarządzania bezpieczeństwem informacji w obszarze technik informacyjnych oraz deklaruje zaangażowanie kierownictwa i wyznacza podejście do zarządzania bezpieczeństwem informacji.

Systemy informatyczne przetwarzające dane, w tym osobowe umieszczane są w kontrolowanych przez odpowiedzialnego za dany sprzęt pracownika. Pracownicy upoważnieni i zarazem odpowiedzialni za ochronę danych są zobowiązani do stosowania procedur wynikających z Polityki Bezpieczeństwa Informacji.

Dostęp użytkowników do systemu informatycznego jest kontrolowany za pomocą mechanizmów uwierzytelniania, autoryzacji i rozliczalności. Podstawą uwierzytelniania użytkownika jest wykorzystanie unikalnego identyfikatora i hasła. Autoryzacja użytkownika odbywa się na podstawie nadanych przez Administratora Bezpieczeństwa Informacji, a wprowadzonych przez Administratora Systemu Informacyjnego zakresu indywidualnych uprawnień.

System informatyczny przetwarzający dane, w tym osobowe, jest wyposażony w mechanizmy pozwalające w sposób jednoznaczny przypisać wykonanie określonych operacji użytkownikowi.

Wszelkiego rodzaju nośniki danych osobowych, które są przekazywane osobom lub podmiotom nieupoważnionym, pozbywa się danych lub też doprowadza do stanu uniemożliwiającego ich odczytanie.

Dane, w tym osobowe zabezpieczane są przez tworzenie kopii zapasowych i awaryjnych, jak również bezpieczne składowanie nośników kopii i ich udostępnianie. Nośniki danych, w tym kopie zapasowe przechowywane są w sposób zapewniający odpowiednią ochronę przed dostępem do nich osób niepowołanych oraz przed celowym lub przypadkowym zniszczeniem. W przypadku wystąpienia naruszenia bezpieczeństwa danych, w tym także danych osobowych istnieje procedura wprowadzenia zabezpieczeń redukujących ryzyko wystąpienia w przyszłości podobnego incydentu. Pracownicy, którzy zauważą naruszenie bezpieczeństwa informacji są zobowiązani do natychmiastowego powiadomienia ABI lub ASI.

W Urzędzie Gminy Kozy prowadzone są na bieżąco działania mające na celu zabezpieczenie systemu informatycznego przetwarzającego dane, w tym osobowe, przed zainfekowaniem wirusami lub innymi niebezpiecznymi kodami, a także podejmuje się działania zmierzające do usunięcia ich skutków w przypadku ich wystąpienia.

Pracownicy Urzędu Gminy Kozy korzystający z systemu informatycznego są zobowiązani do stosowania szczególnych zaleceń w zakresie ochrony antywirusowej, a także do wydawanych przedmiotowych zaleceń. System informatyczny wyposażony jest w techniczne i organizacyjne mechanizmy zabezpieczające przed możliwością wystąpienia krytycznych, z punktu widzenia ciągłości działania Urzędu Gminy Kozy, procesów związanych z przetwarzaniem danych.

Wszyscy pracownicy mający dostęp do systemu informatycznego przetwarzającego dane osobowe są poddawani przeszkoleniu obejmującemu zapoznanie się z obowiązującymi przepisami w zakresie ochrony tych danych, jak również zasadami bezpiecznego ich przetwarzania. Przeszkolenie pracownika jest warunkiem koniecznym do dopuszczenia do korzystania z systemu informatycznego.

Polityka Bezpieczeństwa określa zasady bezpiecznej pracy w zakresie ochrony informacji oraz przyjmowania klientów:

- zasada czystego biurka – dokumenty papierowe i nośniki komputerowe, kiedy nie są używane przechowywane są w specjalnych segregatorach, teczkach, szafach, półkach, szczególnie poza godzinami pracy,
- pracownicy przechowują wszystkie dokumenty zgodnie z wymaganiami Klasyfikacji informacji,
- zasada czystego ekranu – w przypadku opuszczania stanowiska pracy należy zablokować stację roboczą, monitor ustawiony jest w taki sposób, by osoby postronne nie miały możliwości wglądu do przetwarzanych aktualnie informacji,
- wygaszacze ekranu na stacjach roboczych zostały ustawione na 10 minut,

- zasada odbioru wydruków z drukarki – wszelkie wydruki zawierające dane osobowe, informacje wrażliwe zabierane są natychmiast z drukarki po zakończeniu drukowania,
- zasada zamykania pomieszczeń – ostatni pracownik opuszczający pomieszczenie zobowiązany jest do zamknięcia okien oraz drzwi zewnętrznych na klucz, bezwzględnie zabrania się zostawiania klucza w zamku po zewnętrznej stronie drzwi,
- zasada poufności rozmów – w przypadku prowadzenia rozmów, w tym telefonicznych zarówno w siedzibie Urzędu jak i poza obszarem Urzędu należy zadbać, aby rozmowy nie były prowadzone w obecności osób nieupoważnionych do otrzymania informacji,
- zasada nadzorowania klienta – klienci przyjmowani są w pomieszczeniach pracy tylko i wyłącznie pod nadzorem pracowników Urzędu,
- pracownik opiekujący się osobą trzecią jest zobowiązany do nie pozostawiania jej bez nadzoru w przypadku, gdy istnieje możliwość spowodowania incydentu bezpieczeństwa.

Nie stwierdzono nieprawidłowości w zakresie bezpieczeństwa danych w systemach informatycznych, które są przetwarzane w sposób bezpieczny i gwarantują ciągłość pracy.

IV. Uwagi i wnioski

Na podstawie dokonanej analizy rekomenduje się wykonanie następujących działań:

Przeprowadzić niezapowiedzianą kontrolę wszystkich pomieszczeń w Urzędzie Gminy Kozy w zakresie stosowania polityki bezpieczeństwa informacji, której celem będzie niezależna i obiektywna ocena dotycząca przestrzegania przez pracowników jednostki wprowadzonej Zarządzeniem Nr 73/2011 Wójta Gminy Kozy z dnia 29 sierpnia 2011 r. Polityki Bezpieczeństwa Informacji i ochrony danych osobowych Urzędu Gminy Kozy.

W związku z powyższym rekomendacja ma charakter doradczy, powinna przyczynić się do doskonalenia działań w zakresie bezpieczeństwa informacji.

Należy stwierdzić, że na podstawie przeprowadzonego zadania badany obszar funkcjonuje prawidłowo.

V. Ustalenia końcowe

1. Sprawozdanie sporządzono w dniu 1 października 2013 r. w 2 egzemplarzach.
2. Kierownikowi jednostki przysługuje prawo zgłoszenia na piśmie w terminie 7 dni od otrzymania sprawozdania dodatkowych wyjaśnień lub umotywowanych zastrzeżeń do ustaleń stanu faktycznego, analizy przyczyn i skutków stwierdzonych uchybień oraz uwag i wniosków zawartych w sprawozdaniu.
3. Brak odpowiedzi w podanym terminie oznacza zgodę ze wszystkimi ustaleniami zawartymi w sprawozdaniu, co skutkuje jego zatwierdzeniem i uznaniem za ostateczną wersję sprawozdania.
4. Na podstawie sprawozdania z przeprowadzonego zadania audytowego kierownik jednostki podejmuje działania mające na celu usunięcie uchybień i usprawnienie funkcjonowania jednostki.

Zadanie zostało przeprowadzone zgodnie z Komunikatem Nr 2 Ministra Finansów z dnia 17 czerwca 2013 r. w sprawie standardów audytu wewnętrznego w jednostkach sektora finansów publicznych (Dz. Urz. MF z dnia 24 czerwca 2013 r., poz. 15) oraz Księgą procedur audytu wewnętrznego.