Załącznik nr 2
do Zarządzenia nr 358/2020
Burmistrza Miasta Kętrzyn
z dnia 30.11.2020

INSTRUKCJA ZARZĄDZANIA SYSTEMAMI INFORMATYCZNYMI W URZĘDZIE MIASTA KĘTRZYN

1. Wstęp

Instrukcja stanowi wykaz procedur oraz stosowanych środków technicznych i organizacyjnych mających na celu, zgodnie z Art. 32 RODO, zabezpieczyć przetwarzane dane osobowe przed: przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją danych osobowych, nieuprawnionym ujawnieniem danych osobowych oraz nieuprawnionym dostępem do danych osobowych.

2. Zabezpieczenia fizyczne

1. Budynek Urzędu Miasta Kętrzyn przy ul. Wojska Polskiego 11 posiada dwa wejścia, wyposażone w drzwi metalowe z przeszkleniami, z dwoma zamkami patentowymi.
2. Budynek Urzędu Miasta Kętrzyn przy Placu Marszałka Józefa Piłsudskiego 2 (Ratusz) posiada dwa wejścia, wyposażone w drzwi drewniane z dwoma zamkami patentowymi.
3. Wdrożono zasadę dostępu osób nieupoważnionych do miejsc przetwarzania danych wyłącznie w obecności osoby upoważnionej.
4. Urządzenia służące do przetwarzania danych osobowych znajdują się w pomieszczeniach biurowych – ograniczono dostęp osób nieupoważnionych. Wszystkie pomieszczenia biurowe, w których przetwarza się dane osobowe chronione są poprzez zastosowanie drzwi drewnianych z zamkami mechanicznymi.
5. Krytyczne elementy infrastruktury zabezpieczono w zamykanych na klucz pomieszczeniach serwerowni.
6. Rozdzielnie elektryczne zabezpieczono w szafach zamykanych na klucz.
7. Dostęp do serwerowni zabezpieczono drzwiami zamykanymi na klucz.
8. Dostęp do archiwum zabezpieczono drzwiami zamykanymi na klucz.
9. Dostęp do dokumentacji i danych w pomieszczeniach zabezpieczono w zamkniętych niemetalowych szafach, w szafach metalowych i w sejfach.
10. Stosowana jest polityka kluczy:
    a) klucze do wszystkich pomieszczeń budynku Urzędu Miasta Kętrzyn przy ul. Wojska Polskiego 11 są w posiadaniu pracowników, a klucze zapasowe przechowywane są w skrzynce w Straży Miejskiej,
    b) klucze do pomieszczeń budynku Urzędu Miasta Kętrzyn przy Placu Marszałka Józefa Piłsudskiego 2 są w posiadaniu pracowników, a klucze zapasowe przechowywane są w skrzynce w USC.
11. Szczegółowe zapisy polityki kluczy są zawarte w „Instrukcji postępowania z kluczami oraz zabezpieczenia pomieszczeń i obiektów Urzędu Miasta Kętrzyn".
12. Zapewniono ochronę obiektu - firma ochroniarska.
13. System alarmowy:

    lokalizacja:

    a) w budynkach Urzędu Miasta Kętrzyn został zamontowany system alarmowy obejmujący działaniem wszystkie pomieszczenia w budynku,
    b) sterowanie systemem w zakresie uzbrajania/rozbrajania zapewniają centralki systemu zlokalizowane w budynkach przy ul. Wojska Polskiego 11 i Placu Marszałka Józefa Piłsudskiego1,
    c) system alarmowy został zainstalowany i jest administrowany przez firmę: „STEKOP" S.A., 02-127 Warszawa, ul. Mołdawska 9 (Adres korespondencyjny: Kol. Porosły 52, 16-070 Choroszcz, tel. 85 748 90 15), Biuro Terenowe: 11-400 Kętrzyn, ul. Szkolna 1, tel. 89 751 24 57(osoba do kontaktu: Maciej Kosakowski, tel. 691 550 569.

    uprawnienia i autoryzacja:

    a) uprawnienia do uzbrajania/rozbrajania alarmu w pomieszczeniach budynku Urzędu Miasta Kętrzyn mają: Burmistrz, Zastępca Burmistrza, Skarbnik, Sekretarz oraz Sprzątaczki i Konserwator,

b) dostęp do systemu umożliwia klawiatura sterująca zlokalizowana przy drzwiach wejściowych.

konfiguracja:

a) w systemie wprowadzono ograniczenie czasowe w dostępie osób uprawnionych,
b) system przewiduje możliwość telefonicznego powiadamiania o sytuacji alarmowej; w sytuacji alarmowej informowana jest firma „STEKOP" S.A. – Biuro Terenowe, 11-400 Kętrzyn, ul. Szkolna 1, tel. 89 751 24 57 (osoba do kontaktu: Maciej Kosakowski, tel. 691 550 569).

14. W Gminie Miejskiej Kętrzyn jest zainstalowany system monitoringu.
15. Dostęp fizyczny do baz danych osobowych mają wyłącznie uprawnieni użytkownicy, oraz osoby sprzątające obiekt.

3. Zabezpieczenia sprzętowe

1. Do likwidacji zbędnych dokumentów papierowych zawierających dane osobowe zastosowano niszczarki o podwyższonej klasie niszczenia.
2. Systemy informatyczne przetwarzające dane osobowe są zainstalowane na komputerach przyłączonych do sieci LAN oraz na samodzielnych stanowiskach niepodłączonych do LAN.
3. Dostęp do komputerów przetwarzających dane osobowe jest chroniony poprzez hasła na systemie operacyjnym i hasła aplikacji.
4. Lokalna sieć komputerowa ma połączenie z siecią publiczną Internet w sposób zapewniający kontrolę przepływu danych pomiędzy LAN a Internetem. Dane są filtrowane za pomocą urządzenia Fortinet Fortigate 100D.
5. Dane w systemach są przetwarzane w sposób scentralizowany, nie występują rozproszone bazy danych.
6. Wszystkie komputery na których przetwarzane są dane osobowe są zabezpieczone przed utratą danych na skutek zaniku napięcia: komputery stacjonarne są podłączone do wydzielonej sieci pracującej pod kontrolą UPS-a, który znajduje się w pomieszczeniu serwerowni. UPS podtrzymuje pracę urządzeń w przypadku zaniku zasilania, laptopy posiadają własną baterię wewnętrzną.

4. Środki ochrony w ramach oprogramowania systemu:

1. Konfiguracja systemu umożliwia użytkownikom dostęp do danych osobowych tylko za pośrednictwem aplikacji; zabronione jest instalowanie narzędzi programowych umożliwiających dostęp do baz danych z pominięciem aplikacji.
2. Systemy operacyjne komputerów mają zdefiniowane prawa dostępu do zasobów systemu dla poszczególnych użytkowników oraz system ich autoryzacji poprzez identyfikatory i hasła.
3. Dostęp do systemów sieciowych jest chroniony poprzez system identyfikatorów i haseł użytkowników.
4. Zainstalowany program antywirusowy ESET Endpoint Antivirus posiada funkcje skanera zasobów dyskowych, monitora systemu, skanera poczty elektronicznej oraz funkcje, która umożliwia wykrywanie i blokowanie niepożądanych procesów w systemie (tzw. Heurystyka antywirusowa).
5. Systemy operacyjne są na bieżąco aktualizowane poprzez instalowanie Serwis Pack'ów i update'ów systemu - aktualizacje automatyczne.

5. Środki ochrony w ramach narzędzi baz danych i aplikacji:

1. W bazach danych i aplikacjach skonfigurowano identyfikatory i hasła uprawnionych użytkowników.
2. Użytkownicy mają nadane identyfikatory, hasła i prawa dostępu do aplikacji w stopniu zapewniającym właściwe wykonanie pracy i jednocześnie bezpieczeństwo przetwarzania danych.
3. Nie występuje udostępnianie danych osobowych w systemach informatycznych.

6. Procedura nadawania uprawnień do przetwarzania danych osobowych.

Celem procedury jest minimalizacja ryzyka przetwarzania danych przez osoby nieupoważnione.

1. Dostęp do systemu informatycznego (np. stacji roboczej, dysku sieciowego, programu lub aplikacji, poczty elektronicznej) nadawany jest każdemu użytkownikowi w formie indywidualnego identyfikatora (loginu).
2. Każdemu użytkownikowi uprzywilejowanemu (administratorowi) nadawane jest indywidualne konto administracyjne.

3. Nadawanie, zmiana, odbieranie uprawnień użytkownika do zasobów i aplikacji odbywa się na polecenie przełożonych (lub innych osób upoważnionych).
4. Za wykonanie czynności nadawania, zmiany, odbierania uprawnień użytkownikowi odpowiada informatyk.
5. Powyższą procedurę wykonuje się w oparciu o pisemny wniosek, w którym to wniosku zostaje zawarty profil uprawnień. Profil uprawnień powinien być zgodny z obowiązującym katalogiem profili uprawnień lub przyjętym zakresem obowiązków na danym stanowisku.
6. Wniosek o nadanie uprawnień może być przekazany drogą mailową.
7. Obowiązuje zasada minimalizacji uprawnień.
8. Identyfikator użytkownika po wyrejestrowaniu z systemu informatycznego nie może być przydzielany innej osobie.
9. Użytkowników obowiązuje zasada pracy na własnym koncie. Zabronione jest umożliwianie innym osobom pracy na koncie innego użytkownika. Zasada ta obowiązuje również administratorów systemów.
10. W przypadku pracy z uprawnieniami użytkownika uprzywilejowanego, każdy Administrator systemu zobowiązany jest do bieżącej pracy na koncie roboczym. Użycie tzw. konta administracyjnego (np. "root" lub "admin") dopuszczalne jest jedynie w sytuacjach awaryjnych lub podczas poważnych zmian wprowadzanych w administrowanym systemie.

7. Metody i środki uwierzytelnienia (polityka haseł)

Celem procedury jest zapewnienie, że do systemów informatycznych przetwarzających dane osobowe mają dostęp jedynie osoby do tego upoważnione.

1. Pierwsze (pierwotne) hasło użytkownika nadawane jest przez administratora i przekazywane mu w poufny sposób.
2. Użytkownik systemu zobowiązany jest do niezwłocznej zmiany tego hasła.
3. Użytkownik systemu w trakcie pracy w aplikacji może zmienić swoje hasło.
4. W przypadku, gdy użytkownik zapomni hasła, administrator nadaje je ponownie, w trybie pierwszego (pierwotnego) ustawienia.
5. Hasła nie mogą być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: dat, imion, nazwisk, inicjałów, numerów rejestracyjnych samochodów, numerów telefonów.
6. Użytkownik zobowiązuje się do zachowania hasła w poufności, nawet po utracie przez nie ważności.
7. Zabronione jest zapisywanie haseł w sposób jawny oraz przekazywanie ich innym osobom.
8. Standard hasła do wszystkich programów i systemów to: hasło minimum 8 – znakowe, zmieniane co 90 dni. Zmiana hasła i jest wymuszana przez system. Do programów, w których są przetwarzane dane osobowe – zmiana hasła następuje co 30 dni.
9. W przypadku utraty uprawnień przez osobę administrującą systemem należy niezwłocznie zmienić hasła, do których miała dostęp.
10. W przypadkach awaryjnych (np. nieobecność administratora) hasło może być przekazane decyzją Głównego Informatyka osobie zastępującej administratora.
11. Po ustaniu sytuacji awaryjnej, Administrator jest zobowiązany do zmiany hasła.

8. Procedura tworzenia kopii zapasowych

1. Zbiory danych, oprogramowanie oraz konfiguracja systemów operacyjnych serwerów Administratora powinny być zabezpieczone w postaci cyklicznie wykonywanych kopii bezpieczeństwa lub archiwalnych.
2. Kopie bezpieczeństwa należy wykonywać minimum:
    a) przed dokonaniem zmian w konfiguracji systemów operacyjnych lub oprogramowania,
    b) przed dokonaniem zmian w programach (np. zmiana wersji),
    c) przed i/lub po każdej istotnej zmianie danych w bazie danych.

3.Oprócz kopii, o których jest mowa w pkt 2 należy wykonywać kopie archiwalne:
    a) miesięczne - na koniec danego miesiąca,
    b) roczne – na koniec danego roku.

4.Kopie bezpieczeństwa należy:
    a) Wykonywać w co najmniej dwóch egzemplarzach, każdą, przy czym przynajmniej jedną zachować na zaszyfrowanym nośniku wymiennym,

b) Przechowywać w dwóch różnych miejscach, innych niż te, w których zbiory są przechowywane na bieżące (co najmniej w innej strefie pożarowej, w metalowej szafie zamykanej na klucz).

5. Miejsce przechowywania kopii zabezpieczone jest przed nieuprawnionym dostępem oraz skutkami zdarzeń takich jak: pożar, zalanie, oddziaływanie silnego pola elektromagnetycznego, zanieczyszczenia środowiska.

9. Utylizacja elektronicznych nośników i wydruków oraz czyszczenie danych

1. Podlegające likwidacji uszkodzone lub przestarzałe nośniki a szczególności macierze dyskowe / twarde dyski z danymi osobowymi ze stacji roboczych i laptopów / pendrive / pamięci flash / dyski SSD / płyty DVD / telefony komórkowe / smartfony są niszczone w sposób fizyczny. Stosowana metoda niszczenia, to fizyczne niszczenie (pocięcie, nawiercenie, młotkowanie) wymontowanych nośników / zmielenie w specjalistycznej firmie potwierdzone protokołem zniszczenia lub certyfikatem bezpieczeństwa firmy utylizacyjnej lub nagraniem z procesu transportu i utylizacji.
2. Nośniki informacji zamontowane w sprzęcie IT a w szczególności twarde dyski muszą być wyczyszczone zanim zostaną przekazane poza obszar organizacji (np. sprzedaż lub darowizna komputerów stacjonarnych / laptopów / smartfonów).
3. Dokumentacja papierowa niszczona jest w niszczarkach paskowych oraz tam, gdzie to wymagane w niszczarkach o podwyższonym standardzie.
4. Dokumentacja papierowa niszczona jest za pośrednictwem firmy niszczącej dokumenty. Firma zobowiązana jest do wykazania się bezpieczną procedurą utylizacji (np. posiadać certyfikat ISO27001, nagrania z procesu transportu i utylizacji.

10. Procedura zabezpieczenia systemu informatycznego

10.1. Bezpieczeństwo przetwarzania danych poza organizacją

1. Użytkownicy komputerów przenośnych wynoszonych poza obszar organizacji, na których są przetwarzane dane osobowe są zobowiązani do przestrzegania zasad bezpieczeństwa i podpisania regulaminu użytkowania komputerów przenośnych.
2. Stosuje się procedurę zabezpieczenia sprzętu mobilnego.
3. Sprzęt mobilny (smartfony/tablety) zabezpieczono mechanizmem uwierzytelniania.
4. Sprzęt mobilny wyposażony jest w oprogramowanie umożliwiające jego nadzór, blokowanie dostępu, czyszczenie zawartości.
5. W przypadku użycia komputerów przenośnych lub sprzętu mobilnego do zdalnego dostępu do zasobów wewnętrznej sieci przez Internet, stosuje się szyfrowanie tego połączenia z użyciem VPN.
6. W przypadku użycia komputerów przenośnych lub sprzętu mobilnego do zdalnego dostępu do zasobów wewnętrznej sieci przez Internet uwierzytelnienia dokonuje się z użyciem loginu i podania hasła.

10.2. Ochrona przed nieautoryzowanym dostępem do sieci lokalnej

Stosowane zabezpieczenia mają na celu zabezpieczenie systemów informatycznych przed nieautoryzowanym dostępem do sieci lokalnej np. przez programy szpiegujące, hackerów.

1. Dokonuje się aktualizacji oprogramowania (firmware / sterowniki) urządzeń sieciowych oraz innych (np. w urządzeniach jak: routery, switche, access pointy, firewalle, macierze, dyski NAS, drukarki, skanery).
2. Dokonywana jest konfiguracja urządzeń sieciowych oraz innych (routery, switche, access pointy, firewalle, macierze, drukarki, skanery) w celu zabezpieczenia przed nieuprawnionym dostępem do nich (np. zmiana domyślnych haseł na urządzeniach, zmiana domyślnych nazw kont administratora w urządzeniach, konfiguracja portów na routerze).
3. Dokonuje się aktualizacji oprogramowania systemów i aplikacji (systemy operacyjne na stacjach roboczych / systemy operacyjne serwerów / przeglądarki www / Dedykowany CMS / Adobe / Flash / Java / inne). Aktualizacja dokonywana jest zgodnie z zaleceniami producentów oraz opinią rynkową co do bezpieczeństwa i stabilności nowych wersji (np. aktualizacje, service pack-i, łatki).

4. Monitoring usług sieciowych, np.: (np. DHCP, DNS, SSH, http, telnet, FTP, SMTP, SNMP) oraz utrzymuje się niezbędne usługi oraz dezaktywuje pozostałe.
5. Zastosowano system antywirusowy na serwerach i na stacjach roboczych.
6. Zastosowano filtr antyspamowy.
7. Stosowany jest Firewall na serwerach**,** na stacjach roboczych.
8. Zastosowano mechanizmy kontroli dostępu do sieci w postaci: IPS/IDS - do wykrywania i blokowania ataków do sieci komputerowej.
9. Sieć bezprzewodową zabezpieczono technologią WPA.
10. Separacja sieci wewnętrznej od sieci przeznaczonej dla gości (dla wifi i dla Ethernet) np. w salach konferencyjnych.

10.3. Zabezpieczenia infrastruktury IT

1. Serwer wyposażono w macierz dyskową w celu ochrony danych osobowych przed skutkami awarii pamięci dyskowej.
2. Dokonano dezaktywacji nieużywanych gniazd sieciowych (np. przez wypięcie przewodów lub wyłączenie portów na switchu).
3. Na stacjach roboczych zastosowano „zahasłowane wygaszacze ekranu", aktywowane po 5 minutach nieaktywności użytkownika.
4. Ustawienie monitorów uniemożliwiające wgląd w dane przez osoby postronne.

10.4. Zabezpieczenia aplikacji

1. Zapewniono rozliczalność operacji dla pracy w kluczowych aplikacjach / bazach / serwerach plików.
2. W ramach rozliczalności logowane są operacje tworzenia, zmiany (historii zmian), usuwania rekordu, wglądu w dane, eksportu danych do plików.
3. Kluczowe aplikacje/bazy z danymi osobowym zabezpieczono przed eksportem danych do plików (np. tekstowych, .csv, .xls).
4. Zabezpieczono interfejsy programistyczne poprzez zmianę domyślnych loginów i haseł / wyłączenie dostępu zdalnego, gdy nie jest wymagany.
5. Szyfrowanie baz danych.

11. Procedura wykonywania przeglądów i konserwacji

1. Administrator / Informatyk jest odpowiedzialny za monitoring/przegląd logów aktywności aplikacji /baz.
2. Administrator / Informatyk jest odpowiedzialny za monitoring/przegląd logów aktywności oraz uprawnień użytkowników i administratorów.
3. Administrator / Informatyk odpowiada za optymalizację zasobów serwerowych, wielkości pamięci i dysków, optymalizację baz danych.
4. Administrator / Informatyk odpowiada za sprawdzanie poprawności działania systemu IT, w tym: stacji roboczych, serwerów, drukarek, baz danych, aplikacji, poczty email.
5. Administrator / Informatyk odpowiada za identyfikację i przyjmowanie zgłoszeń o nieprawidłowościach w działaniu systemu informatycznego oraz oprogramowania celem ich niezwłocznego usunięcia.
6. W przypadku napraw dokonywanych na zewnątrz z komputerów należy uprzednio wymontować dyski, z urządzeń mobilnych karty pamięci, usunąć dane z nośnika.
7. W przypadku naprawy sprzętu z danymi osobowymi na nośniku - rekomendowane jest zawarcie specjalnego zapisu w umowie serwisowej, gwarantującego bezpieczną naprawę (należy na to zwrócić uwagę przy zakupach sprzętu).
8. W przypadku naprawy sprzętu z danymi osobowymi na nośniku - rekomendowane jest przekazywanie do naprawy uszkodzonego sprzętu z danymi zaszyfrowanymi na dysku / karcie pamięci. Sprzęt przekazywany jest do serwisu bez podania hasła.
9. Rekomendowane jest korzystanie z serwisu, który dokonuje napraw u klienta (umowy gwarancyjne on-site).
10. Czynności konserwacyjne i naprawcze wykonywane przez osoby nieposiadające upoważnień do przetwarzania danych (np. specjalistów z firm zewnętrznych) muszą być wykonywane pod nadzorem osób upoważnionych.

11. Wszelkie prace konserwacyjne i naprawcze sprzętu komputerowego oraz uaktualnienia systemu informatycznego wykonywane przez podmiot zewnętrzny, powinny odbywać się na zasadach określonych w szczegółowej umowie z uwzględnieniem klauzuli dotyczącej ochrony danych.

12. Plan ciągłości działania

12.1. Plan awaryjny odtwarzania systemu informatycznego po awarii krytycznej

1. Zasady postępowania przy odtworzeniu systemu informatycznego w lokalizacji podstawowej:
    a. w przypadku stwierdzenia krytycznej awarii serwera podstawowego w centrali, osoba upoważniona podpina serwer zapasowy, konfiguruje serwer, zgrywa dane z kopii dziennej (zgodnie z wewnętrzną procedurą IT),
    b. po uruchomieniu serwera osoba upoważniona podłącza go do sieci,
    c. Przewidywany czas operacji uruchomienia serwera zapasowego – 6h (sześć godzin),
    d. W przypadku nieobecności osoby upoważnionej, procedurę odtworzenia należy wykonać z pomocą podmiotu zewnętrznego ustalonego w drodze zawartej umowy.
2. Zasady postępowania przy odtworzeniu systemu informatycznego w lokalizacji alternatywnej:
    a. w przypadku zniszczenia miejsca serwerowni wraz z serwerem, należy zaplanowaną uprzednio lokalizację przeznaczyć na alternatywną serwerownię,
    b. przygotowanie serwerowni wymaga: zapewnienia energii elektrycznej, UPS, łącz telekomunikacyjnych,
    c. Informatyk jest odpowiedzialny za dostawę serwera zapasowego, jego konfigurację, wgranie danych z kopii zapasowych (zgodnie z wewnętrzną procedurą IT),
    d. po uruchomieniu serwera Informatyk podłącza go do sieci.
    e. Przewidywany czas operacji uruchomienia serwera zapasowego – 2 dni robocze

12.2. Plan awaryjny na wypadek braku zasilania w sieci komputerowej

1. W razie awarii transformatora zasilającego sieć energetyczną następuje automatycznie przełączenie na drugi transformator.
2. Sieć komputerowa podłączona jest do UPS wyposażonego w baterie wystarczające na ok. 2 godz. pracy.
3. W przypadku dłuższej awarii sieci zasilającej Informatyk zobowiązany jest do powiadomienia wszystkich użytkowników o konieczności zakończenia pracy w systemach.
4. Informatyk wykonuje kopie podstawowych danych.

12.3. Plan awaryjny na wypadek utraty dostępu do sieci Internet

1. W przypadku niedostępności Internetu awarię zgłaszać do informatyka pod numerem 89 752 05 83.
2. W przypadku dłuższej niedostępności Internetu, zgłosić awarię do dostawcy łącza internetowego Orange Sp. z o.o. numer telefonu 510 600 600

Załącznik nr 1
do Instrukcji Zarządzania
Systemami Informatycznymi

PROTOKÓŁ USUNIĘCIA DANYCH OSOBOWYCH

Dnia …… Komisja powołana przez …….

W składzie:

1. Przewodniczący: ……
2. Członkowie : 1)……..
   2)……..

dokonała trwałego zniszczenia zbioru danych osobowych o nazwie …….

Zniszczenie obejmuje:
-wersje papierową zbioru. Zniszczenia dokonano poprzez …….(opisać sposób zniszczenia)
-bazę danych. Zniszczenie dokonano poprzez ……(opisać sposób zniszczenia)
-kopie bezpieczeństwa. Zniszczenia dokonano poprzez …….(opisać sposób zniszczenia)

Dokonanie w/w czynności zostaje potwierdzone własnoręcznymi podpisami Komisji:
……..
……
……