URZĄD GMINY JABŁONNA
ul. Modlińska 152
05-110 Jabłonna
-1-

WÓJT GMINY JABŁONNA
05-110 Jabłonna
ul. Modlińska 152

ZARZĄDZENIE NR 144/2019
WÓJTA GMINY JABŁONNA

z dnia 12 listopada 2019 r.

w sprawie audytu i monitoringu systemu teleinformatycznego w zakresie bezpieczeństwa informacji służących realizacji zadań publicznych oraz wprowadzenia procedury bezpieczeństwa sieci informatycznej w Urzędzie Gminy Jabłonna

Na podstawie art. 33 ust. 3 ustawy z dnia 8 marca 1990 r. - o samorządzie gminnym (tekst jedn. Dz.U. z 2019 r. poz. 506 ze zm.) oraz § 20 ust. 1 i ust. 2 pkt 14 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. z 2016 r. poz. 113 ze zm.) zarządzam, co następuje:

§ 1. 1. W celu zapewnienia bezpieczeństwa systemu teleinformatycznego w Urzędzie Gminy Jabłonna okresowo będzie przeprowadzany audyt bezpieczeństwa informacji.

2. W celu zabezpieczenia systemu teleinformatycznego Urzędu Gminy Jabłonna będzie stosowany stały monitoring komputerów służbowych pod kątem bezpieczeństwa sieci informatycznej przez system nVision.

3. Wprowadza się "Procedurę bezpieczeństwa sieci informatycznej w Urzędzie Gminy Jabłonna" stanowiącą załącznik nr 1 do niniejszego zarządzenia.

§ 2. Wszyscy Pracownicy Urzędu Gminy Jabłonna, będący użytkownikami komputerów, zobowiązani są złożyć pisemne oświadczenie potwierdzające zapoznanie się z treścią niniejszego zarządzenia, celem dołączenia do akt osobowych pracowników.

§ 3. Wykonanie zarządzenia powierzam Kierownikowi Referatu Adminitracyjno-Gospodarczego, Naczelnikowi Wydziału Obsługi Urzędu, a nadzór ogólny nad jego wykonaniem Sekretarzowi Gminy.

§ 4. Zarządzenie wchodzi w życie z dniem 01 grudnia 2019 roku.

WÓJT
Jarosław Chodorski

SEKRETARZ GMINY
Agnieszka Sobczak

Załącznik Nr 1 do zarządzenia Nr 144/2019
Wójta Gminy Jabłonna
z dnia 12 listopada 2019 r.

Procedura bezpieczeństwa sieci informatycznej w Urzędzie Gminy Jabłonna

Niniejsza procedura jest zgodna z zachowaniem prawa do prywatności pracownika uregulowanego w:

1) Konstytucji RP prawo do prywatności, przepisy art.30,31 ust.1 i 2, 47 oraz 51;
2) Kodeksie Cywilnym, ochrony dobra osobistego, jakim jest prywatność, w zakresie przepisów art.23, 24;
3) Kodeksie Pracy – zachowany zostaje obowiązek poszanowania godności i innych dóbr osobistych pracownika wynikających z art.111;
4) warunkach ochrony danych osobowych określonych w ustawie o ochronie danych osobowych.

§ 1. Niniejsza procedura bezpieczeństwa ustala zasady:

1) monitorowania komputerów służbowych;
2) wysyłania służbowej poczty elektronicznej;
3) nadzoru nad bezpieczeństwem sieci IT w Urzędzie;
4) nadzoru nad ochroną danych osobowych w Urzędzie.

§ 2. Celem wdrożenia procedury bezpieczeństwa jest wsparcie bezpieczeństwa informacji w Urzędzie Gminy Jabłonna, a w szczególności:

1) ochrona bezpieczeństwa informatycznego Urzędu;
2) zabezpieczenie danych osobowych przetwarzanych w Urzędzie Gminy Jabłonna.

Wszelkie dane uzyskane w wyniku monitoringu przechowywane będą zgodnie z ustawą o ochronie danych osobowych.

§ 3. 1. Zabronione jest wykorzystywanie przez pracownika komputera służbowego do celów prywatnych.

2. Zabronione jest instalowanie i wykorzystywanie jakiegokolwiek oprogramowania bez wiedzy i udziału Inspektora ds. informatyki. Wszelkie działania pracownika w tym zakresie będą monitorowane.

3. Zabronione jest zapisywanie, przechowywanie na dyskach lokalnych lub zasobach sieciowych wszelkich plików multimedialnych niezwiązanych z wykonywaniem czynności służbowych.

4. Zabronione jest używanie sprzętu komputerowego poza siedzibą Urzędu bez pisemnej zgody na wykorzystywanie sprzętu poza siedzibą pracodawcy.

5. Zabronione jest wykorzystywanie połączenia z siecią internet do celów innych niż służbowe.

6. Zabroniona jest samodzielna zmiana konfiguracji sprzętowej zestawu komputerowego i jego ustawień systemowych bez zgody Inspektora do spraw informatyki.

7. Zabronione jest udostępnianie innym użytkownikom haseł dostępowych i ich przechowywanie w łatwo dostępnych lub widocznych miejscach.

8. Zabrania się samodzielnego wykonywania napraw sprzętu komputerowego (o każdej usterce sprzętu należy powiadomić Inspektora do spraw informatyki).

§ 4. Monitorowanie pracy pracowników przy wykorzystaniu komputerów służbowych będzie przeprowadzone na bazie wspomagającego oprogramowania nVision 11, będącego własnością pracodawcy, który posiada do niego stosowaną licencję.

§ 5. Wszelkie czynności pracownika w zakresie działań Pracodawcy zmierzających do poprawy bezpieczeństwa sieci informatycznej będą monitorowane. Szczegółowy obszar minitoringu określa załącznik Nr 1 do nieniejszej Procedury - „Funkcyjność systemu nVision 11".

§ 6. Zakresem monitoringu w Urzędzie objęte są w szczególności:

1) kontrola zdarzeń na komputerze użytkownika;

2) przesyłanie alertów na komputer pracownika przez Inspektora do spraw informatyki;

3) monitoring używanych przez pracownika aplikacji;

4) możliwość blokowania zbędnych aplikacji, lub stron internetowych;

5) monitoring wykonywanych przez pracowników wydruków;

6) monitoring odwiedzanych przez pracowników stron internetowych;

7) możliwość podglądu on-line ekranu każdego komputera w Urzędzie;

8) monitoring ruchu w sieci informatycznej (LAN, WAN) Urzędu;

9) monitoring legalności oprogramowania;

10) powiadamianie o monitorowaniu każdego użytkownika po uruchomieniu komputera;

11) monitoring służbowych kont poczty e-mail. Pracodawca zastrzega sobie prawo do kontroli treści wysłanych i otrzymanych e-maili z konta służbowego;

12) monitoring używania przenośnych nośników danych (pendrive, karty pamięci, CD-ROM,

HDD, telefony, itp.) z możliwością blokowana, jak i odczytania ich treści;

13) monitoring posiadanego sprzętu w Urzędzie.

§ 7. 1. Każdemu Pracownikowi umożliwia się zapoznanie z pełnym tekstem niniejszej Procedury.

2. Po zapoznaniu się z jego treścią, pracownik jest zobowiązany do podpisania Oświadczenia o zapoznaniu się z jego treścią, którego wzór stanowi Załącznik Nr 2 do niniejszej Procedury.

nVision axence®

Przegląd funkcjonalności modułów

Ogólne

- Agent na Windows
- Agent inwentaryzacji na Linux oraz OS X
- ochrona Agenta przed usunięciem
- pakiet narzędzi diagnostycznych Axence netTools
- alarmy zdarzenie-akcja
- powiadomienia pulpitowe, e-mail, SMS
- akcje korekcyjne (restart, uruchomienie aplikacji itd.)
- raporty dla użytkowników, urządzeń, oddziałów, map sieci lub całego atlasu
- jednoczesna praca wielu administratorów
- zarządzanie uprawnieniami wielu administratorów,
- dziennik dostępu administratorów
- dostęp do Serwera nVision przez przeglądarkę
- menu kontekstowe z możliwością definiowania własnych narzędzi

Network

- skanowanie sieci, wykrywanie urządzeń i serwisów TCP/IP
- interaktywne mapy sieci, mapy użytkownika, oddziałów, mapy inteligentne
- serwisy TCP/IP: poprawność i czas odpowiedzi, statystyka ilości odebranych/utraconych pakietów (PING, SMB, HTTP, POP3, SNMP, IMAP, SQL itp.)
- liczniki WMI: obciążenie procesora, zajętość pamięci, zajętość dysków, transfer sieciowy itp.
- działanie Windows: zmiana stanu usług (uruchomienie, zatrzymanie, restart), wpisy dziennika zdarzeń
- liczniki SNMP v1/2/3 (np. transfer sieciowy, temperatura, wilgotność, napięcie zasilania, poziom tonera i inne)
- monitorowanie listy usług Windows
- kompilator plików MIB
- obsługa pułapek SNMP
- routery i switche: mapowanie portów; informacja, do którego przełącznika jest podłączone urządzenie
- obsługa komunikatów syslog

Inventory

- lista aplikacji oraz aktualizacji Windows na pojedynczej stacji roboczej (rejestr, skan dysków)
- lista kluczy oprogramowania Microsoft
- informacje o wpisach rejestrowych,plikach wykonywalnych, multimedialnych, archiwach .zip oraz metadanych plików na stacji roboczej
- szczegółowe informacje o konfiguracji sprzętowej konkretnej stacji roboczej
- informacje systemowe (komendy startowe, konta użytkowników, foldery udostępnione, informacje SMART itp.)
- audyt inwentaryzacji sprzętu i oprogramowania
- zarządzanie instalacjami/deinstalacjami oprogramowania w oparciu o menedżer pakietów MSI
- historia zmian sprzętu i oprogramowania
- baza ewidencji majątku IT (definiowanie własnych typów środków, ich atrybutów oraz wartości, załączniki, import danych z pliku CSV)
- alarmy: instalacja oprogramowania, zmiana w zasobach sprzętowych
- skaner inwentaryzacji offline
- aplikacja dla systemu Android umożliwiająca spis z natury na bazie kodów kreskowych, QR
- możliwość archiwizacji i porównywania audytów
- monitorowanie harmonogramu zadań Windows

Users

- blokowanie stron WWW
- blokowanie uruchamianych aplikacji
- monitorowanie wiadomości e-mail (nagłówki) - antyphishing
- szczegółowy czas pracy (godzina rozpoczęcia i zakończenia aktywności oraz przerwy)
- użytkowane aplikacje (aktywnie i nieaktywnie)
- odwiedzane strony WWW (tytuły i adresy stron, liczba i czas wizyt)
- audyty wydruków (drukarka, użytkownik, komputer), koszty wydruków
- użycie łącza: generowany przez użytkowników ruch sieciowy
- statyczny zdalny podgląd pulpitu użytkownika (bez dostępu)
- zrzuty ekranowe (historia pracy użytkownika ekran po ekranie)

HelpDesk

- automatyzacje bazujące na założeniu warunek » akcja
- planowanie zastępstw w przydzielaniu zgłoszeń
- rozbudowany system raportów
- powiadomienia w czasie rzeczywistym
- tworzenie zgłoszeń serwisowych i zarządzanie nimi (przypisywanie do administratorów)
- baza zgłoszeń
- widok zgłoszenia odświeżany w czasie rzeczywistym
- komentarze, zrzuty ekranowe i załączniki w zgłoszeniach
- wewnętrzny komunikator (czat) z możliwością przesyłania plików i tworzenia rozmów grupowych
- komunikaty wysyłane do użytkowników/komputerów z możliwym obowiązkowym potwierdzeniem odczytu
- zdalny dostęp do komputerów z możliwym pytaniem uzytkownika o zgodę oraz z możliwością blokady myszy/klawiatury
- zadania dystrybucji oraz uruchamiania plików (zdalna instalacja oprogramowania)
- procesowanie zgłoszeń z wiadomości e-mail
- baza wiedzy z kategoryzacją artykułów i możliwością wstawiania grafik oraz filmów z YouTube
- rozbudowana wyszukiwarka zgłoszeń oraz artykułów w bazie wiedzy
- integracja bazy użytkowników z Active Directory
- przejrzysty i intuicyjny interfejs webowy

DataGuard

- informacje o urządzeniach podłączonych do danego komputera
- lista wszystkich urządzeń podłączonych do komputerów w sieci
- audyt (historia) podłączeń i operacji na urządzeniach przenośnych oraz na udziałach sieciowych
- zarządzanie prawami dostępu (zapis, uruchomienie, odczyt) dla urządzeń, komputerów i użytkowników
- centralna konfiguracja: ustawienie reguł dla całej sieci, dla wybranych map sieci oraz dla grup i użytkowników Active Directory
- integracja bazy użytkowników i grup z Active Directory
- alarmy: podłączono/odłączono urządzenie mobilne, operacja na plikach na urządzeniu mobilnym

Załącznik Nr 2 do Procedury

OŚWIADCZENIE

Ja ..... niżej podpisana(y) informuję, że zapoznałem się z Zarządzeniem nr 144/2019 Wójta Gminy Jabłonna z dnia 12 listopada 2019 r. i zobowiązuję się do przestrzegania zapisów zamieszczonych w „Procedurze bezpieczeństwa sieci informatycznej w Urzędzie Gminy Jabłonna".

Jednocześnie przyjmuję do wiadomości, że Inspektor do spraw informatyki monitoruje wszelkie czynności wykonywane na moim komputerze oraz ma możliwość zdalnej pracy na komputerze pracownika.