SPRAWOZDANIE Z AUDYTU WEWNĘTRZNEGO

TEMAT ZADANIA	Audyt bezpieczeństwa informacji, zgodnie z wymogiem § 20 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.2012.526)
IMIĘ I NAZWISKO AUDYTORA PRZEPROWADZAJĄCEGO AUDYT	Aneta Krawczyk, audytor wewnętrzny
NR UPOWAŻNIENIA	AK.077.3.2014
CEL AUDYTU	Zadanie to ma charakter zadania zapewniającego, którego celem jest dostarczenie Zarządowi Powiatu Płońskiego niezależnej i obiektywnej oceny działania badanego obszaru oraz wykazanie, że kontrola zarządcza w badanym obszarze funkcjonuje prawidłowo lub wymaga wzmocnienia.
PODMIOTOWY I PRZEDMIOTOWY ZAKRES AUDYTU	Audytowi poddano działanie Powiatowego Urzędu Pracy w Płońsku (dalej „*PUP*") w zakresie bezpieczeństwa informacji przetwarzanej w systemie teleinformatycznym. Przedmiotem audytu było sprawdzenie realizacji obowiązków wynikających z § 20 ust. 1 i 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.2012.526).
PODJĘTE CZYNNOŚCI I ZASTOSOWANE TECHNIKI	Stosowane podczas audytu narzędzia i techniki to testy przeglądowe, zgodności, kontroli i rzeczywiste oraz przegląd dokumentacji, a także wywiady z pracownikami jednostki audytowanej.
OPIS DZIAŁAŃ JEDNOSTKI W BADANYM OBSZARZE	PUP posiada system teleinformatyczny w rozumieniu ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. - Dz.U. z 2013 r., poz. 235), czyli zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu przepisów ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne. Jednostka gromadzi i przetwarza w systemie teleinformatycznym informacje będące informacją publiczną w rozumieniu ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej. Część informacji jest publikowana w serwisie Biuletyn Informacji Publicznej i na stronach internetowych pupplonsk.org.pl. Szczególnym zasadom ochrony podlegają informacje zawierające dane osobowe – zgodnie z wymogami ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. Rozporządzenie do ww. ustawy szczegółowo reguluje kwestię systemów informatycznych, w których przetwarzane są dane osobowe.
TERMIN AUDYTU	17.10.2014 r. – 05.12.2014 r.
DATA SPORZĄDZENIA SPRAWOZDANIA	05.12.2014 r. r.

1. STRESZCZENIE

W trakcie audytu stwierdzono, że jednostka jako podmiot realizujący zadania publiczne ustanowiła system zarządzania bezpieczeństwem informacji i zapewnia poufność, dostępność i integralność informacji przetwarzanych w systemie teleinformatycznym z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność – zgodnie z wymogami § 20 ust. 1 i 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.2012.526).

W trakcie audytu stwierdzono jednak uchybienia w zakresie 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 oraz utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację.

2. USTALENIA STANU FAKTYCZNEGO ZE SKLASYFIKOWANYMI WYNIKAMI OCENY WEDŁUG KRYTERIÓW OCENY STANU FAKTYCZNEGO.

Zgodnie z § 20 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.2012.526) zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie następujących działań:

1) zapewnienia aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia;
2) utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację;
3) przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy;
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 zadań osób, o których mowa w pkt 4);
6) zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak:
   a) zagrożenia bezpieczeństwa informacji,
   b) skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna,
   c) 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:
   a) monitorowanie dostępu do informacji,
   b) czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji,
   c) 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 (nie dotyczy PUP w Płońsku);
9) zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, 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:
   a) dbałości o aktualizację oprogramowania,
   b) minimalizowaniu ryzyka utraty informacji w wyniku awarii,
   c) ochronie przed błędami, utratą, nieuprawnioną modyfikacją,
   d) stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa,
   e) zapewnieniu bezpieczeństwa plików systemowych,
   f) redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych,
   g) niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa,
   h) 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.

Powyższe działania mają na celu zapewnienie, że podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.

Wymagania te uznaje się również za spełnione, jeżeli system zarządzania bezpieczeństwem informacji został opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001, a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie Polskich Norm związanych z tą normą, w tym:
   1) PN-ISO/IEC 17799 – w odniesieniu do ustanawiania zabezpieczeń;
   2) PN-ISO/IEC 27005 – w odniesieniu do zarządzania ryzykiem;
   3) PN-ISO/IEC 24762 – w odniesieniu do odtwarzania techniki informatycznej po katastrofie w ramach zarządzania ciągłością działania.

Niezależnie od zapewnienia działań, o których mowa powyżej, w przypadkach uzasadnionych analizą ryzyka w systemach teleinformatycznych podmiotów realizujących zadania publiczne należy ustanowić dodatkowe zabezpieczenia.

Kierownictwo jednostki nie podejmowało decyzji o wdrażaniu ww. norm, zatem kryterium oceny stanu faktycznego w niniejszym audycie stanowiły przepisy z § 20 ust. 1 i 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.2012.526).

Podczas audytu dokonano kategoryzacji informacji pozostającej w zasobach PUP w Płońsku, przetwarzanych w systemie teleinformatycznym. Wymogi przepisów prawa w zakresie różnych kategorii informacji gromadzonych i przetwarzanych w systemie teleinformatycznym nakładają na różne obowiązki związane z funkcjonowaniem i zabezpieczeniami takiego systemu. I tak zidentyfikowano:

1) informację stanowiącą informację publiczną, do której dostęp należy zapewnić poprzez publikację informacji w urzędowym publikatorze teleinformatycznym na stronie podmiotowej Biuletynu Informacji Publicznej; wymagania dotyczące BIP określone są w ustawie o dostępie do informacji publicznej i rozporządzeniu MSWiA dnia 18 stycznia 2007 r. w sprawie Biuletynu Informacji Publicznej (Dz. U. Nr 10, poz. 68).
2) informację stanowiącą informację publiczną, nie publikowaną w BIP i udostępnianą na wniosek, przetwarzaną w systemie teleinformatycznym; w tym zakresie przepisy prawa nie regulują szczególnych wymogów dla systemów teleinformatycznych;

3) informację, która nie jest informacją publiczną - w tym zakresie przepisy prawa nie regulują szczególnych wymogów dla systemów teleinformatycznych;
4) informację zawierającą podlegające ochronie dane osobowe; system teleinformatyczny powinien spełniać wymogi określone w ustawie o ochronie danych osobowych i rozporządzeniu wykonawczym do tej ustawy.

2.1. Zapewnienie aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia.

Podczas audytu zidentyfikowano następujące regulacje wewnętrzne zawierające unormowania w zakresie zapewnienia bezpieczeństwa informacji w systemie teleinformatycznym jednostki:

1) Zarządzenie nr 27/2014 Dyrektora PUP z dnia 1 października 2014 r. w sprawie wprowadzenia systemu zarządzania bezpieczeństwem informacji. Według zarządzenia na system ten składa się przestrzeganie regulacji jednostki zawierających dane osobowe, prowadzenie aktualności inwentaryzacji sprzętu, analiza ryzyka, szkolenia, zapewnienie fizycznego bezpieczeństwa, współpraca pracowników z administratorem bezpieczeństwa informacji oraz coroczna weryfikacja systemu.
2) Regulamin organizacyjny jednostki przyjęty uchwałą nr 780/2014 Zarządu Powiatu Płońskiego z dnia 10 września 2014 r., w którym nie zamieszczano kompleksowych regulacji w tym zakresie. Zawarto natomiast postanowienia dotyczące rozdziału kompetencji w tym obszarze. Regulamin określa, że do zadań dyrektora jednostki należy zapewnie funkcjonowania adekwatnej, skutecznej i efektywnej kontroli zarządczej oraz koordynacja zadań z zakresu obsługi informatycznej urzędu. Do zadań zastępcy dyrektora należy nadzór nad gromadzeniem, przetwarzaniem i stosowaniem procedur udostępniania informacji o bezrobotnych, poszukujących pracy i cudzoziemcach zmierzających wykonywać lub wykonujących pracę na terytorium RP. Do obszaru odpowiedzialności głównego księgowego włączono organizację i nadzorowanie gromadzenia i przechowywania dokumentacji księgowej w sposób zabezpieczający ją przed dostępem osób nieuprawnionych, zaginięciem lub zniszczeniem. Wydział Organizacyjno-Administracyjny jest odpowiedzialny za nadzór nad bezpieczeństwem systemów teleinformatycznych PUP w szczególności przestrzeganie zasad i procedur określonych w polityce bezpieczeństwa informacji, administrowanie i utrzymanie portalu internetowego w tym biuletynu informacji publicznej, obsługa spraw związanych z „e-urzędem".
3) Zarządzenie nr 26/2014 Dyrektora PUP z dnia 1 października 2014 r. w sprawie wprowadzenia regulacji w obszarze zarządzania i zabezpieczenia systemu informatycznego. Na instrukcję składają się: polityka bezpieczeństwa, instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, instrukcję postępowania w sytuacji naruszenia ochrony danych osobowych. Polityka bezpieczeństwa zawiera wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe, wykaz zbiorów danych osobowych przetwarzanych elektroniczne wraz ze wskazaniem programów zastosowanych do ich przetwarzania, sposób przepływu danych pomiędzy poszczególnymi systemami, środki techniczne i organizacyjne niezbędne do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych, opis rejestracji baz danych. Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych zawiera procedury nadawania uprawnień, metody i techniki uwierzytelniania oraz procedury związane z zarządzaniem użytkowaniem, procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu, procedury tworzenia kopii zapasowych, sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe, w tym kopii zapasowych, sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu, procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych, sposób postępowania w zakresie komunikacji sieci komputerowej, zasady korzystania z komputerów przenośnych w zakresie przetwarzania danych osobowych, kontrola nad wprowadzeniem,

dalszym przetwarzaniem i udostępnianiem danych osobowych, procedury korzystania ze sprzętu i oprogramowania komputerowego, procedury korzystania z Internetu i poczty elektronicznej. Instrukcja zawiera również stosowane w jednostce wzory upoważnień i oświadczeń. Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych opisuje tryb zgłaszania incydentów naruszenia bezpieczeństwa informacji zawierającej dane osobowe.

Na podstawie analizy ww. regulacji wewnętrznych stwierdzono, że są one aktualne i zmieniane w miarę potrzeb, stosownie do zmian zachodzących w otoczeniu audytowanej jednostki.

2.2. Utrzymywanie aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację.

Do audytu przedstawiono „*wykaz sprzętu komputerowego – jednostka centralna, monitor*", w którym zaewidencjonowano 135 komputerów, monitorów i zestawów komputerowych, „*wykaz maszyn biurowych – drukarka, urządzenie wielofunkcyjne, skaner*", w którym zarejestrowano 49 sztuk pozostałego sprzętu. Ewidencja zawiera zestawienie nazwy sprzętu i numeru inwentarzowego.
Ponadto informatyk urzędu prowadzi dla każdego zestawu komputerowego metrykę komputera zawierającą:
- numer inwentarzowy,
- imię i nazwisko głównego użytkownika,
- nazwę i lokalizację komputera,
- określenie systemu operacyjnego,
- wyszczególnienie oprogramowania zainstalowanego na danym komputerze oprogramowania z uwzględnieniem producenta, nazwy produktu oraz licencji.

Aktualność metryk podpisuje informatyk urzędu.

W trakcie audytu sprawdzono na losowo wybranej próbie 20 komputerów aktualność ww. metryk. Stwierdzono, że:
- nr inwentarzowy ŚT-4-49-491/107: brak informacji o zainstalowaniu programów Ashampoo, Java, G-Data, DVD Maker;
- nr inwentarzowy ŚT-4-49-491/111: brak informacji o zainstalowaniu programów Ashampoo, Java, DVD Maker;
- nr inwentarzowy ŚT-IV-491/104: brak informacji o zainstalowaniu programów Cyberlink, Java, PDF Complete, Skype, Wild Tangent Games, DVD Maker, WinZip;
- nr inwentarzowy Dz.VIB.k30 poz. 366: brak informacji o zainstalowaniu DVD Maker, Java;
- nr inwentarzowy ŚT-IV-491/67: brak informacji o zainstalowaniu DVD Maker, Java, 7-Zip, PDF Complete, Roxio, Unizeto.
- nr inwentarzowy ŚT-IV-491/67: brak informacji o zainstalowaniu DVD Maker, Java, 7-Zip, PDF Complete, Roxio, Unizeto.
- nr inwentarzowy ŚT-IV-491/74: brak informacji o zainstalowaniu DVD Maker, Java, PDF Complete.
- nr inwentarzowy Dz. VIBk 300p 350 (komputer): brak informacji o zainstalowaniu 7-Zip, DVD Maker, Java.
- nr inwentarzowy ŚT-4-49-491/113: brak informacji o zainstalowaniu Ashampoo, Unizeto, DVD Maker.
- nr inwentarzowy ŚT-4-49-491/119: brak informacji o zainstalowaniu DVD Maker, Ashampoo, Java.
- nr inwentarzowy ŚT-4-491/115: brak informacji o zainstalowaniu Ashampoo, G-Data, Java, DVD Maker.
- nr inwentarzowy Dz.VIBk30p.373: brak informacji o zainstalowaniu DVD Maker, Java.
- nr inwentarzowy Dz.VIB k30p330 (komputer): brak informacji o zainstalowaniu Unizeto oraz informacja o zainstalowaniu SOETO, którego nie ma na tym komputerze.
- nr inwentarzowy ŚT-IV-491/99 (komputer dyrektora jednostki): brak metryki komputera, którą uzupełniono podczas audytu, w uzupełnionej metryce brak jest informacji o zainstalowanych programach Unizeto, Java, Okoszefa.

- nr inwentarzowy ŚT-IV-491/79 (laptop informatyka): brak metryki komputera, w trakcie audytu uzupełniono metrykę.
- nr inwentarzowy Dz.VIBk30p287 (komputer), Dz.VIBk30p.302 (komputer), ŚT-IV-491/58, Dz.VIB.k30p.263, Dz.VIBk30p285, Dz.VIBk30p.259: brak metryki komputera. Zgodnie z wyjaśnieniami informatyka, sprzęt ten jest wycofany z użytku i obecnie nie jest na wyposażeniu żadnego z pracowników.

Powyższe dostarcza dowodów dotyczących konieczności dołożenia należytej staranności w zakresie ewidencji sprzętu i oprogramowania.

2.3. Przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy.

Procedura analizy ryzyka w Powiecie Płońskim wprowadzona została Zarządzeniem nr 44/2012 Starosty Płońskiego z dnia 22 października 2012 r. w sprawie ustalenia procedur kontroli zarządczej w Starostwie Powiatowym w Płońsku i jednostkach organizacyjnych powiatu. Polityka zarządzania ryzykiem w powiecie płońskim stanowi załącznik nr 2 do zarządzenia. Polityka reguluje: odpowiedzialność za zarządzanie ryzykiem; procedurę corocznej identyfikacji ryzyka; bieżące zarządzanie ryzykiem oraz dokumentowanie procesu zarządzania ryzykiem. Polityka określa coroczną identyfikację i analizę ryzyka, z której wynika jednostki organizacyjne są zobowiązane do przeprowadzenia udokumentowanej identyfikacji i analizy ryzyka w drugim półroczu każdego roku kalendarzowego, według zasad określonych w tej polityce. Jednostki wypełniają rejestr ryzyk według wzoru stanowiącego załącznik nr 1 do polityki. W PUP zidentyfikowano10 najważniejszych ryzyk w odniesieniu do celów jednostki. Zidentyfikowane ryzyka umieszczono się w rejestrze i dokonano ich wyceny. Dla dziesięciu ryzyk, dla których istotność ryzyka nieodłącznego jest największa w powiecie sporządzane są szczegółowe programy zarządzania ryzykiem, zgodnie z wzorem karty indywidualnego ryzyka.

W rejestrze ryzyk na 2013 rok zidentyfikowano dziesięć ryzyk i dokonano ich wycen: ryzyka nieodłącznego i rezydualnego. Dla ryzyka nr 3 opisanego jako „*awarie systemów informatycznych i utrata danych*", dla którego poziom ryzyka nieodłącznego ustalono jako średni, sporządzono Kartę Indywidualnego Ryzyka z terminami wdrożenia planowanych działań. W celu wdrożenia i funkcjonowania mechanizmów kontrolnych zaplanowano następujące działania:
a) szkolenia użytkowników z zakresu ochrony danych osobowych, ABI przeprowadza czynności kontrolno-szkoleniowe wybranych użytkowników danych osobowych. W przypadku zaistnienia potrzeby (np. zmian przepisów, sugestii kierowników działów, itp.) zlecane jest szkolenie dla pracowników jednostkom zewnętrznym. Zaplanowano to jako działanie ciągłe a odpowiedzialnymi zostali pan Piotr Pokrzywnicki (ABI) oraz Pani Monika Zabłocka (Kierownik Wydziału Organizacyjno-Prawnego);
b) chroniony dostęp do komputerów i serwerowni (zabezpieczenia fizyczne), wykonywanie kopii zapasowych, firewall, program antywirusowy, system bezpieczeństwa informatycznego FortiGate, bieżący nadzór informatyka, utrzymanie dokumentacji w formie papierowej. Odpowiedzialni za to są kierownicy działów i informatyk;
c) Aktualizacja procedur, zaplanowana na styczeń 2014 r. oraz na bieżąco w miarę potrzeb, wyznaczono do tego Panią Monikę Zabłocką.

Podczas audytu stwierdzono podjęcie wszystkich zaplanowanych działań. W obu przypadkach poziom ryzyka rezydualnego po zastosowaniu zaplanowanych mechanizmów kontrolnych określono jako „niski".

2.4. Podejmowanie 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. Zmiana uprawnień.

Administratorem bezpieczeństwa informacji w zakresie ochrony danych osobowych jest Pan Piotr Pokrzywnicki powołany na to stanowisko w dni 12 kwietnia 1999 r. zarządzeniem nr 3/99 Kierownika PUP w Płońsku. Pracownicy posiadający dostęp do danych osobowych mają wystawione stosowne upoważnienia, zgodnie z art. 37 ustawy o ochronie danych osobowych i podpisali oświadczenia, zgodne z przyjętą w jednostce procedurą.

Do audytu przedstawiono ewidencję osób na dzień 23.10.2014 r. uprawnionych do pracy w systemie oraz raport użytkowników wygenerowany przez system *Syriusz* z informacją o ograniczeniach uprawnień do poszczególnych modułów systemu.

Stwierdzono nieaktualne zakresy czynności w kwestii dotyczącej dostępu do modułów systemu informatycznego - w zakresie czynności wskazanie, że pracownik może przetwarzać dane w szczególności w FOB, a ma on również dostęp do innych modułów – np. p. Monika Gajewska; Bartosiewicz Bożena; Monika Zabłocka, poza tym w zakresach czynności są nazwy (skróty modułów z poprzedniego, nieobowiązującego już systemu informatycznego choć skróty podobne do aktualnych Nieaktualne nazwy modułów w zakresie czynności – Węgier Michał (pośrednik pracy) – Grodkiewicz Edyta (pośrednik pracy) - wskazywany jest w zakresie moduł (np. formalna obsługa osób, lub prace okresowe i staże – dotyczy to poprzedniego systemu); Walter-Jakubiak Anita (specjalista do spraw rozwoju zawodowego) - wskazywany jest w zakresie moduł (np. formalna obsługa osób, świadczenia finansowe, prace okresowe i staże, pośrednictwo pracy, szkolenia i poradnictwo zawodowe – dotyczy to poprzedniego systemu).

Pojawiły się rozbieżność pomiędzy stanowiskiem w zakresie czynności a stanowiskiem na wydruku z systemu informatycznego – np.

- p. Monika Gajewska; W zakresie czynności pracownik ma p.o. kierownika działu usług rynku pracy, a na wydruku z Syriusza stanowisko Kierownik Wydziału;
- p. Frąckiewicz Grażyna - w zakresie czynności pracownik ma stanowisko: kierownik Wydziału Instrumentów Rynku Pracy, a na wydruku z *Syriusza* stanowisko Zastępca Kierownika Wydziału;
- p. Koniec Iwona; w zakresie czynności pracownik ma stanowisko: zastępca kierownika Działu Instrumentów Rynku Pracy, a na wydruku z *Syriusza* stanowisko Inspektor;
- p. Magdalena Kędzik - W angażu pracownik ma stanowisko: pomoc administracyjna, a na wydruku z systemu *Syriusz* stanowisko kancelista;
- p. Magdalena Szcześniak - Stanowisko w zakresie czynności - pomoc administracyjna, a w wykazie podinspektor.

W zakresie wyznaczonych zastępstw stwierdzono, że Pani Braun Renata (specjalista ds. rozwoju zawodowego) ma dostęp do modułów UiRP i WK, a zastępuje p. Walter-Jakubiak Anitę, która ma dostęp do czterech modułów: poza w/w jeszcze FOB i IFA.

Ponadto:

- Pan Dariusz Grzelak (pośrednik pracy) - osoba zastępująca, tj. p. Wierzejski nie jest pracownikiem PUP;
- Pani Hanna Bombała (starszy inspektor) - Osoba zastępująca – nie ma takiej osoby w wydziale; Najprawdopodobniej nie ma takiego pracownika;
- Pani Ziółkowska Marzena (doradca zawodowy) - osoba zastępująca tego pracownika, tj. p. Łukasz Brzostek od dn. 01.06.2014 r. jest zatrudniony na stanowisku inspektora ds. kadr.
- Pani Anna Markowska (pośrednik pracy) - osoba zastępująca tego pracownika nie jest pośrednikiem pracy, a specjalistą ds. rozwoju zawodowego (jej zakres czynności w głównej mierze dotyczy szkoleń);
- Pan Marcin Gortat (pośrednik pracy) - osoba zastępująca nie jest pośrednikiem pracy, a specjalistą ds. rozwoju zawodowego (jej zakres czynności w głównej mierze dotyczy szkoleń).

W jednostce nie ma procedury unieważniania anulowanych upoważnień (np. przekreślenie i opis: anulowano, lub w inny widoczny sposób; na upoważnieniach nieaktualnych nie stwierdzono śladów potwierdzających, że zostały one anulowane oraz wskazania daty ich anulowania.

W rejestrze co do zasady widnieją daty odebrania uprawnień wynikających z jednego upoważnienia i nadania (nawet tych samych uprawnień) w oparciu o inne upoważnienie, ale stwierdzono, iż:

- dla pracownika: Bogucka Sylwia (doradca zawodowy) – z rejestru wynika, iż pracownikowi dwukrotnie przyznano uprawnienia do tych samych modułów w 2011 i 2014 r.; (w rejestrze nie wskazano daty odebrania uprawnień wynikających z upoważnienia 129, a wprowadzono uprawnienia w oparciu o upoważnienie nr 203);
- dla pracownika Załęcka Jolanta (stanowisko w zakresie czynności - pomoc administracyjna, a w wykazie podinspektor) – znów na wykazie nie wskazano daty wygaśnięcia upoważnienia 130 –dwa razy przyznano uprawnienie do FOB – upoważnienie 130 i 182.

Z informacji udzielonych przez informatyka wynika, iż przy każdej zmianie danych (np. zmiana stanowiska, zmiana nazwiska pracownika, itp.) powinno być sporządzane nowe upoważnienie do dostępu do systemu informatycznego. Jednak w poniższych przypadkach stwierdzono:

- Pani Markowska Anna - była zmiana nazwiska i stanowiska a aktualne upoważnienie pochodzi z 2011 r.
- Pan Barczak - stażysta obecnie zatrudniony jako pracownik – nie było zmiany upoważnienia.

Stwierdzono przypadki niedostosowania praw dostępu w systemie do zadań wynikających z zakresów czynności np.

- Pani Koniec Iwona (inspektor) - współdziałanie z Głównym Księgowym w zakresie opracowywania projektów planów finansowych i planowania wydatków FP i innych funduszy celowych i sprawozdawczości (p.8); w związku z p.8 powinien być możliwy dostęp do modułu *MF - Syriusz - Monitoring Finansowy*, na to wskazuje zakres czynności, choć aktualnie zajmowane stanowisko (wg danych w *Syriuszu* to inspektor);
- Pani Piotrowska Joanna (inspektor) - ocena efektywności staży (wskaźniki efektywności), w tym sporządzanie sprawozdań o rynku pracy MPiPS, ustalenie stopy ponownego zatrudnienia, ustalenie kosztu ponownego zatrudnienia (p.3); zwrot kosztów dojazdu do pracy, na staż, w tym przyjmowanie wniosków o zwrot poniesionych kosztów, przyjmowanie rozliczeń o zwrot kosztów, naliczanie i przygotowanie list wypłat, tworzenie raportów w zakresie przyznania zwrotu kosztów dojazdu do pracy i na staż,

monitoring finansowo-rzeczowy dot. zwrotu kosztów dojazdu do pracy i na staż (p.4); zachodzi wątpliwość, czy w związku np. z p.3 i 4 nie powinien być możliwy dostęp do modułu *MF - Syriusz - Monitoring Finansowy i/lub moduł FK.*

- Pani Fibrant Aneta (doradca zawodowy) - pracownik nie posiada przyznanych uprawnień w systemie, zakres jego czynności nie różni się od zakresów p. Bandurskiej i p. Sobolewskiej, które mają dostęp do *Syriusz - Formalna Obsługa Beneficjenta i Syriusz - Usługi i Instrumenty Rynku Pracy*;
- Pan Brzostek Łukasz (inspektor) – pracownik ma dostęp do FOB, w zakresie czynności brak zadań wymagających takiego dostępu, ponieważ obsługuje kadry.
- Pani Draganiak Iwona (podinspektor) - pracownik ma dostęp do FOB, w zakresie czynności brak zadań wymagających takiego dostępu.

Jeśli chodzi o system informatyczny to stwierdzono, że:

- nie ma możliwości odczytania w systemie informatycznym *Syriusz* dat nadania i odebrania upoważnień do poszczególnych modułów lub historii zmian nadawanych uprawnień pracownikom – informacja potwierdzona przez informatyka (mail z dn. 18.11.2014 r.) – brak możliwości zweryfikowania w systemie, kiedy faktycznie nadano/odebrano upoważnienia konkretnym osobom;
- ewidencja prowadzona ręcznie w arkuszu MS Excel zawiera błędy – (sprostowanie dotyczące błędnej ewidencji uprawnień p. Katarzyny Tuwalskiej -mail z dn. 12.11.2014 r.); inne – wydruk ewidencji osób uprawnionych do pracy w systemie na dn. 23.10.2014 r. – s. 6, Lp. 170, data nadania uprawnienia: 08.20.2014; s. 4, Lp. 115 i 16 – błędy w imieniu i nazwisku;
- nie ma możliwości wydruku raportu z systemu wszystkich możliwych uprawnień w poszczególnych modułach, raport generuje wyłącznie informacje o tym, do jakich elementów w module użytkownik nie ma dostępu.

2.5. Zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji.

Sprawdzono prowadzenie szkoleń dla pracowników jednostki. Poddano analizie certyfikaty z odbytych szkoleń przez pracowników:

Pan Piotr Pokrzywnicki, informatyk, administrator bezpieczeństwa informacji

- czerwiec 2014 r. – Zarządzanie i konfiguracja sieci z wykorzystaniem urządzeń rodziny Fortinet
- luty 2014 r. – System analityczno-raportowy CeSAR
- grudzień 2013 r. – szkolenie merytoryczne kadry IT zatrudnionych w strukturach informatycznych służb zatrudnienia
- luty 2013 r. – budowa e-formularzy w ePUAP – praktyczne warsztaty komputerowe
- listopad 2012 r. kurs Novell

Pani Aneta Pomoryn:

- wrzesień 2013 r. - Zasady ochrony danych osobowych przetwarzanych w projektach PO KL

Pani Joanna Piotrowska, Pani Magdalena Szcześniak, Pani Marzena Ziółkowska, Pani Danuta Kocięda, Pan Łukasz Brzostek, Pani Krystyna Rutkowska, Pani Monika Gajewska, Pani Magdalena Koper, pani Magdalena Kosińska, Pani Renata Braun, Pani Marlena Kruszewska, pani Anna Żebrowska, Pan Michał Węgier, Pani Magdalena Sobczyńska, pani Grażyna Frąckiewicz, pani Krystyna Ciska, :

- październik 2012 r. – ochrona danych w PSZ z uwzględnieniem nowelizacji.

2.6. Zapewnienie ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami. Zabezpieczenia fizyczne.

Jednostka posiada również zabezpieczenia systemu teleinformatycznego mające na celu:

a) monitorowanie dostępu do informacji,

b) czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji,

c) zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji;

Administrator systemu posiada systemowy podgląd zdarzeń, dokonuje się kontroli stosowania wprowadzonych zasad przez użytkowników. Ponadto, logowanie do systemu odbywa się z użyciem hasła. Po trzech próbach nieudanego logowania system jest blokowany i może być odblokowany jedynie przez administratora.

2.7. Zawieranie w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji.

Jednostka podpisała następujące umowy serwisowe, które sprawdzono pod kątem stosowania odpowiednich zapisów dotyczących ochrony informacji:

- Umowa w sprawie serwisowania, konserwacji oraz przeglądów urządzeń biurowych z dnia 2 stycznia 2014 r. pomiędzy PUP w Płońsku a firmą LCS z siedzibą w Płońsku. Umowa w par. 1 ust. 6 zawiera sformułowanie *„Wykonawca zobowiązuje się do zachowania w tajemnicy wszelkich informacji uzyskanych w związku z wykonywaniem umowy. Podjęte zobowiązanie pozostaje w moc w czasie trwania umowy i po jej zakończeniu."*
- Umowa w sprawie systemu samorządowa elektroniczna platforma informacyjna (SEPI) z dnia 07.10.2013 r. z Sygnity SA z siedzibą w Warszawie. Umowa zawiera zobowiązanie firmy do zapewnienia bezpieczeństwa w zakresie incydentów naruszenia bezpieczeństwa przez nieuprawnionych użytkowników. Podpisano również odrębną umowę dotyczącą przetwarzania danych osobowych.

Pozostałe czynności serwisowe są przypisane w zakresie czynności informatykowi jednostki.

2.8. Ustalenie zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych. Zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych.

Opisane w punkcie 2.1. ustalone zasady postępowania z informacjami i zapewniają minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych.

Wymogi zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych regulują następujące akty prawne:

- rozporządzenie 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.2012.526);
- rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024);

- rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 18 stycznia 2007 r. w sprawie Biuletynu Informacji Publicznej (Dz. U. Nr 10, poz. 68).

Zgodnie z pierwszym rozporządzeniem zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych odbywa się m.in. poprzez:

a) dbałość o aktualizację oprogramowania,
b) minimalizowanie ryzyka utraty informacji w wyniku awarii,
c) ochronę przed błędami, utratą, nieuprawnioną modyfikacją,
d) stosowanie mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa,
e) zapewnienie bezpieczeństwa plików systemowych,
f) redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych,
g) niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa,
h) kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa,

Nie stwierdzono uchybień w powyższym zakresie.

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych również formułuje wymagania względem systemu informatycznego, w którym przetwarzane są dane osobowe. Sposób użytkowania systemu reguluje opisywana już instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych wymaga przepisem par. 3 niniejszego rozporządzenia. W myśl par. 6 instrukcja zawiera wszystkie niezbędne elementy, tzn.:

- procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności;
- stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem;
- procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu;
- procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania;
- sposób, miejsce i okres przechowywania: elektronicznych nośników informacji zawierających dane osobowe, kopii zapasowych,
- sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania szkodliwego;
- procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

Określone zasady dla systemu teleinformatycznego spełniają wymogi ww. rozporządzenia.

Wymagania dotyczące podmiotowej strony Biuletynu Informacji Publicznej zawiera rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 18 stycznia 2007 r. w sprawie Biuletynu Informacji Publicznej (Dz. U. Nr 10, poz. 68). Strona BIP jest wyposażona w mechanizm dziennika, w którym odnotowywane są zmiany w treści informacji publicznych udostępnianych w BIP. Strona BIP zawiera rozwiązanie techniczne uniemożliwiające zniszczenie lub modyfikację informacji publicznych zawartych w BIP przez osoby nieuprawnione. Jednocześnie nie wprowadzano zabezpieczeń przed kopiowaniem i drukowaniem informacji zamieszczonych w Biuletynie. Formaty danych zapewniające dostęp do zasobów i protokoły komunikacyjne są zgodne z wymogami rozporządzenia.

2.9. Zgłaszanie incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących.

Jednostka opracowała procedury w powyższym zakresie. Załącznikiem nr 3 do zarządzenia Nr 26/2014 Dyrektora PUP w Płońsku z dnia 1 października 2014 r. jest instrukcja postępowania w przypadku naruszenia ochrony danych osobowych. Procedura zawiera postanowienia ogólne, opis trybu postępowania w sytuacji naruszenia ochrony danych osobowych, wzór protokołu z naruszenia ochrony danych osobowych.

Do zgłaszania incydentów został zobligowany każdy pracownik, który podejmie wiadomość lub stwierdzi naruszenie danych osobowych. Zobowiązano pracowników do natychmiastowego o tym bezpośredniego przełożonego, a w przypadku danych utrwalonych w zbiorach informatycznych – administratora bezpieczeństwa informacji. Regulacje te ustalają sposób postępowania z incydentami naruszenia ochrony danych osobowych.

2.10. Słabości kontroli zarządczej w odniesieniu do ustalonych kryteriów oceny stanu faktycznego, analiza przyczyn tych słabości oraz skutków i ryzyk wynikających ze wskazanych słabości.

Głównym kryterium oceny stanu faktycznego były przepisy:

- 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.2012.526);
- rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024);
- rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 18 stycznia 2007 r. w sprawie Biuletynu Informacji Publicznej (Dz. U. Nr 10, poz. 68).

Stwierdzono niezgodności w zakresie stosowania § 20 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany w obrębie:

- 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.
- utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację.

2.11. Zalecenia

2.11.1. Dołożyć należytej staranności przy podejmowaniu 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.

2.11.2. Utrzymywać aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację.

3. Opinia audytora w sprawie adekwatności, skuteczności i efektywności kontroli zarządczej w obszarze objętym audytem.

Audyt dostarcza zapewnienia, że w audytowanym obszarze ustanowiono adekwatne, skuteczne i efektywne mechanizmy kontroli zarządczej. PUP w Płońsku posiada wyczerpujące regulacje dotyczące ochrony informacji przetwarzanych w systemie teleinformatycznym.

PUP w Płońsku ustanowiło, wdrożyło, eksploatuje, monitoruje i dokonuje przeglądów oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji, z uwzględnieniem rodzajów przetwarzanych informacji i wymogów przepisów prawa w tym zakresie. Stwierdzono jednak uchybienia, które muszą być wyeliminowane poprzez wdrożenie zaleceń poaudytowych.

Starostwo Powiatowe
w Płońsku
Wydział Audytu i Kontroli
09-100 Płońsk, ul. Płocka 39

NACZELNIK
Wydziału Audytu i Kontroli
Aneta Krawczyk

Aneta Krawczyk